



TIC Y DERECHOS HUMANOS

Julio Gaitán Bohórquez

2017





TIC Y DERECHOS HUMANOS

**CONSEJO SUPERIOR DE LA JUDICATURA
SALA ADMINISTRATIVA
ESCUELA JUDICIAL “RODRIGO LARA BONILLA”**



CONTENIDO

CONVENCIONES	4
PRESENTACIÓN.....	5
SINOPSIS PROFESIONAL Y LABORAL DEL AUTOR.....	6
JUSTIFICACIÓN	7
BREVE RESUMEN DEL MÓDULO.....	9
TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	11
Unidad 1: INTERNET.....	12
1.1 ¿Cómo funciona Internet?	14
1.1.1 Los diferentes niveles de Internet.....	14
1.2 Cómo se gobierna	22
1.2.1 Modelo multistakeholder	22
1.3 Internet como terreno en disputa	23
Unidad 2: LIBERTAD DE EXPRESIÓN Y ANONIMATO EN INTERNET	31
2.1 Libertad de expresión	33
2.2 Preservar la arquitectura de Internet.....	34
2.3 Los intermediarios de Internet	38
2.4 Pluralismo y no discriminación en la expresión digital.....	42
2.5 Limitaciones legislativas y prohibición de la censura previa.	44



2.5.1 Previsión legal clara y expresa.....	44
2.5.2 Objetivos legítimos imperiosos a la luz de la Convención Americana.....	45
2.5.3 Test de necesidad, proporcionalidad e idoneidad de la medida.	
45	
2.5.4 Jurisdicción.....	46
2.5.5 Devido proceso y control judicial.....	48
2.5.6 Prohibición de censura previa	48
2.6. Anonimato.....	49
Unidad 3: INTIMIDAD EN LA ERA DIGITAL	54
3.1 Actividades previas.....	55
3.2 La vigilancia e interceptación de las comunicaciones.....	57
3.3 Retención de datos.....	62
3.4 Explotación de datos.....	67
Unidad 4: FLUJOS DE INFORMACIÓN.....	71
4.1 La neutralidad de la red.....	72
4.2 Filtrado y bloqueo	76
4.3 Violencia de género y entornos digitales.....	79
5. CASO INTEGRADO INTEGRADOR	85
6. BIBLIOGRAFÍA GENERAL	87



CONVENCIONES

Og	Objetivo General
Oe	Objetivos específicos
Co	Contenidos
Ap	Actividades pedagógicas
Ae	Autoevaluación
J	Jurisprudencia
B	Bibliografía



PRESENTACIÓN

En la elaboración de este módulo sobre TIC y Derechos Humanos se han tenido en cuenta las siguientes directrices:

1. Las recomendaciones recogidas en los talleres de planificación realizados por la Escuela Judicial para la identificación de las necesidades en cada una de las temáticas que integrarán cada Módulo y Cartilla.
2. El bloque normativo integrado por el texto de las normas internacionales aplicables en Colombia, la Constitución Política y las normas con fuerza de ley.
3. El texto integral de las Sentencias proferidas por la Corte Constitucional a partir de 1992 sobre cada una de las temáticas de los respectivos Módulos y Cartillas.
4. La doctrina colombiana existente en esta materia, contenida en libros y revistas especializadas, construida a partir de la expedición de la Constitución de 1991.
5. En todo caso, la parte teórica de cada uno de los Módulos y Cartillas se construyen a partir de las líneas jurisprudenciales existentes en cada una de las materias que son objeto de estudio.
6. Los Módulos se desarrollan teniendo en cuenta la supremacía de la Constitución y el respeto, garantía, protección y efectividad de los derechos humanos.
7. Igualmente se tendrán en cuenta los deberes y finalidades de las autoridades en el contexto del Estado Social de Derecho, en especial aquellos que están a cargo de la administración de justicia en todas las ramas del derecho.

La existencia de un módulo sobre TIC dentro del programa de Formación de la Escuela Judicial “Rodrigo Lara Bonilla” encuentra su justificación en la necesidad urgente de pensar y responder a los desafíos planteados a los derechos en los nuevos entornos y dinámicas que han emergido particularmente durante los últimos 20 años con la popularización y los extraordinarios desarrollos de Internet.



SINOPSIS PROFESIONAL Y LABORAL DEL AUTOR

JULIO GAITÁN BOHÓRQUEZ es Profesor Titular en el área de derecho constitucional de la facultad de Jurisprudencia y Director del Centro de Internet y Sociedad de la Universidad del Rosario -ISUR-. Es Abogado egresado de la misma Universidad, Magíster en Derecho Público de la Universidad Autónoma de Barcelona, Doctor en Evolución de los sistemas jurídicos y nuevos derechos de la Universidad de Lecce - Italia. Fue Director del programa de Doctorado en Derecho de la Universidad del Rosario (2010-2016). Ha realizado estancias de Investigación en Instituto Max Planck de Frankfurt (Alemania – 2002) y en la Universidad de California en Berkeley (2007, 2013, 2018). Profesor de Historia del Derecho en la Universidad Autónoma de Barcelona (2004–2005). Fue Magistrado Auxiliar y Conjuez de la Corte Constitucional Colombiana. Coordinó el Área de Memoria Histórica del Centro Internacional para la Justicia transicional en Colombia. Trabaja problemáticas de derecho constitucional, derechos humanos en entornos digitales, pluralismo jurídico, culturas jurídicas e historia del derecho.



JUSTIFICACIÓN

Este módulo posibilita, por una parte, la comprensión básica de la forma y lógica de operación de Internet, tanto en algunos de sus aspectos técnicos como de gobernanza, abordando estas temáticas desde un enfoque cívico y práctico con el propósito de que les sirva a Magistradas y Magistrados, Juezas y Jueces de herramienta para la resolución de casos problemáticos y complejos, a la vez que contribuya de forma significativa a mejorar el acceso efectivo de las usuarias y de los usuarios a una administración de justicia de mayor calidad en un campo que experimenta transformaciones y nuevos retos a ritmos a los que seguramente ningún otro campo del derecho y, en general, de las relaciones sociales, se habían enfrentado.

Tanto la institucionalidad del Estado Social de Derecho como la ciudadanía vienen experimentando situaciones conflictivas desconocidas hasta hace un par de décadas, al menos en su magnitud y potencia de incidencia, así como desarrollos de viejas tensiones derivadas de la potenciación de la comunicación que implica el uso de Internet.

Siempre es previsible que el Constituyente no pueda prever numerosos campos de desarrollo tecnológico y sus implicaciones en las relaciones sociales y político-jurídicas. Sin embargo, las transformaciones asociadas al acelerado desarrollo de Internet y sus impactos en todos los aspectos de la vida humana han sido sustanciales y es apenas previsible que impacten irremediablemente las concepciones que hemos resguardado las y los juristas durante décadas e incluso algunos durante siglos. Desarrollos en campos como la inteligencia artificial o implantes corporales artificiales que reconfiguran las capacidades humanas (Ciborgs), son apenas ejemplos de los retos implicados en pensar los impactos de Internet en las concepciones y los desarrollos de los derechos.

Sin embargo, es necesario reequilibrar la reflexión precedente con la conciencia de que las cuestiones y retos planteados por las relaciones sociales con relevancia jurídica en entornos digitales no son una novedad absoluta, sino que cuentan con importantes referentes y discusiones en el campo doctrinal y jurisprudencial que se han ocupado de las tensiones entre los derechos, así como de las garantías de estos frente a las incidencias de poderes estatales o corporativos.



“El Código es la ley”. La aproximación jurídica a la emergencia de la Internet y de sus consecuencias legislativas regulatorias o judiciales presupone la comprensión del mecanismo y de las lógicas que la atraviesan, así como los esfuerzos por encausarla jurídicamente requieren de adaptaciones o comprensiones más amplias de la actividad regulatoria. En palabras de Lessig:

“El ciberespacio exige una comprensión novedosa de cómo funciona la regulación y, así, nos compele a mirar más allá del ámbito tradicional de los abogados – más allá de las leyes o incluso de las normas. El ciberespacio requiere una concepción más amplia de la «regulación» y, lo que es más importante, el reconocimiento de un regulador de singular relevancia.

Dicho regulador es la oscuridad que da título a este libro – el código. En el espacio real somos capaces de reconocer de qué modo reglamentan las leyes – por medio de constituciones, estatutos y demás códigos legales. En el ciberespacio, hemos de comprender cómo regula un «código» diferente – es decir, cómo el software y el hardware, que hacen del ciberespacio lo que es, constituyen su «código». Como subraya William Mitchell, dicho código es la «ley» del ciberespacio. Joel Reidenberg la denominó Lex informática, si bien prefiero la fórmula «el código es la ley»¹

En las tensiones entre las posibilidades de control estatal o corporativo que facilita el ciberespacio y cuyas coordenadas ordinariamente escapan al control consciente del ciudadano o del consumidor, por una parte, y el resguardo de los derechos y libertades que el Estado social de derecho busca garantizar, por la otra, es fundamental la labor de un poder judicial informado y atento, que comprenda las características del funcionamiento de Internet, sus componentes tecnológicos y los actores del ecosistema digital.

1

Lessig, Lawrence, *El código 2.0*, Madrid, Traficantes de sueños, 2009, pág. 37.



BREVE RESUMEN DEL MÓDULO

El Módulo sobre Tecnologías de la Información y las Comunicaciones pretende satisfacer algunas de las necesidades de formación de Magistradas, Magistrados, Juezas y Jueces, identificadas dentro de los talleres diagnósticos elaborados con antelación por la Sala Administrativa del Consejo Superior de la Judicatura, obedeciendo a los criterios que definen el modelo pedagógico de la Escuela Judicial, tales como la puesta en práctica de metodologías activas de aprendizaje, el aprendizaje basado en el estudio de problemas, el aprendizaje autodirigido, el respeto por los derechos fundamentales y por la dignidad humana, el compromiso socializador.

El módulo de Tecnologías de la Información y Comunicaciones se ocupa de identificar criterios, precedentes y demás elementos de apoyo que les resulten útiles y pertinentes a las operadoras y los operadores judiciales a la hora de resolver los casos problemáticos y complejos que de manera creciente comienzan a llegarles a sus despachos, relacionados con nuevas problemáticas y matices que presentan los desarrollos y tensiones de derechos en los entornos digitales, producto de múltiples confusiones generadas por la apenas emergente, cuando no, ausencia de criterios normativos específicos, apenas en construcción en el ámbito nacional, regional y mundial, de jurisprudencia consolidada y de los nuevos retos planteados a las jurisdicciones nacionales por tecnologías y lógicas de operación y alcance global.

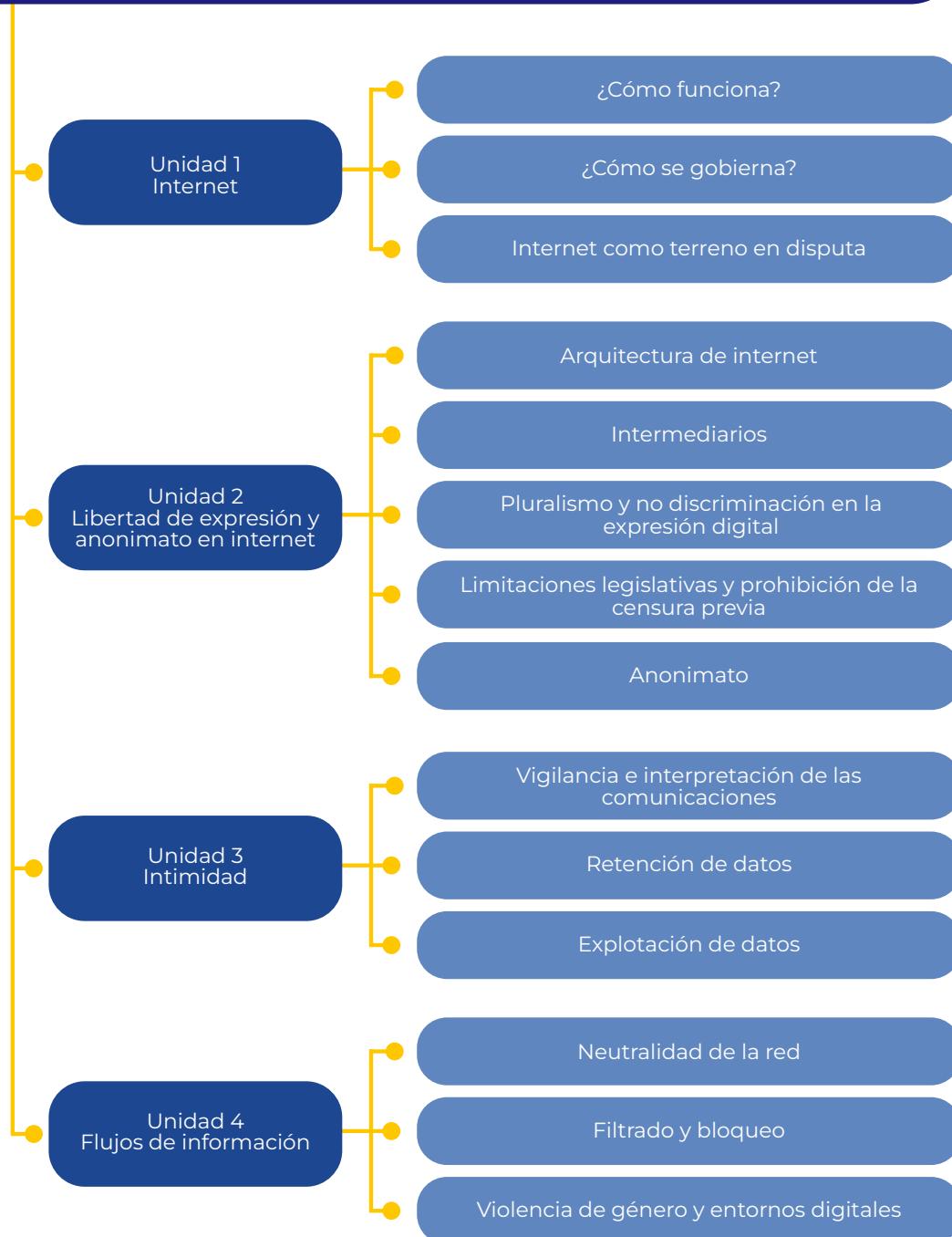
En esta medida, el referente conceptual del trabajo que aquí se propone es el abordaje de las nuevas tensiones de los derechos en los entornos digitales, para lo cual se requiere, en primer lugar, proporcionar las coordenadas técnicas básicas del funcionamiento de Internet, así como de su gobernanza, para luego presentar algunos de los principales escenarios de disputa de los que viene ocupándose la jurisdicción en relación con algunos derechos.

De acuerdo con lo anterior, este trabajo se desarrolla desde la perspectiva de la identificación de los nuevos escenarios en los que se potencian y desarrollan los conflictos de derechos y libertades y las implicaciones de los desarrollos tecnológicos en su ejercicio con el propósito de sensibilizar a las operadoras y los operadores judiciales en relación con los cambios operados por los desarrollos tecnológicos en el campo de los derechos y, en consecuencia, en el abordaje legislativo, judicial y regulador que debe realizar el Estado.



MAPA CONCEPTUAL DEL MÓDULO

MÓDULO DE FORMACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES





TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Og

- Lograr una administración de justicia sensible a las transformaciones operadas por las Tecnologías de la Información y las Comunicaciones -TIC- en el campo de los derechos y de su protección, a partir de la comprensión de sus esquemas generales de funcionamiento técnico y del conocimiento de las principales problemáticas disputadas en el campo judicial contemporáneo, que han producido las primeras decisiones jurisdiccionales en relación con este campo específico.
- Determinar la aplicabilidad de los estándares internacionales, así como los criterios extraídos de la emergente jurisprudencia de las altas cortes sobre estos asuntos, los cuales les permitan a las y los discentes solucionar las problemáticas que llegan a sus despachos, superando las confusiones derivadas de la ausencia de criterios normativos y de la escasa jurisprudencia.
- Motivar a las administradoras y a los administradores de justicia para que armonicen conceptos y sostengan diálogos permanentes con las normativas y decisiones tomadas por tribunales regionales o extranjeros en relación con las problemáticas abordadas en el Módulo.

Oe

- Entender la lógica de funcionamiento de Internet y sus consecuencias en las posibilidades del desarrollo de los derechos, así como los peligros o amenazas para su ejercicio.
- Comprender la manera en la que los estándares internacionales en materia de derechos humanos se aplican a los problemas generados por las nuevas tecnologías de la información y las comunicaciones en el mundo de los derechos.
- Abordar algunas de las problemáticas de los derechos humanos en los entornos digitales.



Unidad 1: INTERNET

Og

Explicar en forma sencilla el nuevo contexto tecnológico con el propósito de brindar los elementos, conceptos y términos básicos, necesarios para el abordaje y comprensión de las problemáticas jurídicas relacionadas con Internet, que van a discutirse en este Módulo.

Oe

Aspectos básicos de Internet
¿Cómo funciona?

- Reconocer los elementos técnicos básicos del funcionamiento de Internet, las capas que contribuyen a su operación y las consecuencias en la responsabilidad diferenciada de quienes intervienen de acuerdo con su vinculación a cada una de esas capas.
- Definir con precisión las diferentes capas de la Red de redes que es Internet. La primera capa, de infraestructura, la segunda, de los protocolos de comunicación y, la tercera, de información, reconociendo la presencia de diferentes actores en cada una de ellas.
- Percibir las particularidades tecnológicas y de arquitectura de la Red implicadas en las disputas por derechos o por la regulación de las actividades en la Red a la hora de administrar justicia, manteniendo los principios y valores del Estado Social de Derecho.

¿Cómo se Gobierna?

- Analizar el surgimiento de Internet y las diferentes aproximaciones discutidas desde sus comienzos a la regulación de su funcionamiento hasta el modelo de múltiples partes interesadas. La definición de los actores en la gobernanza de Internet, los diferentes frentes en los que se ha desarrollado legislación nacional e internacional en aspectos que tocan con Internet.
- Identificar los diferentes actores y sus diferentes funciones en el desarrollo de Internet: Gobiernos, empresas privadas, comunidades académicas y tecnológicas, y sociedad civil. De manera especial se ahondará en el especial rol de los intermediarios. También comprenderá el modelo de colaboración y beneficio mutuo sobre el que se desarrolla Internet y el modelo de gobernanza de múltiples partes interesadas en la discusión de los asuntos relacionados con el desarrollo y aplicación de principios, normas, reglas, procedimientos y programas que dan forma a la evolución y uso de Internet.
- Valorar los diferentes aspectos de las competencias y derechos en los entornos digitales en cuestiones como la seguridad de gobiernos, instituciones o individuos, la privacidad, la libre expresión, los derechos de autor, los derechos humanos, etc.

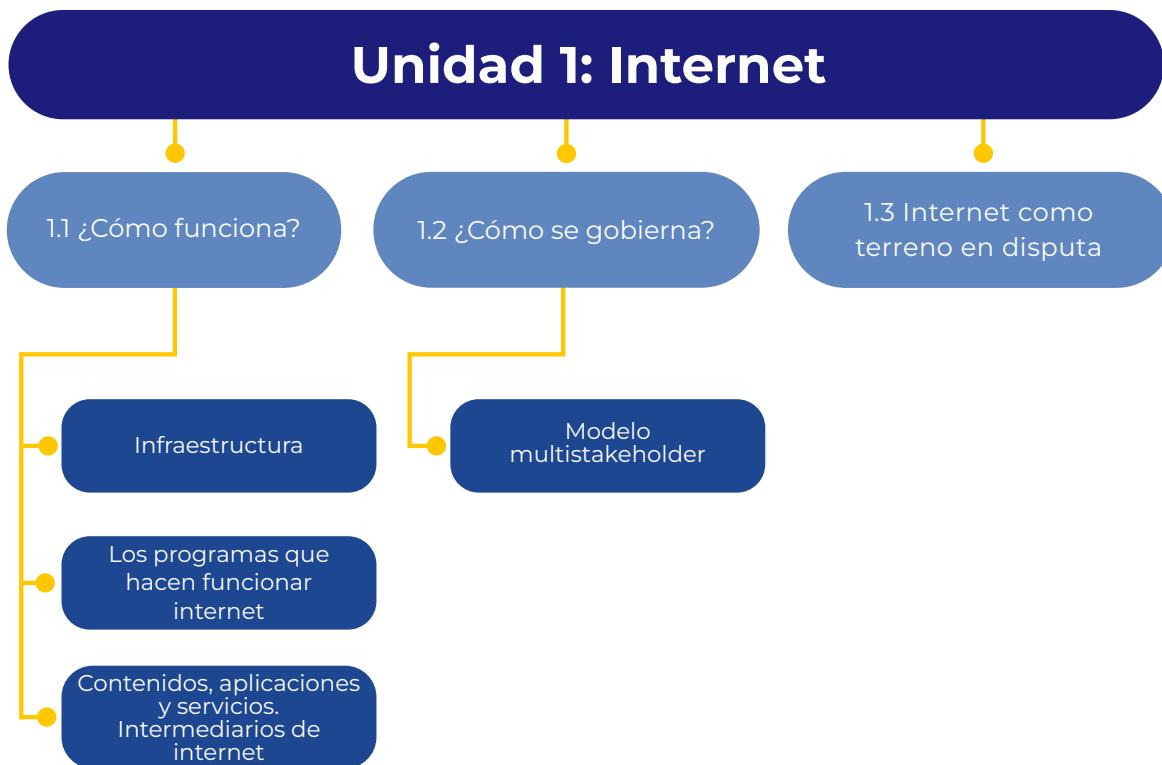


Oe

Internet como terreno de disputa:

- Examinar y aplicar las reglas de interpretación desarrolladas por la jurisprudencia, a la hora de resolver las diferencias conceptuales y los conflictos derivados de las normas y procedimientos, en casos de disputas de derechos humanos en los entornos digitales en el marco de las posibilidades y los límites trazados por la Constitución y las leyes.
- Aplicar los criterios de interpretación a casos concretos, solucionando las renovadas o las nuevas tensiones y problemáticas que se presentan entre derechos y entre estos y su regulación en Internet.
- Velar por la protección de los derechos fundamentales en el marco del Estado social de derecho, priorizando la protección de los derechos humanos sobre otras consideraciones, en el desarrollo de las prácticas posibilitadas por los entornos digitales.

MAPA CONCEPTUAL





Co

Contenidos

1.1 ¿Cómo funciona Internet?

Quizás la parte más visible de Internet es la relacionada con la navegación web y los servicios que se ofrecen a través de ella, es decir, Internet hoy es sinónimo de servicios como el buscador de Google, el servicio de streaming de contenidos Netflix, las tiendas virtuales como Amazon o Mercadolibre o los servicios de mensajería y redes sociales como WhatsApp y Twitter. Sin embargo, Internet está constituida por diversos niveles de infraestructura, programas y servicios, que son administrados por diferentes actores. Cada uno de ellos, tiene a cargo una parte del funcionamiento de Internet, bien sea por razones técnicas o comerciales y puede ser sujeto de distintas obligaciones.

1.1.1 Los diferentes niveles de Internet

Internet está compuesta de un gran número de dispositivos distribuidos por todo el mundo y conectado por diversos medios.² Su arquitectura permite distinguir entre diferentes niveles. Para simplificar, se puede dividir Internet en: (1) el nivel de la infraestructura física, (2) el de los programas que hacen funcionar la transmisión de mensajes y (3) el de los contenidos, aplicaciones o servicios que funcionan a través de Internet.

1.1.1.1 Primer nivel: la infraestructura

El nivel de infraestructura comprende los medios por los cuales se transporta la información en Internet. Por decirlo de otra manera, es el conjunto de antenas, satélites, cables convencionales o de fibra óptica, entre otros, que sirven para enviar y recibir paquetes desde sus orígenes hasta sus destinos. Esta maraña de cables y equipos permite que, por ejemplo, dos computadores situados en diferentes lugares de la red tengan un canal virtual de comunicación.

Así mismo, la infraestructura comprende a los actores relacionados con la administración de los componentes físicos de Internet. Este aspecto resulta más relevante para los propósitos de este manual que los cables y equipos usados para el funcionamiento de Internet pues da cuenta de las responsabilidades de distintos actores de Internet.

² Peña Ochoa, P., *¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas*, Santiago, ONG Derechos Digitales, 2013, p. 7. Recuperado de: <https://www.derechosdigitales.org/wp-content/uploads/Como-funciona-Internet-ebook.pdf> <https://www.derechosdigitales.org/wp-content/uploads/Como-funciona-internet-ebook.pdf>.



TIC Y DERECHOS HUMANOS

Para entender el nivel de infraestructura de Internet es conveniente poner un ejemplo. Para acceder a Internet, en primer lugar, se requiere un dispositivo como un computador o un celular y una conexión. La conexión es un servicio que ofrecen los llamados “proveedores de acceso a Internet” (PAI). Los PAI son responsables por el acceso de cada hogar o teléfono móvil y están sujetos a obligaciones especiales que tienen relación con el goce de derechos fundamentales como la libertad de expresión. Una de estas obligaciones es la de respetar la neutralidad de la red, de la cual se hablará en la unidad 4.

Así como cada persona no tiene acceso a Internet en sí misma, sino sólo a la red de su PAI, los PAI deben conectarse con otras redes. Por eso se dice que Internet es una red de redes. En un principio, Internet era una red de computadores. Cuando en 1969 se envió el primer mensaje de Internet, la red tenía menos de diez computadores. A medida que la utilidad de compartir recursos e información fue puesta en evidencia, la red empezó a crecer, sumando más computadores. Sin embargo, este crecimiento no significó que todos los computadores estuvieran conectados entre sí. Más bien, ocurría que había grupos de computadores conectados entre sí, que formaban redes, pero cada uno de esos grupos no estaba conectado con los demás. Sólo en 1983 se sentaron las bases técnicas necesarias para que las redes tuvieran el lenguaje, o protocolo, necesario para comunicarse entre sí.³

Los PAI, que son redes que ofrecen su conexión al público en general, deben conectarse a redes más grandes, que a su vez se conectan a otras redes, conocidas como redes o PAI de primer nivel (Tier-1 ISP en inglés). Excepto por los PAI de primer nivel, todas las demás redes pagan por la conexión con las demás. Estas conexiones ocurren en lugares conocidos como puntos de intercambio de Internet (IXP en inglés) o puntos de acceso a redes (NAP en inglés). En Colombia existe uno de estos puntos, llamado NAP Colombia, y está integrado por diferentes empresas de telefonía.⁴

La razón por la que las personas quieren conectarse a Internet y por la cual existen todo el andamiaje de conexión entre redes es para conseguir acceso a los diferentes contenidos, aplicaciones y servicios que se ofrecen en la red. Aunque los administradores directos de esos contenidos son materia a tratar en el tercer nivel, es importante aclarar que los contenidos están alojados en complejos conocidos como “servidores”. Cualquier contenido que se encuentre en Internet está alojado en otro computador al cual

³ Blum, A. (2013). *Tubos en busca de la geografía física de Internet*. (E. Mercado, Trad.).
⁴ NAP Colombia. Preguntas frecuentes. Recuperado de <http://nap.co/html/faq.php> <http://nap.co/html/faq.php> <http://nap.co/html/faq.php>



se accede a través de la red. Por esa razón, quienes ofrecen contenidos son también clientes de los PAI. La función de ofrecer alojamiento puede hacerse como un servicio, conocido como servicio de “hosting” o alojamiento de sitios web (p.ej. HostGator, A2 Hosting o DreamHost) o puede ser tipo “cloud” o nube (p.ej. Amazon Web Services, Microsoft Azure o Google Cloud Platform). La diferencia entre alojamiento web y nube es principalmente técnica. En todo caso, ambas cumplen la función de depósito de contenidos a los cuales puede accederse a través de Internet. Físicamente, los servicios de hosting o cloud tienen que estar conectados a la red con una conexión especial y diferente de la que se usa en los hogares.

1.1.1.2 Segundo nivel: los programas que hacen funcionar Internet

El nivel de los programas o estándares y servicios técnicos, “contiene la infraestructura que hace funcionar Internet, donde toma forma y se transportan sus datos”.⁵ Aquí se determinan las reglas de tráfico de los datos que viajan por Internet, es decir, el lenguaje que se utilizará para que los dispositivos puedan comunicarse entre sí. Ese lenguaje se conoce como protocolo, un conjunto de reglas que nos dicen cómo tienen que viajar los datos por Internet. El estándar de Internet es el protocolo TCP/IP, que permite que dispositivos muy diferentes puedan comunicarse entre sí.

Internet funciona a partir del envío y recepción de paquetes de información. Cualquier contenido que circula en Internet es dividido en paquetes más pequeños, que son transmitidos por diferentes caminos. Para que el envío pueda funcionar, también se necesita una forma clara de identificar al emisor y receptor del paquete.

El procedimiento para dividir la información en paquetes y enviarla a los destinatarios correspondientes es el que controla un lenguaje o protocolo conocido como TCP/IP. Por un lado, el protocolo de control de transmisión (TCP en inglés) se encarga de manejar el envío de los datos por Internet. TCP permite que la información viaje por Internet en pequeños paquetes de datos, que se unifican al llegar a su destino final luego de revisar la suma de los paquetes con la información original. En resumidas cuentas, el protocolo TCP se encarga de verificar cómo se dividen, se envían y se unen los paquetes de datos, colocando cada paquete en un sobre IP. El protocolo de Internet (IP en inglés), por su parte, cuida que los paquetes de datos lleguen a la dirección de destino correcta, en donde serán unificados. Así, cada emisor y receptor tienen una dirección IP.

5

Ibid, p. 14



Antes de su llegada, los paquetes de datos pasan por diferentes routers (aparatos encargados de transportar datos a través de Internet), que se ocupan de examinar la dirección de los mismos para que lleguen correctamente a su destino final. Esto es posible porque cada paquete tiene una cabecera con información sobre su origen y su destino (dirección del destinatario y del remitente).

Lo anterior puede ejemplificarse en la siguiente analogía:

Enviar información por Internet usando el protocolo IP es como mandar por correo postal las páginas de un libro en muchos sobres distintos. Todos los sobres tienen la misma dirección del remitente y la misma dirección del destinatario. Aunque algunos sobres viajen por mar y otros por aire, tarde o temprano todos llegarán a su destino previsto y el libro podrá ser encuadrado de nuevo. Da lo mismo que la página 1 llegue después que la 47.⁶

Para acceder a un sitio web usamos una dirección IP⁷ numérica asignada al servidor. Las direcciones IP no son otra cosa que números organizados en bloques, como por ejemplo 74.125.224.72, el IP de uno de los servidores donde está alojado el buscador de Google.

Ahora bien, por razones técnicas, las direcciones IP en sí mismas no son un método infalible para la identificación de personas. Esto es relevante para los casos en los que un titular de derechos de autor pretende una decisión judicial en la que se reconozcan daños y perjuicios en su favor, haciendo responsable a la persona suscrita al servicio de Internet que tuvo asignada la dirección IP desde la que se hizo la descarga ilegal. En Estados Unidos son conocidos los casos⁸ en los que empresas productoras de material pornográfico presentan demandas individuales por cada una de las direcciones IP que pueden identificar como aquellas que descargaron ilegalmente su material. Aunque las vicisitudes del procedimiento estadounidense en este contexto ofrezcan muchos aspectos interesantes

⁶ EDRi (s.f.). ¿Cómo funciona Internet? The EDRi Paper. 3a. edición, p. 3. Recuperado de http://www.edri.org/files/paper03_20120725_02_esp.pdf

⁷ El actual y más popular protocolo de red es IPv4. No obstante, el bloque de direcciones IPv4 está próximo a agotarse. El IPv6 es el sucesor propuesto de IPv4. La diferencia entre esas versiones, es que el IPv6 utiliza direcciones de fuente y destino de 128 bits, muchas más direcciones que las que provee IPv4 con 32 bits.

⁸ Keith Wagstaff, "You are not an IP address, rules judge", TIME, Mayo 7 de 2012. Recuperado de: <http://techland.time.com/2012/05/07/you-are-not-an-ip-address-rules-judge/> <http://techland.time.com/2012/05/07/you-are-not-an-ip-address-rules-judge/>



TIC Y DERECHOS HUMANOS

desde el punto de vista legal y constitucional, puede decirse que es claro que una dirección IP no basta para identificar a una persona en particular como el agente de una conducta ilegal, lo que impone un obstáculo a las demandas en masa presentadas por estas compañías en búsqueda del reconocimiento económico de daños.⁹

Por otro lado, en un contexto distinto al de las infracciones al derecho de autor, el Tribunal de Justicia Europeo ha ratificado que las direcciones IP deben protegerse como datos personales, especialmente cuando quien conoce esta dirección, dispone de los medios legales necesarios para obtener los demás datos necesarios para identificar a una persona detrás de una dirección IP. Esta regla jurisprudencial se expresó con ocasión de la demanda que interpuso un ciudadano alemán en contra de la República Federal Alemana que, en sus sitios web, conserva la información relativa al “nombre del sitio o fichero consultado, los términos introducidos en los campos de búsqueda, la fecha y hora de la consulta, la cantidad de datos transmitidos, la constatación del éxito de la consulta y la dirección IP del ordenador desde el que se ha realizado la consulta”¹⁰.

El contraste entre los debates suscitados alrededor de la dirección IP en Estados Unidos y Europa demuestra la complejidad de la relevancia jurídica de los elementos tecnológicos detrás de Internet y apunta a la necesidad de jueces y magistrados de comprender el papel de una pieza tecnológica como la dirección IP y ponderar su importancia y significado en cada caso concreto.

Más allá de las discusiones jurídicas, los sitios web, en lugar de identificarse con su IP, se reconocen con un nombre de dominio. Para ello se ha creado el Sistema de Nombres de Dominio (DNS, por sus siglas en inglés), que sirve como una especie de guía telefónica para Internet y que relaciona un IP con un nombre. Esto ha facilitado considerablemente la navegación y comercialización de Internet, puesto que lo único que hay que conocer para acceder a un sitio web es el nombre de dominio (p.ej. mercadolibre.com, elespectador.com) y el DNS se encarga de encontrar la dirección IP

⁹ Ver, por ejemplo, *Malibu Media v. Chris Fodge (NJD 14-cv-07611)*, Opinion and Denying motion. Juez Kevin McNulty. Recuperado en <https://ia800404.us.archive.org/24/items/gov.uscourts.njd.312461/gov.uscourts.njd.312461.17.0.pdf> y *Cobbler Nevada, LLC v. Gonzales (ORD 15-cv-00866)*, findings and recommendations. Juez Stacie Beckerman recuperado en <https://ia800203.us.archive.org/13/items/gov.uscourts.ord.121926/gov.uscourts.ord.121926.35.0.pdf>

¹⁰ Tribunal de Justicia Europeo. Asunto C-582/14 – *Breyer vs Bundesrepublik Deutschland*. Sentencia del de 19 de octubre de 2016. Recuperado en <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62014CJ0582>



del servidor web donde se aloja el sitio. Por lo general, una misma IP es compartida por muchos dominios porque están almacenados o alojados en un mismo servidor. Así, bloquear sitios web concretos basándose en su dirección IP suele tener consecuencias adversas para el resto de las páginas alojadas en el mismo servidor.

Por ejemplo, a principios de 2017, varios sitios web quedaron bloqueados como resultado de una orden judicial emitida en España que obligaba al proveedor de acceso a Internet de primer nivel Cogent a bloquear ciertas direcciones IP, sin entender que dichas direcciones pertenecían a un servicio que agrupaba varios sitios web que no eran objeto de la orden.¹¹

Ahora bien, una parte de este nivel tiene que ver con los “[e]stándares de contenidos y aplicaciones, que es la que usualmente ven los usuarios y que identifican como Internet”.¹² Es decir, el medio por el que es posible intervenir o interactuar con Internet: sitios web, correos electrónicos, aplicativos de intercambio de archivos, mensajería instantánea, etc.

Estos medios están basados también en protocolos. Uno de ellos es el HTTP (siglas para HyperText Transfer Protocol) o el conjunto de reglas acordadas para transferir hipertextos de Internet (texto o imágenes que, al hacer clic en ellos, llevan a otro sitio web). Opera por medio de solicitudes y respuestas entre un navegador web (i.e. Firefox, Chrome, Internet Explorer, Safari) y el servidor que aloja el sitio web buscado. HTTP como protocolo no debe ser confundido con la World Wide Web o WWW, que es el conjunto de recursos conectados a través del protocolo HTTP.

Cualquier computador conectado a Internet cumple los protocolos TCP/IP para enviar y/o recibir información. Asimismo, cualquier desarrollador puede inventarse un nuevo protocolo y usarlo en Internet, con la única condición de que el formato sea uno estándar que permita el intercambio de datos. También existen protocolos de Internet que distinguen según el tipo de comunicación: SMTP para enviar correos electrónicos, HTTP para acceder a sitios web y Peer-to-Peer (P2P) para compartir archivos con muchas personas, etc.

¹¹ “Internet Backbone Cogent blocks Cloudflare’s New ‘Pirate Site’ IP-addresses”, Ernesto, marzo 22 de 2017, TF. Recuperado en <https://torrentfreak.com/internet-backbone-cogent-blocks-cloudflares-new-pirate-site-ip-addresses-170322/>

¹² Peña Ochoa, op. cit., p. 22.



TIC Y DERECHOS HUMANOS

El uso universal de un protocolo único para todas las comunicaciones, a su vez, tiene varias ventajas. Los routers no necesitan ser programados en función del tipo de dato, ni tampoco tienen que tener información sobre los datos que transporta. Mientras el protocolo usado sea el IP, lo único que tienen que leer es aquello que, siguiendo la analogía antes utilizada, aparece en el sobre para poder entregar el mensaje, tal cual lo hace el cartero que reparte cartas.

Podría decirse entonces que Internet ofrece un servicio flexible: llevar datos de un dispositivo a otro sin importar la naturaleza de estos, de dónde y cómo se conectan a Internet, o del tipo o contenido de los datos.

1.1.1.3 Tercer nivel: contenidos, aplicaciones o servicios. Intermediarios de Internet

Hasta ahora aparece claro que sin un sinnúmero de facilitadores de tecnología no nos es posible enviar correos, montar una página o leer el periódico. Son muchas las actividades, personas y organizaciones que hacen esa facilitación, por tanto, se pueden definir como intermediarios de Internet. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) propuso en 2011 una definición:

Los intermediarios de Internet acercan o facilitan transacciones entre terceros en Internet. Dan acceso a, hospeda, transmite o indexan contenido, productos y servicios originados por terceros en Internet o proveen servicios basados en Internet a terceros¹³ (Texto original en inglés).

Dado el dinamismo de la red, difícilmente puede hablarse de una lista cerrada de categorías. Sin embargo, la OCDE identificó 6 tipos:

1. Proveedores de Servicios de Internet (PSI), que se refieren a quienes ofrecen la conexión, sea por cable o por celular. Se conocen internacionalmente como Internet access and service providers (ISPs).
2. Procesadores de datos y proveedores de hospedaje para la Web, que incluye a los registradores de nombres de dominio.
3. Motores de búsqueda de Internet y portales.
4. Intermediarios de comercio electrónico.
5. Sistemas de pago para Internet.
6. Plataformas de trabajo colaborativo, que incluyen plataformas de publicación en Internet y de broadcasting. Usualmente este intermediario ni crea ni es propietario del contenido que protege o emite.

¹³ *OECD (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing. Recuperado en <http://dx.doi.org/10.1787/9789264115644-en>.*



El Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye, a propósito del papel del sector privado en el contexto digital, clasificó las actividades de los intermediarios de Internet así¹⁴:

1. Habilitar la conexión a Internet
2. Diseñar y mantener equipos físicos y sistemas operativos que faciliten el procesamiento de la información y el acceso a Internet
3. Asignar dominios de Internet
4. Información sobre alojamiento web
5. Facilitar la agregación, el intercambio y la búsqueda de información
6. Producir contenido propio y regular el acceso
7. Conectar a los usuarios y las comunidades
8. Vender bienes y servicios y facilitar las transacciones
9. Reunir datos, adaptarlos a nuevos fines y venderlos

En términos generales, se trata de actores necesarios para el funcionamiento de Internet y en su calidad de intermediarios, en principio, no son responsables del uso que los usuarios hagan de sus servicios.

Aunque las categorías buscan resaltar las diferencias en el papel de los diferentes “intermediarios” que hay en Internet, lo cierto es que usualmente un mismo intermediario tendrá actividades en más de uno de estos roles. Así, por ejemplo, ETB es un PAI y también presta servicios de alojamiento de contenidos para otros.

El propósito esencial de clasificar a los intermediarios es resaltar que cumplen actividades diferentes que suponen procesos tecnológicos distintos, capacidades diversas, entre otros. Este entorno no ha sido ajeno al marco jurídico, antes bien ha generado efectos importantes en el ejercicio de derechos y ha propiciado el desarrollo de sus propios marcos jurídicos.

¹⁴ Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. A/HRC/32/38. 11 de mayo de 2016.



1.2 Cómo se gobierna

Los aspectos determinantes del funcionamiento de Internet están en manos de las interacciones de los diferentes actores en cada uno de los niveles explicados anteriormente. En particular, existen algunas instituciones encargadas de administrar recursos centrales de Internet como los nombres de dominio, las direcciones IP o de aprobar los diferentes protocolos que pueden ser usados para transmitir información. Por otro lado, todos estos actores confluyen en un modelo de toma de decisiones gobernado por un modelo conocido como “multistakeholder” o “de múltiples partes interesadas. A continuación se especifican las diferentes autoridades de Internet y luego se habla del modelo multistakeholder.¹⁵

1.2.1 Modelo multistakeholder

El creciente reclamo por el control de Internet, específicamente de ICANN, centrado en Estados Unidos llevó a que la organización de las Naciones Unidas y a través de la International Telecommunications Union (ITU) apareciera el World Summit on the Internet Society (WSIS) en 2003.¹⁶ En esta reunión se creó el Working Group for Internet Governance (WGIG) que se encargó de preparar el siguiente WSIS a realizarse en Túnez y construyó una agencia que se supone guiaría el futuro de la Internet.¹⁷ En la agenda de Túnez se definió la gobernanza de Internet y el modelo que debería encargarse de esta tecnología:

“La gobernanza de Internet es el desarrollo y la aplicación, hecha por los gobiernos, el sector privado y la sociedad civil, en sus respectivos roles, de los principios compartidos, las normas, las reglas, los procesos de decisión y los programas que moldean la evolución y el uso de la Internet”¹⁸

Así, se determinó que la gobernanza de la Internet era algo que les concernía a tres actores: los gobiernos, el sector privado y la sociedad civil. Igualmente, la definición dejó claro que cada stakeholder debía participar desde sus respectivos roles, pero no logró definir claramente cuáles eran esos roles.¹⁹ De esta forma, apareció el Foro de Gobernanza de Internet (IGF en inglés)

¹⁵ Para una introducción al tema, puede verse: “Sobre la gobernanza en Internet”, RedPaTodos. Recuperado en https://www.youtube.com/watch?v=HU2Vbo_SxIs.

¹⁶ Mueller, M. (2010). *Networks and states: the global politics of Internet governance*. Cambridge, Mass: MIT Press.

¹⁷ Savage, J. E., & McConnell, B. W. (2015). *Exploring Multi-Stakeholder Internet Governance*. Brown University Bruce W. McConnell, EastWest Institute.

¹⁸ Ibid.

¹⁹ Doria, A. (2014). *Use [and Abuse] of Multistakeholderism in the Internet. In The Evolution of Global Internet Governance (pp. 115-138)*. Springer, Berlin, Heidelberg.



para discutir cuestiones concernientes a la gobernanza de Internet donde todos los actores interesados pudieran participar. A pesar de que el IGF no tuviera poder de decisión tuvo un importante lugar en el desarrollo del modelo, pues logró que los stakeholders se sentarán a compartir sus preocupaciones.²⁰ Desde dicha definición de multistakeholder iniciaron los cambios en el interior de las organizaciones encargadas de factores esenciales para el funcionamiento de la Internet. Con esto, ICANN, IETF, W3C, ITU, ISOC y IOSCO se declararon organizaciones multistakeholder.

El objetivo de involucrar a diferentes partes interesadas ha sido crear procesos participativos para la toma de decisiones sobre Internet, así como crear espacios para que preocupaciones locales puedan tener eco global. El modelo multistakeholder, podría ser definido, siguiente la Agenda de Túnez, como un mecanismo de decisión en el cual participan activamente todas las partes interesadas, entendidas como los gobiernos, el sector privado, la sociedad civil, las organizaciones intergubernamentales y las comunidades técnicas y académicas, de forma igualitaria, abierta y transparente para la construcción de los principios, las normas, las reglas, los procesos de decisión y los programas que moldean la evolución y el uso de Internet.

El foro de gobernanza de Internet ha sido replicado a nivel regional y local. En Latinoamérica, existe el LACIGF mientras que, en Colombia, la Mesa de Gobernanza de Internet funciona como un espacio para que distintos actores, las múltiples partes interesadas, discutan sobre aspectos que consideran relevantes para la toma de decisiones sobre Internet. La Mesa Colombiana de Gobernanza de Internet celebra anualmente el Foro de Gobernanza de Internet local, que tiene los mismos propósitos.

1.3 Internet como terreno en disputa

Es ampliamente reconocido que Internet tiene un importante impacto en la consecución de objetivos de desarrollo social, económico y cultural. Tanto es así que en el seno de las Naciones Unidas se discute la importancia de las tecnologías de la información y las comunicaciones, incluido Internet, como eje central de la Agenda para el Desarrollo Post-2015. Así, en la Declaración Conjunta del Grupo de Trabajo de las Naciones Unidas sobre la Sociedad de la Información, durante la Cumbre de mayo de 2013 en Ginebra, se propuso que se reconozca en la Agenda Post-2015:

²⁰ Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*. Terminus Press



TIC Y DERECHOS HUMANOS

[...] el potencial de las TIC como herramientas clave del desarrollo, y como componentes críticos de soluciones de desarrollo innovadores. Teniendo en cuenta la importancia de contenidos relevantes, habilidades y entornos propicios, las TIC, incluyendo Internet de banda ancha, tecnologías móviles y aplicaciones tecnológicas pertinentes, deben reconocerse plenamente como herramientas que pueden ayudar a empoderar a las personas, permitir un más amplio ejercicio de los derechos humanos, como la libertad de expresión, fomentar el acceso a la información, abrir oportunidades de empleo, ampliar el acceso al aprendizaje, la educación y los servicios básicos. En colaboración con otros grupos de interés, el sistema de las Naciones Unidas debe tratar de sacar el máximo provecho de las TIC para hacer frente a los desafíos de desarrollo del siglo 21 y reconocerlos como facilitadores transversales para el logro de los tres pilares del desarrollo sostenible.²¹ (Texto original en inglés)

Y es la arquitectura descentralizada y abierta de Internet la que ha permitido maximizar el poder de los usuarios de innovar y crear, de buscar contenidos e información y de generarlos, de compartir ideas, de participar más ampliamente en el mercado laboral, en la vida política, de asociarse, de manifestarse, de educarse y un largo etcétera. Cuando existen controles excesivos, gubernamentales o privados, sobre cualquiera de las 3 capas antes discutidas, los beneficios sociales, políticos y económicos pueden quedar mermados significativamente. El acceso y uso de Internet, por lo tanto, amplía las posibilidades para el ejercicio de los derechos humanos, condición necesaria para el mantenimiento de democracias robustas. Pero este infinito mundo de posibilidades para el desarrollo y maximización de potencialidades no está exento de riesgos y amenazas.

Hoy día el gran flujo de la información que circula por Internet aumenta el grado de vulnerabilidad de las personas por posibles injerencias arbitrarias en sus derechos fundamentales. Por lo que el reto de no es menor. De una parte, se espera que los gobiernos sepan enfrentar los retos y amenazas de Internet mediante legislaciones, regulaciones y demás actuaciones legislativas que se construyan a partir de un acercamiento en derechos humanos. De otra, hace falta una mayor alfabetización digital que permita al usuario común prevenir y mitigar riesgos a su seguridad personal, además de hacer valer sus derechos y libertades fundamentales, al igual que respetar los derechos de otros. En la Declaración Conjunta sobre Libertad de Expresión e Internet de los organismos regionales de derechos

²¹ Grupo de Trabajo sobre la Sociedad de la Información (2013). Declaración Conjunta sobre la Agenda para el Desarrollo Post-2015, párr. 4.1. Recuperado en <http://www.ungis.org/Portals/0/documents/JointInitiatives/UNGIS.Joint.Statement.pdf>



TIC Y DERECHOS HUMANOS

humanos, se afirmó que “[d]eben fomentarse medidas educativas y de concienciación destinadas a promover la capacidad de todas las personas de efectuar un uso autónomo, independiente y responsable de Internet ('alfabetización digital')”.

La red global ha permitido, asimismo, que la información circule de manera rápida y amplia, sin discriminación de quien busque la información. Pero ese círculo de información ha cobrado mayor significación, pues, quien recibe la información no es un mero receptor pasivo, sino un activo publicador. Ya para el 2011, el Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), resaltaron

(...) el carácter transformador de Internet, como medio que permite que miles de millones de personas en todo el mundo expresen sus opiniones, a la vez que incrementa significativamente su capacidad de acceder a información y fomenta el pluralismo y la divulgación de información.²²

Y esta realidad es la que ha permitido que hoy Internet se considere un espacio para el disfrute de los derechos humanos y, por tanto, para el desarrollo de sociedades democráticas. Así, el reconocimiento del Internet como un medio esencial para el ejercicio de los derechos humanos, más específicamente para la libertad de expresión, está sustentado en el artículo 19 de la Declaración Universal de Derechos Humanos, en el artículo 19 numeral 2 del Pacto Internacional de Derechos Civiles y Políticos, y en el artículo 13 de la Convención Americana Sobre Derechos Humanos. El anterior Relator Especial de Naciones Unidas (ONU) para la Libertad de Expresión y de Opinión, Frank La Rue, fue enfático en señalar que, al actuar como catalizador para que las personas ejercent la libertad de expresión y de opinión, Internet facilita también la realización de un amplio rango de derechos humanos.²³ Más aún, en julio de 2012, el Consejo de Derechos Humanos de las Naciones Unidas emitió una resolución en la que enfatiza que Internet es un espacio de derechos humanos, por lo tanto, estos deben ser protegidos de igual forma.²⁴

22 Declaración conjunta sobre libertad de expresión e Internet. 1 de junio de 2011, Considerando No. 4. Recuperado en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2>.

23 Report of the Special Rapporteur on freedom of opinion and expression, Frank La Rue (2011, 6 May). A/HRC/17/27. Recuperado en http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

24 Consejo de Derechos Humanos de las Naciones Unidas (2012, 29 de julio). Promoción, protección y disfrute de los derechos humanos en Internet. A/HRC/20/L.13. Recuperado en http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf



Ap

Actividad 1: La infraestructura de Internet

Objetivos

- Evidenciar los diferentes aspectos físicos de Internet
- Mostrar los distintos actores que hacen parte de Internet
- Entender algunos aspectos básicos de la técnica que hace funcionar Internet

Materiales

En hojas individuales, imprimir el documento adjunto con las distintas partes que están involucradas en el envío de un mensaje a través de Internet. El material consiste en un archivo PDF con una imagen que corresponde a un subtítulo. Por ejemplo (Imagen de un computador portátil) - Subtítulo: Portátil.

El número de imágenes que usen los participantes puede variar, pero es esencial que estén involucradas las siguientes:

- Dispositivos de emisión y recepción del mensaje. En cada punta de la cadena debe estar o un celular o un computador portátil.
- Módem o antena de celular o satelital.
- Cables de fibra óptica o UTP.
- Cables submarinos o estación de antena satelital.
- Data center de los proveedores de acceso a Internet nacionales (Claro, ETB, etc.)
- Data center de los proveedores del servicio de correo (Google, Yahoo, etc.)

Ejecución de la actividad

La persona que dirija la actividad dividirá al grupo en grupos menores, si es necesario, y entregará un juego de imágenes completo a cada grupo. Sin explicar previamente ningún concepto sobre la infraestructura de Internet, cada grupo deberá ordenar la cadena de elementos (cables, módems, data centers, etc.) a través de los cuales pasa un mensaje en Internet, según su intuición.

La hipótesis sobre la cual deberán trabajar es la siguiente: "Una persona, a través de su cuenta de Gmail, envía a otra, que tiene una cuenta en Yahoo, un correo electrónico. Una de ellas usa Internet a través de su conexión fija de ETB mientras que la otra usa Internet móvil de Claro".



Ap

Discusión

Una vez los grupos consideran que han armado correctamente la cadena se procederá a explicar cada uno de los pasos. Para orientar este punto se explicará la cadena en un orden particular (desde un portátil a un celular, desde Gmail a Yahoo y desde ETB a Claro) pero es correcto también organizarlo de otra forma, intercambiando empresas o dispositivos.

1. El envío del mensaje se realiza desde un computador portátil, desde una cuenta de Gmail y a través del Internet fijo de ETB. Para ello, el siguiente paso en la cadena es el modem que provee la empresa para realizar la conexión. Aunque la mayoría de modems en hogares tienen capacidades WiFi, también es posible conectarse a ellos a través de un cable UTP. En ese caso, entre el portátil y el modem puede aparecer un cable UTP.
2. El módem se conecta a través de un cable de fibra óptica o cable UTP con el data center de ETB.
3. El data center de ETB se conecta a través de cables submarinos con el data center de Google, que es el proveedor del servicio de correo Gmail. Es posible que estén conectados con cables de fibra óptica o UTP, pero en todo caso, habría una conexión con un cable submarino puesto que la mayoría de servicios de Internet no están alojados en Colombia y la mayor parte del tráfico pasa por Estados Unidos a través de cables submarinos.
4. El data center de Google puede estar conectado con el data center de Yahoo a través de cables UTP, de fibra óptica o submarinos. Los cables UTP o de fibra óptica indicarían que ambos data center se encuentran en el mismo continente. Los cables submarinos, en cambio, indicarían que los data centers están separados por un océano.
5. El data center de Yahoo estaría conectado igual que el de Google con el data center de Claro. Es decir, podría estar conectado por cables submarinos.
6. El data center de Claro estaría conectado con una torre de telefonía celular a través de cables de fibra óptica.
7. La torre envía la señal por radio al celular, por lo cual entre la torre y el celular no hay ningún otro elemento.

A través de esta revisión, deberían poder formularse las siguientes preguntas:

- ¿Qué aspecto técnico de la infraestructura de Internet resulta menos claro?
- ¿Qué aspecto económico de la infraestructura de Internet resulta menos claro?
- ¿Qué implica para la decisión de la jurisdicción competente la particular estructura de Internet?



Ap

Actividad 2: Mi sombra y yo

Objetivos:

- Entender la relación que existe entre la información generada al navegar en Internet, usar servicios en línea y el derecho a la intimidad y la protección de datos.
- Evidenciar la cantidad y tipo de información que recolectan las empresas que prestan servicios de Internet (no de conexión a Internet), es decir, los intermediarios de Internet.
- Reconocer la importancia de los intermediarios de Internet en tanto administradores de información personal de las personas que usan sus servicios.

Materiales:

- Acceso a Internet
- Dispositivo móvil o computador

Ejecución de la actividad:

En la medida de lo posible, cada participante entrará al sitio web: myshadow.org/es. El sitio web "Yo y mi sombra" es desarrollado y mantenido por el colectivo Tactical Technology. El objetivo del sitio es evidenciar los rastros tecnológicos que deja cada persona al usar dispositivos digitales.

El sitio está dividido en tres partes. La primera, explica en detalle en qué consisten los rastros digitales. La segunda, muestra quién y cómo recolecta la información digital. La tercera, rebate algunos argumentos sobre la supuesta irrelevancia de la recolección de datos personales para los derechos fundamentales.

Es recomendable la lectura de los materiales en las partes primera y tercera, aunque la segunda involucra directamente a cada participante. En el enlace: <https://myshadow.org/es/trace-my-shadow> se puede encontrar instrucciones para descubrir cómo funciona el rastreo en cada caso.

Los participantes marcarán las casillas en la izquierda que correspondan a su uso de Internet. Por ejemplo, desde qué dispositivos, con qué sistemas operativos, dónde accede a Internet, etc. En la mitad aparecerán los rastros específicos que van dejando cada una de las opciones marcadas. Por ejemplo, números de teléfono, historial de navegación, etc. Cada uno de ellos tiene una opción para ver más información. En el panel de la derecha aparecerán unos consejos prácticos para proteger cierta la información comprometida por el uso de los dispositivos digitales (marcados en las casillas de la izquierda).



Ap

Discusión

- ¿Cuáles rastros digitales ya se conocían? (P. ej. Historial de navegación)
- ¿Cuáles rastros eran desconocidos?
- ¿Cómo cambian los hábitos de uso de Internet a partir de la comprensión de la información que queda como rastro?
- ¿Quién usa esa información y para qué?
- ¿Compromete la privacidad de las personas el uso de esa información?
- ¿Qué salvaguardas deben reconocerse para el acceso a esa información por parte del Estado a través de sus agencias (investigación criminal o inteligencia, por ejemplo)?

Ae

Autoevaluación

1. ¿Considera usted que es posible el abordaje jurídico de los problemas que plantea Internet desde los marcos constitucionales, legislativos, regulatorios y jurisprudenciales nacionales? Justifique su respuesta, afirmativa o negativa, atendiendo a las características tanto físicas como de lenguajes de comunicación unificados y con alcance global que implica Internet.

J

Jurisprudencia

- Tribunal de Justicia Europeo. Asunto C-582/14 – Breyer vs Bundesrepublik Deutschland. Sentencia del de 19 de octubre de 2016. Recuperado en: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62014CJ0582>
- Malibu Media v. Chris Fodge (NJD 14-cv-07611), Opinion and Denying motion. Juez Kevin McNulty. Recuperado en <https://ia800404.us.archive.org/24/items/gov.uscourts.njd.312461/gov.uscourts.njd.312461.17.0.pdf>
- Cobbler Nevada, LLC v. Gonzales (ORD 15-cv-00866), findings and recommendations. Juez Stacie Beckerman disponible en [https://ia800203.us.archive.org/13/items/gov.uscourts.ord.121926.35.0.pdf](https://ia800203.us.archive.org/13/items/gov.uscourts.ord.121926/gov.uscourts.ord.121926.35.0.pdf)



B

- LESSIG, L. El código 2.0, Madrid, Traficantes de sueños, 2009.
- PEÑA OCHOA, P. (2013). ¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Chile: ONG Derechos Digitales
- BLUM, A. (2013). Tubos en busca de la geografía física de Internet. (E. Mercado, Trad.).
- EDRI (s.f.). ¿Cómo funciona Internet? The EDRI Paper. 3a. edición. Recuperado en http://www.edri.org/files/paper03_20120725_02_esp.pdf.
- MUELLER, M. (2010). Networks and states: the global politics of Internet governance. Cambridge, Mass: MIT Press.
- SAVAGE, J. E., & McConnell, B. W. (2015). Exploring Multi-Stakeholder Internet Governance. Brown University Bruce W. McConnell, EastWest Institute
- DORIA, A. (2014). Use [and Abuse] of Multistakeholderism in the Internet. In The Evolution of Global Internet Governance (pp. 115-138). Springer, Berlin, Heidelberg.
- MUELLER, J. (2008). Multi-stakeholder governance and the Internet Governance Forum. Terminus Press.
- OECD (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing. Disponible en <http://dx.doi.org/10.1787/9789264115644-en>.
- Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. A/HRC/32/38. 11 de mayo de 2016.
- Report of the Special Rapporteur on freedom of opinion and expression, Frank La Rue (2011, 6 May). A/HRC/17/27. Disponible en http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf



Unidad 2: LIBERTAD DE EXPRESIÓN Y ANONIMATO EN INTERNET

Og

Aproximarse a las particularidades de la libertad de expresión en Internet a la luz de los estándares internacionales.

Oe

- Identificar estándares internacionales y precedentes jurisprudenciales que le permitirán resolver de forma sustentada las tensiones que se están presentando en Internet entre la libertad de expresión y otros derechos como la honra, la reputación, la imagen y la intimidad. Se plantearán también los temores que el anonimato ha generado y la actual tendencia hacia su prohibición y el debilitamiento del cifrado.
- Resolver de forma técnicamente fundamentada y jurídicamente soportada, los problemas jurídicos que se presenten en la práctica judicial producto de los conflictos por derechos o por regulación de Internet, aplicando la normativa nacional e internacional, los estándares sobre derechos humanos y los precedentes jurisprudenciales objeto de estudio.
- Promover mediante las decisiones judiciales la protección de los derechos implicados frente a tendencias invasivas de control, vigilancia y perfilamiento que tienden a restringir ilegítimamente su ejercicio o que lo desincentivan.



MAPA CONCEPTUAL

Unidad 2: Libertad de expresión y anonimato en internet

- 2.1 Arquitectura de internet
- 2.2 Intermediarios
- 2.3 Pluralismo y no discriminación en la expresión digital
- 2.4 Limitaciones legislativas y prohibición de la censura previa
- 2.5 Anonimato



2.1 Libertad de expresión

Existe prolíjo material sobre libertad de expresión. Se recomienda hacer un repaso sobre el tema en general antes de comenzar la lectura de este capítulo, que aplica esos parámetros generales a las problemáticas y particularidades de Internet.

Las lecturas sugeridas en relación con Libertad de Expresión en su conexión con Internet son las siguientes:

- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. Documento oea/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Disponible en: <http://bit.ly/1WHR6cD> <http://bit.ly/1WHR6cD>
- Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 22 de mayo de 2015. Documento ONU A/HRC/29/32, Cifrado y anonimato en las comunicaciones digitales. Disponible en: <http://bit.ly/2pa0zYu>
- 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. Disponible en: <http://on.unesco.org/2qwfUaS>
- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 2014. Disponible en <http://bit.ly/1qR7bYf> <http://bit.ly/1qR7bYf>
- Universidad de los Andes, Dejusticia y Open Society Foundations. Nuevos Desafíos: Libertad de Internet. Unesco. Cajadeherramientas para escuelas judiciales iberoamericanas. Formación de formadores en libertad de expresión, acceso a la información pública y seguridad de periodistas. Edición Marine González, 2017. Disponible en <http://unesdoc.unesco.org/images/0025/002515/251593S.pdf> <http://unesdoc.unesco.org/images/0025/002515/251593S.pdf>
- Comisión Interamericana de Derechos Humanos (CIDH). Relatoría Especial para la Libertad de Expresión. Video: "Libertad de expresión e Internet". 17 de junio de 2014. Disponible en <https://www.youtube.com/watch?v=YaTvcMCrcNg> <https://www.youtube.com/watch?v=YaTvcMCrcNg>



TIC Y DERECHOS HUMANOS

- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Recuperado en <http://www.globalmediapolicy.net/node/15836>.
- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/38/35. Abril 6 de 2018. Recuperado en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.
- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Párr. 56. Recuperado en <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>.
- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Párr. 56. Recuperado en <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>. <http://www.globalmediapolicy.net/node/15836>.

La presente unidad ajusta, amplia y localiza elementos sustanciales del módulo 8 del texto “El Derecho a la Libertad de Expresión. Curso Avanzado para Jueces y Operadores Jurídicos en las Américas”. Propuesta curricular y materiales de estudio. Elaborado por Catalina Botero, Federico Guzmán, Sofía Jaramillo y Salomé Gómez para DeJusticia con el apoyo de Open Society Foundations (OSF). 2017, Disponible en: <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf>. En todo caso.

2.2 Preservar la arquitectura de Internet

¿Cómo preservar la arquitectura de Internet como un instrumento de ejercicio de la libertad de expresión al regularla, limitarla o intervenirla?

La libertad de expresión es un derecho que protege la emisión y recepción de todo tipo de pensamientos, opiniones, ideas e información personal de quien se expresa. Tiene sustento en el artículo 20 de la Constitución Política de 1991 que prescribe:



"Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".

El derecho a la libertad de expresión es un principio fundamental para una sociedad democrática, reconocido en instrumentos internacionales de derechos humanos suscritos por Colombia como, por ejemplo, la Convención Americana sobre Derechos Humanos, en su artículo 13, en la Declaración de Principios sobre Libertad de Expresión y la Declaración Americana, en su artículo IV.

Por su parte los organismos internacionales también reconocen la prevalencia de este derecho. La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la Comisión Interamericana y la jurisprudencia de la Corte Interamericana de Derechos Humanos han resaltado que la libertad de expresión cumple una triple función en el sistema democrático:

1. asegura el derecho de toda persona a pensar por cuenta propia y a compartir su pensamiento y opinión personal,²⁵
2. tiene una relación esencial y estructural con la democracia, y en esa medida, responde al objetivo del artículo 13 de la Convención Americana de fortalecer el funcionamiento de sistemas democráticos, pluralistas y deliberativos, mediante la protección y fomento de la libre circulación de ideas y opiniones,²⁶ y
3. es una herramienta clave para el ejercicio de otros derechos fundamentales pues "se trata de un mecanismo esencial para el ejercicio del derecho a la participación, a la libertad religiosa, a la educación, a la identidad étnica o cultural y, por supuesto, a la igualdad, no sólo entendida como el derecho a la no discriminación, sino como el derecho al goce de ciertos derechos sociales básicos".²⁷

²⁵ CIDH, Informe No. 11/96. Caso No. 11.230. *Francisco Martorell vs. Chile*. 1996, párr. 56.

²⁶ Corte I.D.H., *Opinión Consultiva OC-5/85 del 13 de noviembre de 1985; La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos)*.

²⁷ Relatoría Especial para la Libertad de Expresión, *Comisión Interamericana de Derechos Humanos CIDH; "Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión"*, 30 de diciembre de 2009. Disponible en <http://www.oas.org/es/cidh/expresion>



TIC Y DERECHOS HUMANOS

Este marco ha quedado registrado en la jurisprudencia nacional,

"Aunque la libertad de expresar y difundir el propio pensamiento y opiniones es un derecho de toda persona, no es sólo un derecho individual, sino también garantía de una institución política fundamental. "la opinión pública libre". Una opinión pública libre está indisolublemente ligada con el pluralismo político, que es un valor fundamental y un requisito de funcionamiento del estado democrático. Sin una comunicación pública libre quedarían vacíos de contenido real otros derechos que la Constitución consagra, reducidos a formas hueras las institucionales (sic) representativas y participativas y absolutamente falseado el principio de la legitimidad democrática".²⁸

El desarrollo jurisprudencial en materia de libertad de expresión en Colombia es muy amplio. El sistema judicial enfrenta ahora el reto de hacerlo pertinente a la nueva realidad tecnológica dado que las características de Internet ofrecen un importante potencial para permitir la expresión y la comunicación humanas. La arquitectura original descrita en el capítulo 1 permite el libre intercambio de información y opiniones. Esa es la gran diferencia en relación con las tecnologías que facilitaban los medios de comunicación que precedieron a Internet. Por ejemplo, Internet, al desarrollar sus principios fundacionales, permite comunicaciones de muchos a muchos, mientras que la TV, la radio, el cine, etcétera, funcionan de uno a muchos, y esa diferencia es sustancial para potenciar la libertad de expresión de cualquier persona, no solo de algunas.

Para conservar Internet con estas características se requiere que se preserve esa arquitectura. Las autoridades que pretendan regular las comunicaciones en línea o de cualquier manera limitar las expresiones que se realizan a través de esta red deben tener este propósito expreso. En este sentido, los Relatores para la Libertad de Expresión de la Organización de Estados Americanos (OEA), la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana han expresado que: "los enfoques de reglamentación desarrollados para otros medios de comunicación —como telefonía o radio y televisión— no pueden transferirse sin más a Internet, sino que deben ser diseñados específicamente para este medio, atendiendo sus particularidades".²⁹

²⁸ Corte Constitucional, *Sentencia T-403 de 1992. M. P. Eduardo Cifuentes Muñoz*

²⁹ *El Relator Especial para la Libertad de Opinión y de Expresión de Naciones Unidas (ONU), la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial para la Libertad de Expresión de la Organización de Estados Americanos (OEA) y la Relatora Especial para la 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, punto 1 (c). Disponible en <http://bit.ly/1eX83sn> <http://bit.ly/1eX83snhttp://bit.ly/1eX83sn>*



TIC Y DERECHOS HUMANOS

Por su parte la Comisión Interamericana de Derechos Humanos (CIDH) ha afirmado que

Internet se ha desarrollado a partir de determinados principios de diseño, cuya aplicación ha propiciado y permitido que el ambiente en línea sea un espacio descentralizado, abierto y neutral. Es importante que cualquier regulación que se produzca [...] mantenga las características básicas del entorno original, potenciando su capacidad democratizadora e impulsando el acceso universal y sin discriminación.³⁰

Más aún, por su condición de medio sin parangón para el ejercicio de la libertad de expresión, es ese derecho fundamental (art.20 C.P.) el que debe ser uno de los principales criterios guía en el momento de establecer regulaciones o intervenciones sobre Internet. Al decir de la Relatora de la CIDH,

(...) todas las medidas que puedan de una u otra manera afectar el acceso y uso de Internet deben interpretarse a la luz de la primacía del derecho a la libertad de expresión, sobre todo en lo que respecta a los discursos especialmente protegidos en los términos del artículo 13 de la Convención Americana.³¹

Por su parte, la Corte Constitucional colombiana ha recogido esta visión. En la sentencia T-277 de 2015 cuando indicaba:

El acceso masivo de personas a Internet, sin lugar a dudas, ha representado un cambio en la forma en que se lleva a la práctica el derecho a la libertad de expresión... Dentro de las características que hacen de Internet un espacio idóneo para la manifestación de diversas formas de expresión se incluyen: (i) libertad de acceso; (ii) multiplicidad de formatos de información; (iii) descentralización en la producción y consumo de información; (iv) posibilidad de interacción de los usuarios en tiempo real; (v) neutralidad en cuanto al tipo de información compartida, entre otras. En consecuencia, no se tiene duda de la importancia que tiene Internet para la garantía de la libertad de expresión en el siglo XXI.³²

La libertad de expresión es un derecho en sí misma y es, además, herramienta esencial para la defensa de otros derechos, por lo tanto, es un elemento fundamental de la democracia y aprovechar las características de Internet para potenciarla sirve para ampliar el impacto de derechos como el de libre asociación o el de la igualdad.

³⁰ CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. oea/Ser.L/V/II.cidh/rele/inf.11/13.31 de diciembre de 2013. párr. 11. Recuperado en <http://bit.ly/1WHR6cD> <http://bit.ly/1WHR6cD>

³¹ Ibídem. párr. 14.

³² Corte Constitucional, Sentencia T-277 de 2015 <http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm>. M.P. María Victoria Calle Correa.



2.3 Los intermediarios de Internet

Un elemento importante en la función judicial de buscar la conservación de la arquitectura de Internet como espacio de ejercicio de derechos humanos consiste en proteger el rol de los intermediarios de Internet, en su mayoría actores privados, como se expuso en el capítulo 1. El Relator de Naciones Unidas para la libertad de expresión, en su informe de 2016 sobre el rol del sector privado para el desarrollo de Internet³³, reconoce e identifica la profunda influencia que tienen, en general, los actores privados en el respeto a la libertad de expresión en la era digital. En su informe, también busca hacer visibles las responsabilidades que recaen sobre las autoridades para asegurarse de que se proteja este espacio en defensa y promoción de la libertad de expresión. El informe reconoce como problemática la tendencia de que los Estados hagan responsables a los intermediarios por los contenidos que alojan de terceros, justificando esta intervención de muy diversas formas, entre otras, difamación. El informe llama la atención sobre las restricciones extralegales que se desarrollan en algunos Estados cuando presionan a "redes sociales y otras empresas que alojan contenido generado por usuario para monitorear y retirar contenido por su propia iniciativa, en lugar de esperar requerimientos con base legal".

La preocupación relacionada con hacer o no responsables a los intermediarios de las actuaciones de los usuarios es una constante para los organismos internacionales. En la Declaración Conjunta sobre Libertad de Expresión e Internet se afirma que

(...) no se debe exigir a los intermediarios controlar el contenido generado por usuarios, y (debe reconocerse) la necesidad de protegerlos respecto de cualquier responsabilidad siempre que no intervengan específicamente en los contenidos ni se nieguen a cumplir una orden judicial que exija su eliminación.³⁴

En el eje de la discusión está que los servicios que proveen los intermediarios pueden ser usados tanto para actividades totalmente legales como para otras tipificadas en las legislaciones nacionales como ilegales (tales como actividades de terrorismo, abuso sexual contra menores, fraude, piratería y un largo etcétera). Por tanto, no hay duda de que existe una importante tensión para convertirlos en actores de control en el cumplimiento de las

³³ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 mayo 2016. párr. 45.

³⁴ Declaración conjunta sobre libertad de expresión e Internet. 1 de junio de 2011, Considerando No. 4. Recuperado en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2> y <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2>.



TIC Y DERECHOS HUMANOS

normas respecto de las personas que los usan. Por el papel que pueden jugar en ese control, durante las últimas décadas se ha discutido hasta dónde y cómo estos intermediarios son responsables de las acciones de los usuarios.

Como se vio en la unidad 1 el intermediario es un actor privilegiado para interferir en los contenidos y, en general, en la información que circula por Internet. Es por ello por lo que buena parte del debate sobre la circulación de contenidos indeseables, ilegales o su uso indebido o ilegal busca llevar al intermediario a una posición de “guardián” de la actividad de los usuarios.

Para hacer frente a esta discusión se habla de la necesidad de exonerar a los intermediarios de responsabilidad. Con ese fin los organismos internacionales han desarrollado la regla que se ha denominado “principio de mera transmisión”, que fue desarrollada en la Declaración Conjunta así:

- Ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, siempre que no intervenga específicamente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo (“principio de mera transmisión”).
- Debe considerarse la posibilidad de proteger completamente a otros intermediarios, incluidos los mencionados en el preámbulo, respecto de cualquier responsabilidad por los contenidos generados por terceros en las mismas condiciones establecidas en el párrafo 2(a). Como mínimo, no debería exigirse a los intermediarios que controlen el contenido generado por usuarios y no deberían estar sujetos a normas extrajudiciales sobre cancelación de contenidos que no ofrezcan suficiente protección para la libertad de expresión (como sucede con muchas de las normas sobre “notificación y retirada” que se aplican actualmente).

En Colombia no hay disposiciones legales para la inmunidad de los intermediarios, excepto para contenidos sobre abuso sexual con menores. Colombia no ha regulado el tema, generando un vacío que hasta ahora vienen llenando los jueces.

La jurisprudencia colombiana en esta materia ha sido sustancialmente consistente. Recoge lo dispuesto en la Declaración Conjunta para concluir que el responsable del contenido es su generador y que el intermediario



TIC Y DERECHOS HUMANOS

debe ser beneficiario de una suerte de inmunidad, que es lo que garantiza el ejercicio de derechos fundamentales por parte de las personas usuarias de sus servicios, siempre que cumpla con unas condiciones. Eso sucedió en la decisión T-040 de 2013 y en la sentencia T-277 de 2015.

En la sentencia T-277 de 2015, por ejemplo, en relación con Google, la corte acogió la Declaración Conjunta sobre libertad de expresión e Internet y reconoció:

(...) que se propende por dotar a los intermediarios de Internet de cierta inmunidad, de tal forma que no se les haga responsables por los contenidos y actividades que los usuarios del sistema desarrollan. Lo anterior se explica porque atribuir responsabilidad a quienes prestan estos servicios, por lo general actores privados, podría afectar la neutralidad de Internet y sus principios de no discriminación y acceso en condiciones de igualdad, al convertir a los intermediarios en censores que controlarían el contenido y tipo de información que comparten los usuarios.³⁵

La jurisprudencia de la Corte Constitucional había sido consistente en este tema de la responsabilidad de los intermediarios. Hasta 2017 la Corte había recogido los estándares internacionales de derechos humanos que se vienen construyendo en esta materia para concluir que --siempre que se cumpla con unas condiciones-- el responsable del contenido es su generador, tanto en la sentencia T-040 de 2013 como en la T277 de 2015 recogió lo dicho en la Declaración Conjunta para afirmar que el intermediario debe ser beneficiario de una suerte de inmunidad que es lo que garantiza el ejercicio de derechos fundamentales por parte de las personas usuarias de sus servicios. Sin embargo, en la reciente sentencia T-063A de 2017 la Corte se separó de esta jurisprudencia al sugerir que no aplica la exoneración de responsabilidad a Google pues en el caso en concreto no actúa como motor de búsqueda. Esta sentencia fue anulada por la misma Corte.

En la sentencia T-063A de 2017, la Corte ordenó a Google retirar un blog de su plataforma Blogger en reacción con una denuncia por "honra y buen nombre" que interpuso el dueño de una empresa de muebles. En el blog su autor anónimo acusaba a la empresa de estafar a sus clientes. Google manifestó que, dado que el contenido del blog no es inapropiado ni abiertamente ilegal no podía bloquear el blog mientras no

35 Declaración conjunta sobre libertad de expresión e Internet. 1 de junio de 2011, Considerando No. 2. Recuperado en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2>.



tuviera una orden judicial. El juez de primera instancia le dio la razón a Google. Posteriormente la Corte Constitucional seleccionó la decisión y la modificó ordenando el bloqueo del blog y otras obligaciones negativas para el ejercicio de derechos humanos, en perspectiva de los estándares internacionales señalados.

La Corte citó la Declaración conjunta en lo que corresponde, pero parcialmente, pues se limitó al párrafo que la jurisprudencia de 2013 y 2015 ya había recogido y que efectivamente solo menciona a los motores de búsqueda. La Corte no aplicó el párrafo 2(b) de la Declaración Conjunta que expresamente extiende la inmunidad a otros intermediarios al indicar que

"Debe considerarse la posibilidad de proteger completamente a otros intermediarios, incluidos los mencionados en el preámbulo, respecto de cualquier responsabilidad por los contenidos generados por terceros en las mismas condiciones establecidas en el párrafo 2(a). Como mínimo, no se debería exigir a los intermediarios que controlen el contenido generado por usuarios y no deberían estar sujetos a normas extrajudiciales sobre cancelación de contenidos que no ofrezcan suficiente protección para la libertad de expresión (como sucede con muchas de las normas sobre "notificación y retirada" que se aplican actualmente)." ³⁶

En el auto 285 de 2018, la Corte anuló la sentencia T-063A de 2017 por vulneración al debido proceso por omisión en el análisis de asuntos de relevancia constitucional. En particular, la Corte consideró que la orden impuesta a Google de verificar blogs anónimos que resulten injuriantes o agraviantes es de imposible cumplimiento porque no hay una regla única para definir qué puede calificarse de esta forma. Así, la orden de filtrado de contenidos por parte de un intermediario no responde a un análisis del alcance de los derechos a la libertad de expresión y pensamiento. Así mismo, la Corte consideró que la distribución del contenido no es principalmente responsabilidad del intermediario aunque a él se haya dirigido exclusivamente la orden. Finalmente, revisó la orden en relación con la inscripción en el registro TIC y el consiguiente monitoreo de sus actividades por parte del Ministerio de las TIC. Concluyó respecto a esa orden que esta obligación de la Ley 1341 de 2009 sólo aplica para los proveedores de redes y de servicios de telecomunicaciones.³⁷

³⁶ Declaración conjunta sobre libertad de expresión e Internet. 1 de junio de 2011, Párrafo 2b. Recuperado en <http://www.oas.org/es/cidh/expresion/showarticle.asp?partID=849&IID=2>

³⁷ Corte Constitucional. Sentencia T-063A de 2017. M.P. Jorge Iván Palacio Palacio y Auto 285 de 2018. Recuperado de: <http://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm>



Durante los últimos años una preocupación especial y recurrente ha sido la de regular internet con la idea de evitar los efectos nocivos que están evidenciándose por los abusos de los contenidos generados por usuarios en Internet. Se evidencia una tensión entre la libertad de expresión y otros derechos. Se invoca la protección de los menores de edad, de la propiedad intelectual, de los derechos al buen nombre e imagen o evitar el terrorismo, como las justificaciones para tener mecanismos más activos y efectivos en el control de los contenidos que circulan por internet.

La necesidad de encontrar mecanismos que puedan evitar estos abusos y proteger derechos en redes sociales exige una reflexión importante sobre cómo traer al entorno digital las garantías que existen fuera de línea y resaltar la protección reforzada que tiene la libertad de expresión. En este proceso el informe del Relator de la ONU para la libertad de expresión de 2018³⁸ propone un marco para la moderación del contenido en línea generado por los usuarios que sitúe los derechos humanos en el centro mismo de la cuestión.

Entre otras recomendaciones de este informe vale la pena resaltar dos: "Los Estados y las organizaciones intergubernamentales deberían abstenerse de promulgar leyes o concertar acuerdos que requieran la vigilancia o el filtrado "activo" del contenido, que es incompatible con el derecho a la privacidad y puede ser equivalente a la censura previa a la publicación."³⁹

"Los Estados deberían de abstenerse de adoptar modelos de regulación en los que los organismos gubernamentales y sus normas, y no las autoridades judiciales, se erijan como árbitro"⁴⁰, sobre este tema regresaremos más adelante cuando hablamos de filtrado y bloqueo de contenidos.

2.4 Pluralismo y no discriminación en la expresión digital.

En tanto concreción del deber general del Estado de promover la máxima diversidad y pluralismo en los medios de comunicación, el Estado debe proveer garantías para que la mayor cantidad de actores puedan expresarse libremente a través de Internet. El contenido específico de este deber relacionado con pluralismo y no discriminación implica que las autoridades deban

³⁸ Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, David Kaye. A/HRC/38/35. Abril 6 de 2018. Recuperado en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.

³⁹ Ibídem. párr. 67.

⁴⁰ Ibídem. párr. 68



TIC Y DERECHOS HUMANOS

(...) asegurar que no se introduzcan en Internet cambios que tengan como consecuencia la reducción de voces y contenidos", y "proteger la naturaleza multidireccional de Internet y promover las plataformas que permitan la búsqueda y difusión de informaciones e ideas de toda índole, sin consideración de fronteras, en los términos del artículo 13 de la Convención Americana.⁴¹

Por su parte, el principio de no discriminación exige al Estado remover los obstáculos que pueden enfrentar determinados sectores de la población para acceder a Internet o expresarse a través de él. Los Relatores de la ONU y de la OEA han precisado que:

(...) en el entorno digital, la obligación de no discriminación implica, además de los deberes de acceso y pluralismo ya referidos, la adopción de medidas, a través de todos los medios apropiados, para garantizar que todas las personas —especialmente aquellas que pertenecen a grupos vulnerables o que expresan visiones críticas sobre los asuntos de interés público— puedan difundir contenidos y opiniones en igualdad de condiciones.⁴²

La Corte Constitucional colombiana en su sentencia T-277 de 2015 menciona y recoge los principios rectores para el respeto de la libertad de expresión en Internet con base en los pronunciamientos de la Relatoría de la CIDH, incluyendo pluralismo y no discriminación, así:

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) presentó una serie de principios orientadores del funcionamiento de la red, para guiar las medidas de los gobiernos en relación con esta (sic), todo ello con el fin de conservar las cualidades que han hecho de Internet un espacio propicio para que las personas compartan ideas, informaciones y opiniones. Los aducidos principios rectores son: (i) acceso en condiciones de igualdad; (ii) pluralismo; (iii) no discriminación; y (iv) privacidad].⁴³

El principio de no discriminación también se aplica a los contenidos difundidos por Internet en la medida en que no formen parte de alguna de las categorías de expresión proscritas, que no están dentro del ámbito de protección de este derecho, de allí se deriva, entre otras, el principio de neutralidad de la red que veremos en otro aparte del presente manual.

⁴¹ CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de expresión e Internet*. oea/Ser.L/V/II. CIDH/rele/inf.11/13. 31 de diciembre de 2013. párr. 19. Disponible en: <http://bit.ly/1WHR6cD>.

⁴² Ibídем. párr. 21.

⁴³ Corte Constitucional, Sentencia T-277 de 2015. M.P. María Victoria Calle Correa.



2.5 Limitaciones legislativas y prohibición de la censura previa.

Toda limitación del flujo comunicacional de Internet, al ser directa y evidentemente una limitación de la libertad de expresión, debe cumplir con los requisitos del artículo 13.2 de la Convención Americana de Derechos Humanos.

No obstante, es necesario considerar que la libertad de expresión protegida por el artículo 13.2 de la Carta varía en su aplicación dependiendo del contexto, y en el contexto de Internet existen algunas especificidades que deben ser tenidas en cuenta por quienes examinan la licitud de una determinada limitación a la libertad de expresión digital.

En igual sentido, el Comité de Derechos Humanos de Naciones Unidas en su Observación General No. 34 indicó que:

Toda limitación al funcionamiento de los sitios web, los blogs u otros sistemas de difusión de información en Internet, electrónicos o similares, incluidos los sistemas de apoyo a estas comunicaciones, como los proveedores de servicios de Internet o los motores de búsqueda, solo serán admisibles en la medida en que sean compatibles con el párrafo 3. Las restricciones permisibles se deben referir en general a un contenido concreto; las prohibiciones genéricas del funcionamiento de ciertos sitios y sistemas no son compatibles con el párrafo 3. Tampoco es compatible con el párrafo 3 prohibir que un sitio o un sistema de difusión de la información publique material por el mero hecho de que ese material pueda contener críticas al gobierno o al sistema político al que este se adhiere.^{44 45}

Traemos a colación este párrafo con la idea de mencionar el tema del marco legislativo aplicable, mientras que, en relación con filtrado y bloqueo de contenidos, será un tema para tratar en otro capítulo.

2.5.1 Previsión legal clara y expresa

Toda limitación de la libertad de expresión en Internet debe haber sido prevista con anticipación en una ley redactada de manera clara y precisa, que no dé lugar a ambigüedades ni a márgenes interpretativos sobre las potestades de intervención de la autoridad.

⁴⁴ *Observaciones finales sobre la República Árabe Siria (ccpr/CO/84/SYR). Disponible en: http://bit.ly/2pLjmxv http://bit.ly/2pLjmxv http://bit.ly/2pLjmxv*

⁴⁵ Naciones Unidas. Comité de Derechos Humanos. *Observación General No. 34 - «Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos: Libertad de opinión y libertad de expresión».* Aprobada en el 102º período de sesiones, 11 a 29 de julio de 2011. ccpr/c/gc/34. pár. 43. Disponible en: <http://bit.ly/1nmREgm> <http://bit.ly/1nmREgm> <http://bit.ly/1nmREgm>



En el ámbito digital, las leyes vagas y ambiguas pueden tener un efecto sistémico silenciador, al “impactar especialmente en este universo creciente de personas, cuya incorporación al debate público es una de las principales ventajas que ofrece Internet como espacio de comunicación global”.⁴⁶

2.5.2 Objetivos legítimos imperiosos a la luz de la Convención Americana

Solo pueden introducirse limitaciones a las comunicaciones por Internet cuando ello sea necesario para el logro de alguno de los objetivos legítimos previstos expresamente en el artículo 13.2 de la Convención Americana, y ello interpretando su alcance de conformidad con la jurisprudencia del sistema, y no en forma amplia.

Así, la CIDH ha ejemplificado esta regla explicando que:

(...) la protección de la seguridad nacional puede ser invocada para imponer restricciones al derecho a la libertad de expresión. No obstante, [...] no debe fundarse en una idea de seguridad nacional incompatible con una sociedad democrática. No tendría entonces una finalidad legítima un programa de vigilancia que, pese a invocar la defensa de la seguridad nacional, intercepte, capture o utilice información privada de disidentes, periodistas o defensores de derechos humanos con finalidades políticas o para evitar o comprometer sus investigaciones o denuncias.⁴⁷

2.5.3 Test de necesidad, proporcionalidad e idoneidad de la medida

Al evaluar la necesidad, proporcionalidad e idoneidad de las limitaciones a Internet para el logro de los objetivos imperiosos invocados, se debe asumir una perspectiva sistémica de valoración enfocada no solo en los derechos de los emisores y los efectos que la limitación tendrá sobre sus expresiones, sino particularmente sobre los impactos que, en virtud del diseño mismo de Internet, tendrá la limitación sobre el sistema como un todo. Dado que las limitaciones a la libertad de expresión por Internet afectan no solamente a quien se expresa, sino a toda la red, la potencialidad de generar un efecto sistémico de inhibición, o de otro tipo, debe ser evaluada de forma especializada y expresa al momento de considerar la proporcionalidad de la medida de limitación propuesta.

⁴⁶ CIDH. *Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet.* oea/Ser.L/V/II. CIDH/rele/inf.11/13. 31 de diciembre de 2013. párr. 58. Disponible en: <http://bit.ly/1WHR6cD>

⁴⁷ *Ibid.*, párr. 60.



TIC Y DERECHOS HUMANOS

Asimismo, al evaluar la necesidad de la medida de limitación y valorar, en consecuencia, si existen alternativas menos restrictivas para lograr el mismo objetivo, debe tenerse en cuenta que la red ofrece posibilidades mucho más amplias para ejercer el derecho a la rectificación, por lo cual “la imposición de una responsabilidad ulterior que podría resultar legítima y proporcional en un contexto tradicional, podría no serlo cuando se produce en línea”.⁴⁸

Por otra parte, en virtud de las características propias de las páginas web, ha de evaluarse al determinar la necesidad y proporcionalidad de una medida de limitación, si es necesario afectar todo el contenido de la página, o solo una parte.

2.5.4 Jurisdicción

Dada la naturaleza transnacional de Internet, su regulación plantea problemas jurídicos atinentes a la jurisdicción de los Estados para regularlo o imponer otro tipo de limitaciones. Desde la perspectiva de la maximización de la comunicación virtual, la Relatoría de la OEA ha interpretado este asunto en forma tal que únicamente los Estados con el vínculo jurisdiccional más cercano a una determinada expresión por Internet puedan ejercer sus potestades soberanas sobre la misma. En palabras de la CIDH,

(...) con la finalidad de evitar la existencia de barreras indirectas que desincentiven o directamente limiten de manera desproporcionada el ejercicio del derecho a la libertad de expresión en Internet, la competencia (jurisdicción) respecto de causas vinculadas con expresiones en Internet debería corresponder exclusivamente a los Estados con los que tales causas presenten los contactos más estrechos, normalmente debido a que el autor reside en ese Estado, la expresión se publicó desde allí o este se dirige específicamente al público ubicado en el Estado en cuestión (ONU, OSCE, OEA y CADHP, 2011, punto 4 a).

Estos asuntos jurisdiccionales también se predicen del ejercicio del poder judicial del Estado y, en consecuencia, de la jurisdicción competente para conocer de potenciales demandas judiciales por parte de personas que aleguen una afectación desproporcionada de sus derechos como resultado de una expresión en Internet: “Los particulares solo deberían poder iniciar acciones judiciales en una jurisdicción en la que puedan demostrar

⁴⁸ *Ibid.*, párr. 71; UN. Informe Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión. A/HRC/17/27 (16 mayo de 2011), párr. 27.



haber sufrido un perjuicio sustancial, de manera que se prevenga lo que se conoce como ‘turismo de la difamación’ (forum shopping)» (ONU, OSCE, OEA y CADHP, 2011, punto 4 a).⁴⁹ En efecto, podría generarse una limitación indirecta de la libertad de expresión por Internet si se crea un «mercado judicial» en el que las personas pueden iniciar indefinidamente procesos judiciales en todos los países en los que se puede consultar una determinada expresión transmitida por Internet. Para evitar este riesgo, la CIDH ha llamado a los Estados adoptar

(...) reglas jurisdiccionales compatibles con la noción de publicación única que previene tanto el efecto indeseable de la selección deliberada de una jurisdicción [...] como el doble juzgamiento por una misma causa [...]. En el caso de contenidos similares, publicados con el mismo formato y en el mismo lugar, los plazos para la interposición de acciones judiciales deberían contarse a partir de la primera vez que fueron publicados. Asimismo, solo debería permitirse que se presentara una única acción por daños respecto de tales contenidos y, cuando corresponda, se debería permitir una única reparación por los daños sufridos en todas las jurisdicciones (regla de la publicación única).⁵⁰

En su informe de 2018, el relator para libertad de expresión de la ONU, puso la lupa también sobre el rol de los gobiernos que intentan controlar en entorno en que las empresas moderan contenidos y, también, el papel de los términos y condiciones de uso de las empresas.

El relator llama la atención sobre cómo es cada vez más frecuente que los Estados “expidan leyes restrictivas con una redacción de carácter muy general sobre el “extremismo”, la blasfemia, la difamación, el discurso “ofensivo” las “noticias falsas” y la “propaganda” suelen servir como pretexto para exigir que las empresas supriman la expresión legítima”⁵¹, e indica que si bien es frecuente que estas regulaciones tengan jurisdicción nacional algunos Estados exigen que la eliminación sea extraterritorial lo que genera lógicas de censura más allá de las fronteras. Adicionalmente, el relator resaltó en este informe que cuando se presentan controles derivados de las condiciones de servicios de las empresas la restricción se aplica a nivel mundial⁵².

49

Ibid.

50

Ibid., párrs. 67, 68.

51

Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, David Kaye. A/HRC/38/35. Abril 6 de 2018. Recuperado en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35. Párr. 14 y siguientes.

52

Ibid. párr. 19.



2.5.5 Debido proceso y control judicial

En cualquier caso, las medidas de limitación de la expresión por Internet deben ser completamente transparentes, adoptadas de conformidad con el procedimiento legal aplicable y sujetas a control tanto administrativo –por organismos autónomos, independientes e idóneos– como judicial. En palabras de la CIDH, “en todo caso las medidas restrictivas deben ser transparentes y estar sometidas a rigurosos controles de órganos autónomos y especializados de manera tal que tengan la capacidad técnica y las garantías suficientes para resguardar posibles amenazas estructurales respecto de Internet o de la integridad de las comunicaciones”.⁵³

2.5.6 Prohibición de censura previa

El artículo 20 de la Constitución Política de 1991 dispone que:

Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

En Colombia, por tanto, para garantizar el respeto por la libertad de expresión no hay cabida a la censura previa. El artículo 20 se encuentra, en este sentido, en consonancia con el artículo 13.2 de la Convención Americana, que tan solo consagra una excepción (numeral 4) que busca la protección moral de la infancia y la adolescencia. Por tanto, la ley que establezca una limitación a la libertad de expresión solo podrá hacerlo en la forma de responsabilidades ulteriores.

Ya en 2011 los Relatores para la Libertad de Expresión de la Organización de Estados Americanos (OEA), la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana han expresado que: “En ningún caso se puede imponer una medida ex-ante que impida la circulación de cualquier contenido que tenga presunción de cobertura”.⁵⁴ Y, en concreto, agregan que “Los sistemas de filtrado de contenidos impuestos por gobiernos o proveedores de servicios comerciales que no sean controlados por el usuario final constituyen una forma de censura previa y no representan una restricción justificada a la libertad de expresión”.

⁵³ *Ibid.*, párr. 71; UN. Informe Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión. A/HRC/17/27 (16 mayo de 2011), párr. 56.

⁵⁴ *El Relator Especial para la Libertad de Opinión y de Expresión de Naciones Unidas (ONU), la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial para la Libertad de Expresión de la Organización de Estados Americanos (OEA) y la Relatora Especial para la 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, párrafo 88. Disponible en <http://bit.ly/1eX83sn> <http://bit.ly/1eX83sn>*



Este riesgo y sus efectos para la libertad de expresión se alertan una vez más en 2018⁵⁵ en el informe del relator para la Libertad de Expresión de la ONU, que reacciona a una nueva tendencia regulatoria que avanza en la Unión Europea donde los Estados están imponiendo a las empresas intermediarias de internet para que empleen mecanismos de automatización para controlar contenidos de usuarios incluso antes de que sean publicados, es decir, institucionalizando un mecanismo de censura previa desproporcionada que empieza con la protección de la propiedad intelectual pero se está extendiendo a otros temas como el terrorismo. El relator afirma:

"La exigencia de la eliminación de contenido de forma rápida y automática lleva consigo el riesgo de que aparezcan nuevas formas de censura previa que ya amenazan los esfuerzos creativos en el contexto de los derechos de autor. Las cuestiones complejas de hecho y de derecho deberían ser resueltas por las instituciones públicas, no por agentes privados cuyos procedimientos actuales tal vez no sean compatibles con las normas relativas a las debidas garantías procesales y cuya motivación es principalmente económica."⁵⁶

2.6. Anonimato

El anonimato es instrumental al ejercicio de la libertad de expresión. El anonimato sirve de apoyo para una verdadera participación ciudadana y para facilitar el debate político. La relatora especial para libertad de expresión de la CIDH en 2013, Catalina Botero, retomó las palabras del ex-relator de la ONU ese mismo año para afirmar:

En virtud de esta relación estrecha entre libertad de expresión y privacidad, los Estados deben evitar la implementación de cualquier medida que restrinja, de manera arbitraria o abusiva, la privacidad de los individuos (artículo 11 de la Convención Americana), entendida en sentido amplio como todo espacio de intimidad y anonimato, libre de amedrentamiento y de represalias, y necesario para que un individuo pueda formarse libremente una opinión y expresar sus ideas así como buscar y recibir información, sin ser forzado a identificarse o a revelar sus creencias y convicciones o las fuentes que consulta.⁵⁷

55 Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, David Kaye. A/HRC/38/35. Abril 6 de 2018. Recuperado en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35. Párr. 32 y siguientes.

56 Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, David Kaye. A/HRC/38/35. Abril 6 de 2018. Recuperado en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35. Párr. 17.

57 OEA, "Libertad de expresión e Internet", Catalina Botero, 31 diciembre de 2013, párr. 132. Recuperado en [http://www.oas.org/es/CIDH/expresion/docs/informes/2014_04_08_Internet_web.pdf](http://www.oas.org/es/CIDH/expresion/docs/informes/2014_04_08_internet_web.php)



En el texto del relator de la ONU se elogiaba como una de las características que ofrecía importantes beneficios y posibilidades en Internet al anonimato. En dicho documento también se reconocía que generaba temor entre los gobiernos y los poderosos que han reaccionado aumentando las restricciones a Internet.⁵⁸

En 2015 el nuevo relator para la libertad de expresión de la ONU, David Kaye, se refería al anonimato y al cifrado en el entorno tecnológico como garantes de la libertad de expresión:

(...) el cifrado y el anonimato, y los conceptos de seguridad detrás de estos temas, proveen la privacidad y seguridad necesarias para el ejercicio del derecho a la libertad de expresión en la era digital. Esta seguridad puede ser esencial para el ejercicio de otros derechos incluyendo los derechos económicos, la intimidad, el debido proceso, la libertad de reunión y asociación y el derecho a la vida y a la integridad personal. Por su importancia para los derechos a la opinión y a la libertad de expresión, las restricciones al cifrado y al anonimato deben ser estrictamente limitadas de acuerdo con los principios de legalidad, necesidad, proporcionalidad y legitimidad en el objetivo.⁵⁹

Para la ONU una de las tensiones actuales en Internet tiene que ver con la forma como los Estados afectan la seguridad y la privacidad en línea especialmente justificados por amenazas terroristas. Entre las preocupaciones que se identifican en esta tensión la ONU habla de la prohibición del anonimato en línea como una forma de interferir con el derecho a la libertad de expresión.⁶⁰

Con el fin de exemplificar los problemas que se están presentando, concretamente el Relator de la ONU en su informe menciona prohibiciones al anonimato en línea que interfieren en el derecho a la libertad de expresión, como las prohibiciones constitucionales al anonimato que se encuentran en Brasil y Venezuela, el registro obligatorio de quienes usan computadores en cibercafés de Irán, o el registro celular colombiano que existe desde 2011.⁶¹ También menciona cómo en Rusia se exige a los blogueros que tienen más de 3000 lectores que se registren como medios

⁵⁸ Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, Frank La Rue. A/HRC/17/27. Mayo 16 de 2011, Párr. 82. Recuperado en <http://www.acnur.org/t3/fileadmin/Documentos/BDL/2015/10048.pdf?view=1>.

⁵⁹ Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Párr. 56. Recuperado en <http://www.globalmediapolicy.net/node/15836> <http://www.globalmediapolicy.net/node/15836> <http://www.globalmediapolicy.net/node/15836>

⁶⁰ Ibid. Párr. 49.

⁶¹ Castañeda, J.D. "Un rastreador en tu bolsillo" (2017). Fundación Karisma. Disponible en: <https://nomascelusvigilados.karisma.org.co/> <https://nomascelusvigilados.karisma.org.co/>



ante la autoridad, que se identifiquen públicamente y a los usuarios de cibercafés se les exige identificarse para acceder a la conexión WiFi. Para el relator estos y otros son ejemplos de políticas que afectan directamente el anonimato, especialmente entre quienes acceden a Internet solo mediante tecnologías móviles⁶² y van en contravía de la obligación del Estado que es precisamente la de proteger y promover el respeto por las herramientas que permiten el ejercicio de los derechos humanos.

Ahora bien, esto no significa que toda información esté protegida por el anonimato. En palabras de la relatoría especial de la OEA en su informe de 2013:

135. Ello no significa, sin embargo, que el anonimato resguarde a cualquier tipo de información. Por ejemplo, el anonimato del emisor de ninguna manera protegería a quien difunda pornografía infantil, a quien hiciera propaganda a favor de la guerra o apología del odio que constituya incitación a la violencia o incitare pública y directamente al genocidio 180. Estos discursos no están protegidos por la Convención Americana y el anonimato no puede resguardar a los emisores de las consecuencias jurídicas que cada ordenamiento interno establezca—de conformidad con el derecho internacional de los derechos humanos—respecto de cada uno de esos casos. Lo mismo ocurriría en el caso de que el ejercicio del derecho a la libertad de pensamiento y expresión fuera objeto de responsabilidades ulteriores del tipo que autoriza la Convención Americana. En todos esos casos, las autoridades judiciales estarían autorizadas para tomar medidas razonables tendientes a descubrir la identidad del emisor de conductas prohibidas para aplicar la respuesta proporcionada que prevé el ordenamiento jurídico.⁶³

Ap

En grupos de 3 a 5 personas vean el video de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos sobre el informe de 2013 "Libertad de expresión e Internet". Se encuentra en <https://youtu.be/YaTvcMCrcNg> <https://www.youtube.com/watch?v=GxseK7d4lys>.

⁶² Naciones Unidas. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión*, David Kaye. A/HRC/29/32. Mayo 22 de 2015. párr. 49.

⁶³ CIDH, *Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet*. OEA/Ser.L/V/II. CIDH/RELE/INF.11/13, 31 de diciembre de 2013, párr. 66. *Ibid.*, párrs. 84-85.



Ae

Autoevaluación

Caso Gloria vs. Google (Colombia)

Tomando como base la sentencia T-277 de 2015 de la Corte Constitucional:

- Responda ¿qué importancia le da la Corte a Internet como un espacio de ejercicio de derechos?
- Establezca si y, de ser el caso, cómo la Corte acoge la inmunidad de los intermediarios de Internet.
- Reflexione sobre la obligación de actualización que la Corte impone a los medios de comunicación y sobre la decisión que adopta en materia de jurisdicción respecto a Google.

J

Jurisprudencia

Corte Constitucional, Sentencia T-403 de 1992. M.P. Eduardo Cifuentes Muñoz

Corte Constitucional. Sentencia T- 260 de 2012. M.P. Humberto Antonio Sierra Porto.

Corte Constitucional. Sentencia T-040 de 2013. M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional. Sentencia C-634 de 2013. M.P. María Victoria Calle Correa.

Corte Constitucional. Sentencia T-277 de 2015. M.P. María Victoria Calle Correa.

Corte Constitucional. Sentencia T-357 de 2015. M.P. Gabriel Eduardo Mendoza Martelo.

Corte Constitucional. Sentencia T-050 de 2016. M.P. Gabriel Eduardo Mendoza Martelo.

Corte Constitucional, Sentencia T-063A de 2017. MP. Jorge Iván Palacio Palacio. Salvamento de Voto de Aquiles Arrieta Gómez.

Tribunal Superior de Distrito Judicial de Cali. Sentencia del 17 de febrero de 2014.



B

- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. Documento oea/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Disponible en: <http://bit.ly/1WHR6cD>
- Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 22 de mayo de 2015. Documento ONU A/HRC/29/32, Cifrado y anonimato en las comunicaciones digitales. Disponible en: <http://bit.ly/2pa0zYu>
- 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. Disponible en <http://on.unesco.org/2qwfUaS>
- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 2014. Disponible en <http://bit.ly/1qR7bYf>
- Universidad de los Andes, Dejusticia y Open Society Foundation. Nuevos Desafíos: Libertad de en Internet. Unesco. Caja de herramientas para escuelas judiciales iberoamericanas. Formación de formadores en libertad de expresión, acceso a la información pública y seguridad de periodistas. Edición Marine González, 2017. Disponible en <http://unesdoc.unesco.org/images/0025/002515/251593S.pdf>
- Comisión Interamericana de Derechos Humanos (CIDH). Relatoría Especial para la Libertad de Expresión. Video: “Libertad de expresión e Internet”. 17 de junio de 2014. Disponible en <https://www.youtube.com/watch?v=YaTvcMCrcNg>.
- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Párr. 56. Recuperado en <http://www.globalmediapolicy.net/node/15836>



Unidad 3: INTIMIDAD EN LA ERA DIGITAL

Og

Estudiar y analizar las especificidades y la forma como se debe expresar la protección y garantías del derecho a la intimidad en el contexto tecnológico a la luz de los estándares internacionales de derechos humanos y en el contexto del marco jurídico colombiano.

Oe

- Identificar estándares internacionales y precedentes jurisprudenciales que le permitirán resolver de forma sustentada problemas referentes a interceptación de comunicaciones, retención de datos y casos de violencia en Internet.
- Resolver de forma sustentada problemas referentes a interceptación de comunicaciones, retención de datos y casos de violencia en Internet, aplicando los principios y valores constitucionales en armonía con los estándares internacionales y precedentes jurisprudenciales.
- Sensibilizarse sobre los riesgos a los derechos humanos derivados, por una parte, de la gran cantidad de datos que produce cada persona y de la necesidad de su debido resguardo jurídico frente a injerencias o usos indebidos por parte tanto de los poderes públicos como de los privados.

MAPA CONCEPTUAL

Unidad 3: Intimidad en la era digital

3.1 Vigilancia e interpretación de las comunicaciones

3.2 Retención de datos

3.3 Explotación de datos



3.1 Actividades previas

Se recomienda hacer un repaso sobre el tema en general antes de comenzar la lectura de este módulo, que aplica esos parámetros generales a Internet. Es importante resaltar que existe una relación estrecha entre la libertad de expresión y la intimidad, lo que permitió que buena parte del desarrollo del concepto de intimidad y sus características se produjera durante los últimos años a partir de las relatorías de Libertad de Expresión.

Las lecturas sugeridas en relación con intimidad en su conexión con Internet son las siguientes:

- Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 17 de abril de 2013. Documento A/HRC/23/40. Disponible en <http://undocs.org/es/A/HRC/23/40>
- Naciones Unidas. Asamblea General. El Derecho a la privacidad en la era digital. Documento A/RES/68/167. Resolución aprobada el 18 de diciembre de 2013. Disponible en <http://undocs.org/es/A/RES/68/167> <http://undocs.org/es/A/RES/68/167> <http://undocs.org/es/A/RES/68/167> <http://undocs.org/es/A/RES/68/167>
- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. Documento OEA/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Disponible en: <http://bit.ly/1WHR6cD> o en [CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e internet. Documento OEA/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Disponible en: http://bit.ly/1WHR6cD o en http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf](http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf).
- Naciones Unidas. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). El derecho a la privacidad en la era digital. A/HRC/27/37, parr. 19.



TIC Y DERECHOS HUMANOS

- Tribunal de Justicia de la Unión Europea, sentencia en los asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Seitlinger y otros, sentencia de 8 de abril de 2014, párrs. 26, 27 y 37, disponible en <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN>.
- Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 22 de mayo de 2015. Documento ONU A/HRC/29/32, Cifrado y anonimato en las comunicaciones digitales. Disponible en: <http://bit.ly/2pa0zYu>
- 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. Disponible en <http://on.unesco.org/2qwfUaS> <http://on.unesco.org/2qwfUaS>
- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 2014. Disponible en <http://bit.ly/1qR7bYf> <http://bit.ly/1qR7bYf>.
- Universidad de los Andes, Dejusticia y Open Society Foundations. Nuevos Desafíos: Libertad de Internet. Unesco. Cajadeherramientas para escuelas judiciales iberoamericanas. Formación de formadores en libertad de expresión, acceso a la información pública y seguridad de periodistas. Edición Marine González, 2017. Disponible en <http://unesdoc.unesco.org/images/0025/002515/251593S.pdf> <http://unesdoc.unesco.org/images/0025/002515/251593S.pdf>.
- Comisión Interamericana de Derechos Humanos (CIDH). Relatoría Especial para la Libertad de Expresión. Video: "Libertad de expresión e Internet". 17 de junio de 2014. Disponible en <https://www.youtube.com/watch?v=YaTvcMCrcNg>. <https://www.youtube.com/watch?v=YaTvcMCrcNg>.
- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Párr. 56. Recuperado en <http://www.globalmediapolicy.net/node/15836> <http://www.globalmediapolicy.net/node/15836>.
- "El Derecho a la Libertad de Expresión. Curso Avanzado para Jueces y Operadores Jurídicos en las Américas". Propuesta curricular y materiales de estudio. Elaborado por Catalina Botero, Federico



Guzmán, Sofía Jaramillo y Salomé Gómez para DeJusticia con el apoyo de Open Society Foundations (osf). 2017, Disponible en: <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf> <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf>

3.2 La vigilancia e interceptación de las comunicaciones.

Frente a la obligación de los Estados de proteger el derecho a la intimidad o a la vida privada (art. 11, Convención Interamericana sobre Derechos Humanos) está el reto reconocido que supone el vertiginoso avance de las tecnologías disponibles para captar y monitorear comunicaciones privadas. Las diferentes relatorías de libertad de expresión de los organismos internacionales han constatado que

Internet ha creado oportunidades sin precedentes para la libertad de expresión, comunicación, búsqueda, posesión e intercambio de información. Con ello, se ha facilitado también la captura, almacenamiento y administración de enormes cantidades de datos y de información que puede resultar altamente reveladora, incluso de los aspectos más íntimos de la vida privada de las personas. En este sentido, como ya lo han manifestado las relatorías, resulta preocupante que los marcos jurídicos que regulan los programas de vigilancia de las comunicaciones no se hayan adecuado a los desarrollos de las nuevas tecnologías en la era digital y que se hubieren trasladado criterios análogos sobre vigilancia que resultan obsoletos para aplicarse equitativamente al entorno digital.⁶⁴

En Colombia, la Constitución establece en el artículo 15 que:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

(...)

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

⁶⁴ CIDH. Relatoria Especial para la Libertad de Expresión. *Libertad de expresión e Internet*. Documento OEA/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Párr. 137 Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf.



TIC Y DERECHOS HUMANOS

En el mismo sentido, el artículo 14 del Código de Procedimiento Penal (CPP) dispone:

Toda persona tiene derecho al respeto de su intimidad. Nadie podrá ser molestado en su vida privada.

No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este código. Se entienden excluidas las situaciones de flagrancia y demás contempladas por la ley.

De la misma manera deberá procederse cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones.

El derecho a la intimidad tiene profundas relaciones con otros derechos. Así, la Corte Constitucional ha reconocido que

(...) el fundamento último de la Constitución de 1991 es la dignidad de la persona, una de cuyas principales premisas es el desarrollo de la personalidad, el cual a su vez tiene como supuesto la intimidad.⁶⁵

Esto no significa que estamos frente a un derecho absoluto. El derecho a la intimidad puede ser objeto de restricciones o limitaciones en determinadas circunstancias excepcionales.

La vigilancia estatal de las comunicaciones busca recaudar datos para la investigación de inteligencia o criminal. En ese proceso, recolectan, almacenan, procesan y circulan datos usando diferentes técnicas. Las técnicas más comunes son la interceptación de comunicaciones, la retención de datos y el uso de herramientas de hackeo (p. Ej. pruebas de penetración y explotación de vulnerabilidades de seguridad).

El Relator especial de las Naciones Unidas para la libertad de expresión en 2013 analizó las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos a la intimidad y a la libertad de expresión.⁶⁶ En dicho informe se abordaban las modalidades más

65

Corte Constitucional. *Sentencia T-011 de 1992. M. P. Alejandro Martínez Caballero.*

66

Naciones Unidas. *Informe del Relator Especial para la promoción y protección de la libertad de expresión, 17 de abril de 2013. Documento A/HRC/23/40.* Disponible en: <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40>



TIC Y DERECHOS HUMANOS

comunes de vigilancia a las comunicaciones, pero se hacía también un llamado a mantener en constante revisión la forma como evolucionaban estas tecnologías y prácticas.

La CIDH es clara al afirmar que es obligación de los estados:

de una parte, abstenerse de hacer intromisiones arbitrarias en la órbita del individuo, su información personal y sus comunicaciones y, de otra parte, deben garantizar que otros actores se abstengan de realizar tales conductas abusivas.⁶⁷

De hecho, en diciembre de 2013 la Asamblea General de las Naciones Unidas por consenso adoptó la Resolución “El derecho a la privacidad en la era digital” donde se exhorta a los Estados a que:

- a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales;
- b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos;
- c) Examen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos;
- d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado;⁶⁸

De manera expresa, en los diferentes documentos que tratan sobre el tema, los organismos internacionales de derechos humanos se han pronunciado para indicar que es legítima la interferencia del Estado en

67 CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de expresión e Internet. Documento OEA/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Párr. 137* Disponible en:http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

68 Naciones Unidas. Asamblea General. *El Derecho a la privacidad en la era digital. Documento A/RES/68/167. Resolución aprobada el 18 de diciembre de 2013. Disponible en <http://undocs.org/es/A/RES/68/167>*



TIC Y DERECHOS HUMANOS

las comunicaciones privadas solo en casos excepcionales cuando cumpla con los requisitos de (1) legalidad, (2) objetivo imperativo, (3) necesidad, idoneidad y proporcionalidad, y (4) control judicial y debido proceso.⁶⁹

Así por ejemplo desde Naciones Unidas en 2013 se reconoció la seguridad nacional y la actividad delictiva como justificantes para el uso excepcional de tecnologías de vigilancia de las comunicaciones, pero recuerda que

La vigilancia de las comunicaciones debe considerarse un acto sumamente perturbador que podría suponer una injerencia en los derechos a la libertad de expresión y la intimidad, y que atenta contra los fundamentos de una sociedad democrática. La legislación debe estipular que la vigilancia de las comunicaciones por el Estado solo se realice en las situaciones más excepcionales y únicamente con la supervisión de una autoridad judicial independiente. La legislación debe incluir salvaguardias relativas a la naturaleza, el alcance y la duración de las posibles medidas, los motivos que se requieren para disponerlas, las autoridades competentes para autorizarlas y supervisarlas, y el tipo de reparaciones previstas en la legislación nacional.⁷⁰

En Colombia, para que la intervención en las comunicaciones privadas sea legítima, se requiere:

- a) Que exista orden judicial;
- b) Que exista una ley en la que se contemplen los casos en los cuales procede tal medida y,
- c) Que exista un procedimiento fijado en la ley para llevar a cabo dicha actuación.⁷¹

Al interpretar los requisitos mencionados, la Corte Constitucional ha sostenido que “el derecho a la comunicación se vuelve inútil cuando se pierde espontaneidad por temor a interferencias o a la exposición pública del mensaje”.⁷² De ahí la necesidad de que las intervenciones cumplan con los mencionados requisitos constitucionales.

⁶⁹ Esta clasificación la viene desarrollando la Relatoría especial de libertad de expresión de la OEA y se ve reflejada también en documentos de la ONU, en todo caso, en el documento *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, elaborado y suscrito por varias organizaciones de derechos humanos (2013) se hace este análisis con detalle. El documento se encuentra disponible en <https://necessaryandproportionate.org/es/necesarios-proporcionados> <https://es.necessaryandproportionate.org/>

⁷⁰ Naciones Unidas. *Informe del Relator Especial para la promoción y protección de la libertad de expresión*, 17 de abril de 2013. Documento A/HRC/23/40. Parr. 81. Disponible en <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40>

⁷¹ Corte Constitucional. *Sentencias T-343 de 1993. M.P. Fabio Morón Díaz y C-179 de 1994. M.P. Carlos Gaviria Díaz.*

⁷² Corte Constitucional. *Sentencia C-626 de 1996. M.P. José Gregorio Hernández Galindo.*



TIC Y DERECHOS HUMANOS

De acuerdo con el artículo 15 de la Constitución Nacional ya mencionado, en Colombia hay reserva legal y judicial para la limitación al derecho a la intimidad. Además, el artículo 28 de la Constitución establece que toda persona es libre y que, por lo tanto, el domicilio de ninguna persona puede ser registrado, “sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley”. Esta regla general tiene tan solo una excepción, también establecida en la Constitución, que es la facultad que tiene la Fiscalía General de realizar “registros, allanamientos, incautaciones e interceptaciones de comunicaciones” (artículo 250 de la Constitución) sin orden judicial previa, aunque en todo caso especificando que deberá existir un control de legalidad posterior de la actuación. El artículo 235 del Código de Procedimiento Penal complementa esta facultad de la Fiscalía para intervenir las comunicaciones de forma legítima. Adicionalmente, la Fiscalía puede ordenar la recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones de la persona indiciada o imputada, según establece el artículo 236 CPP. Estas actividades están sometidas a control judicial posterior.⁷³

En la práctica la situación puede ser muy diferente. En un análisis comparado de las normas de interceptación de comunicaciones en América Latina realizado por la organización Electronic Frontier Foundation, se estableció que hay importantes falencias en Colombia en relación con la consagración y en aplicación de las normas de interceptación de comunicaciones por parte del Estado. Así por ejemplo respecto del respeto al principio de legalidad en el marco jurídico colombiano afirman:

En Colombia, La ley 1621, que regula las actividades de inteligencia, también define vagamente la vigilancia de las comunicaciones, dejando un amplio margen para un potencial abuso. Posteriormente, la Corte Constitucional de Colombia interpretó estas imprecisiones como una autorización para permitir que las agencias de inteligencia puedan monitorear todo el espectro electromagnético con independencia de los medios tecnológicos empleados. Pero esta ley no autoriza explícitamente la vigilancia masiva: En virtud de la jurisprudencia bajo la cual se aprobó la nueva ley de inteligencia de Colombia, el Tribunal Constitucional hace hincapié en que la interceptación sólo es permisible durante una investigación criminal y con autorización judicial. Bajo esta ley, a las agencias de inteligencia sólo

⁷³ Cortés, C. *Vigilancia de las comunicaciones en Colombia*, Bogotá, De justicia. Disponible en: <https://www.dejusticia.org/publication/vigilancia-de-las-comunicaciones-en-colombia-el-abismo-entre-la-capacidad-tecnologica-y-los-controles-legales/> <https://www.dejusticia.org/publication/vigilancia-de-las-comunicaciones-en-colombia-el-abismo-entre-la-capacidad-tecnologica-y-los-controles-legales/>



se les permite monitorear el espectro, que es teóricamente diferente a interceptar las comunicaciones, de acuerdo con el Tribunal. La ley no define “el monitoreo del espectro” pero en tanto la Ley 1621 establece claramente que “el monitoreo no constituye intercepción”, una frase que puede ser interpretada ampliamente, es bastante probable que la ley pueda ser usada con ese mismo propósito. De hecho, esto puede haber ocurrido ya: durante los últimos años, y sin ninguna autorización legal aparente, se han articulado varios programas de vigilancia de masiva. Estos programas se extenderán, supuestamente, a través de mecanismos tales como la Plataforma Única de Monitoreo y Análisis (PUMA) y el Sistema Integral de Grabación Digital, SIGD].⁷⁴

El reto del sistema judicial colombiano es velar por garantizar que se apliquen los estándares de derechos humanos.

3.3 Retención de datos

Como ya se mencionó las tecnologías digitales ofrecen amplias capacidades para la captura, almacenamiento y administración de enormes cantidades de datos y de información que puede resultar altamente reveladora, incluso de los aspectos más íntimos de la vida privada de las personas. Esta actividad se hace usando diferentes métodos que se han visto incrementados o mejorados por la tecnología. En esta oportunidad analizaremos uno: la retención de datos.

Los datos de las personas se encuentran en bases de datos que tienen diversos fines y son administrados por entidades públicas o privadas, que recogen información constantemente, incluso sin que lo notemos. Los Estados también están disponiendo la obligatoriedad de conservar y retener los datos de las comunicaciones para poder llevar a cabo una vigilancia histórica.⁷⁵ Ese almacenamiento de datos en el tiempo que tiene como fin un uso posterior, es la retención de datos.

⁷⁴ Katitza Rodríguez, “Análisis comparativo de las leyes y prácticas de vigilancia en Latinoamérica”, disponible en <https://necessaryandproportionate.org/es/an%C3%A1lisis-comparado-de-las-leyes-y-pr%C3%Accticas-de-vigilancia-en-latinoam%C3%A9rica> <https://necessaryandproportionate.org/es/an%C3%A1lisis-comparado-de-las-leyes-y-pr%C3%Accticas-de-vigilancia-en-latinoam%C3%A9rica> <https://necessaryandproportionate.org/es/an%C3%A1lisis-comparado-de-las-leyes-y-pr%C3%Accticas-de-vigilancia-en-latinoam%C3%A9rica>

⁷⁵ Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 17 de abril de 2013. Documento A/HRC/23/40. Párr. 15. Disponible en <https://necessaryandproportionate.org/es/an%C3%A1lisis-comparado-de-las-leyes-y-pr%C3%Accticas-de-vigilancia-en-latinoam%C3%A9rica> <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40>



TIC Y DERECHOS HUMANOS

El nivel de riesgo que estas capacidades suponen hizo que ya en 2013 el Relator Especial para la Libertad de Expresión de las Naciones Unidas, en su informe sobre vigilancia de las comunicaciones, afirmara:

Las leyes nacionales de conservación de datos son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental.⁷⁶

Con fundamento en su análisis concluyó en forma enfática que los Estados deben facilitar comunicaciones privadas, seguras y anónimas, y “esto los obliga a no conservar ni exigir la retención de información determinada puramente con fines de vigilancia”.⁷⁷

El computador registra desde la hora en que se enciende hasta los sitios por los que navega una persona, mientras que los celulares por su parte están constantemente registrando su ubicación geográfica, coleccionan las llamadas que se hacen y reciben y el tiempo que duran, por ejemplo. El conjunto de estos datos es el que ofrece el riesgo, pues su análisis y cruce puede ser tan revelador que puede constituir una grave violación a la intimidad de una persona. Es frecuente que la entrega de estos datos se haga voluntariamente o sin conciencia plena, pues resultan necesarios para la prestación de servicios (como transporte o telecomunicaciones) y, por tanto, se entregan sin ninguna resistencia o cuestionamiento.

Tradicionalmente se habla de la protección de las comunicaciones y se entiende con ello su contenido. Sin embargo, dadas las capacidades descritas desarrolladas por las tecnologías digitales, los organismos internacionales mencionan también los “metadatos” o datos de las comunicaciones para hacer extensivas sus protecciones.⁷⁸ Los metadatos son precisamente esos datos que se producen por las propias comunicaciones como el tiempo de duración de una llamada, el número al que se llamó, la ubicación geográfica del dispositivo que la produce, etcétera.

⁷⁶ Naciones Unidas. *Informe del Relator Especial para la promoción y protección de la libertad de expresión*, 17 de abril de 2013. Documento A/HRC/23/40. Parr. 67. Disponible en <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40> <http://undocs.org/es/A/HRC/23/40>

⁷⁷ *Ibid.* Parr. 90.

⁷⁸ *Ibid.* Parr. 15.



TIC Y DERECHOS HUMANOS

Dado que la agregación de datos es más reveladora incluso que el propio contenido de las comunicaciones se ha establecido que la retención de datos es una medida que restringe y afecta los derechos a la intimidad y a la libertad de expresión. En esa línea el Tribunal de Justicia de la Unión Europea señaló que los metadatos “considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado”.⁷⁹

En consecuencia, las Naciones Unidas en su informe sobre privacidad en la era digital, citando también fallos del Tribunal de Justicia Europeo, afirma que

(...) toda captura de datos de las comunicaciones es potencialmente una injerencia en la vida privada y, además, la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, independientemente de si posteriormente se consultan o utilizan esos datos. Incluso la mera posibilidad de que pueda captarse información de las comunicaciones crea una injerencia en la vida privada y puede tener un efecto negativo en derechos como los relativos a la libertad de expresión y de asociación. La mera existencia de un programa de vigilancia en masa crea, por lo tanto, una injerencia en la privacidad. Incumbiría al Estado demostrar que tal injerencia no es arbitraria ni ilegal.⁸⁰

En tanto injerencia en la vida privada de una persona, si un Estado quiere desarrollar una obligación de retención de datos está obligado a cumplir con los requisitos de (1) legalidad, (2) objetivo imperativo, (3) necesidad, idoneidad y proporcionalidad, y (4) control judicial y debido proceso, derivados de los estándares internacionales. Con fundamento en lo anterior los argumentos con los que el Tribunal de Justicia de la Unión Europea declaró la invalidez de la Directiva 2006/24/EC sobre retención de datos son relevantes, pues apuntan a muchos de los problemas que tienen los regímenes de retención de datos en el mundo.⁸¹

79 Tribunal de Justicia de la Unión Europea, sentencia en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros*, sentencia de 8 de abril de 2014, párrs. 26, 27 y 37, disponible en [http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=ENhttp://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN). Véase también Oficina Ejecutiva del Presidente, “*Big Data and Privacy: A Technological Perspective*”, pág. 19, disponible [https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy](https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacyhttps://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy).

80 Naciones Unidas. *Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). El derecho a la privacidad en la era digital.* A/HRC/27/37, párr. 19.

81 Tribunal de Justicia de la Unión Europea, sentencia en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros*, sentencia de 8 de abril de 2014, párrs. 26, 27 y 37. Disponible en [http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=ENhttp://eur-lex.europa.eu/legal_content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN) <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN>



Un análisis judicial tuvo un resultado parecido en Argentina. En ese país la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal declaró inconstitucional, por violar los requisitos de legalidad y necesidad y proporcionalidad, la Ley No. 25.873 y su decreto reglamentario No. 1563 de 2004. Estas normas obligaban a los prestadores de servicios de telecomunicaciones a “registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos” durante 10 años y con el fin de permitir su acceso al Poder Judicial o del Ministerio Público.

El Tribunal argentino señaló⁸² que era vago invocar el interés general para soportar la retención de datos, dada la afectación que comportaba para los intereses de la ciudadanía. Concretamente, al analizar la legalidad de la medida, manifestó la poca claridad sobre lo que eran los datos de tráfico que podían confundirse con el contenido de la comunicación. Respecto al acceso a los datos, indicó que no solo no era claro cuáles eran las autoridades que podían accederlos, sino que reiteró que es un requisito indispensable que exista autorización judicial para ese propósito. Respecto al principio de proporcionalidad señaló que “la norma en cuestión pone bajo sospecha a todos los usuarios de los servicios de telecomunicaciones por el amplísimo término de 10 años”, lo que se agrava en el ámbito de las comunicaciones digitales porque allí “todos los movimientos quedan registrados”.

En Colombia, la retención de datos se encuentra consagrada en dos normas:

1. El Decreto No. 1704 de 2012, que trata de la retención de datos para efectos de investigación criminal.
2. La Ley No. 1621 de 2013, que lo hace para efectos de actividades de inteligencia.

La retención de datos en el caso de investigación criminal, supone la obligación para los proveedores de servicios de telecomunicaciones de conservar la información del suscriptor y los datos que permitan saber la localización de terminales en tiempo real (artículos 4 y 5 del Decreto 1704 de 2012). En el caso de las actividades de inteligencia, se pide la retención del “historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación” y los datos de localización (artículo 44 Ley 1621 de 2013).

⁸² Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal (2005, 29 de noviembre). Halabi v. Estado Nacional.



TIC Y DERECHOS HUMANOS

Muchas son las críticas que se derivan de analizar el sistema de retención de datos colombiano⁸³, por ejemplo: que no está claro qué significa “historial de comunicaciones”, ni el alcance de las cláusulas generales empleadas en estas normas (p. ej. “entre otras” o “cualquier otra información”) o, sobre la duración, decir que en ambos casos los datos deben ser retenidos por 5 años sin establecer diferencias ni explicar su propósito (p. ej. en la Unión Europea y en Argentina los plazos que rechazaron los Tribunales en su análisis de derechos humanos fueron 2 y 10 años respectivamente).

La tecnología digital facilita la retención de datos que se intuye como una herramienta muy útil para la investigación por parte de las autoridades. Sin embargo, como dan cuenta los fallos judiciales en Europa y Argentina, existen cuestionamientos importantes sobre su verdadera utilidad frente al riesgo que representa para la vulneración de los derechos de las personas. Fundación Karisma hizo un análisis comparativo de los marcos jurídicos de retención de datos en cinco países de América Latina para concluir:

(...) la mayoría de regímenes están establecidos en una mezcla de leyes y decretos, por lo que la retención de datos no siempre ha sido materia de discusión en los congresos. En cuanto a la legalidad, la legislación colombiana usa términos particularmente ambiguos y las autoridades que pueden acceder a los datos retenidos.

Pero el principal problema no es la legalidad, pues bien puede aprobarse una ley que viole derechos fundamentales. El problema es la falta de objetivos legítimos y de ahí que la retención de datos no sea una medida necesaria y proporcional.

A excepción de México, ningún otro país define qué es la seguridad nacional, que es el objetivo que se persigue cuando la retención de datos se establece como una herramienta para labores de inteligencia. Colombia, como los demás países, simplemente evoca este objetivo sin desarrollarlo ni limitarlo. Por tanto, si el objetivo que busca la medida no es legítimo, no puede hablarse de necesidad y proporcionalidad pues estos requisitos existen en relación con ese objetivo. Por naturaleza la orden de retener datos es automática y no pasa por ningún control judicial, de ahí que tampoco esté a la altura de los estándares internacionales de los que hemos hablado.

Esta situación, en combinación con la falta de notificación a las personas usuarias y la escasa implementación de obligaciones de transparencia hace que el uso de la retención de datos aún esté en la sombra y, por tanto, la ciudadanía carezca de datos para determinar la utilidad de esta medida.⁸⁴

83 Castañeda, J.D. “*¿Es legítima la retención de datos en Colombia?, análisis comparativo de una herramienta de vigilancia masiva que restringe los derechos humanos*”. Fundación Karisma, 2016. Disponible en <https://karisma.org.co/es-legitima-la-retencion-de-datos-en-colombia-2/>

84 *Ibid.*



También en este caso, la tecnología plantea retos específicos para los jueces que deberán equilibrar los marcos legales para buscar la garantía de los derechos fundamentales de las personas.

3.4 Explotación de datos

El hecho de que los dispositivos digitales estén diseñados para producir datos sobre su uso, lo que termina por significar la generación de datos sobre el comportamiento de los usuarios, ha generado una serie de retos para la aplicación de los derechos humanos respecto a las tecnologías digitales. Así mismo, los datos están en el centro de nuevos mercados que actualmente superan por mucho las concentraciones de capital del pasado. De ahí la frase, cada vez más común: "los datos son el nuevo petróleo".⁸⁵

WeChat, por ejemplo, es una aplicación china de tal tamaño que un 85% de sus más de 900 millones de suscriptores usa la aplicación diariamente. Aunque empezó siendo una aplicación de chat, hoy incorpora muchos servicios más: la funcionalidad "wallet" (billetera) es una plataforma de pagos usada en diversos establecimientos, por ejemplo, para pagar los servicios de Didi Chuxing, una versión local de Uber e incluso, en algunas ciudades puede gestionar el servicio de salud, por ejemplo, para pedir citas médicas. La aplicación recolecta toda clase de información personal: datos biométricos, financieros, ubicación, búsquedas en Internet, perfiles visitados, metadatos de las comunicaciones (con quién, cuándo y dónde el usuario ha entablado comunicación), entre otros. WeChat ofrece estos datos a empresas para vender publicidad a sólo ciertos usuarios o para determinar el nivel de crédito de una persona a partir del análisis de su actividad en línea.⁸⁶

En este contexto, el derecho a la intimidad, formulado de manera negativa como la prohibición de injerencias arbitrarias en la vida de cada persona, no es suficiente para hacer frente a los retos que presenta para los derechos humanos el desarrollo de la tecnología. En ocasiones, la tecnología digital más novedosa se aproxima desde una visión de optimismo:

85 "The world's most valuable resource is no longer oil, but data", *The Economist*, Mayo 6 de 2017. Disponible en <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>

86 Un análisis más detallado del papel de una "súper aplicación" como WeChat puede encontrarse en: *Privacy International. Case Study: Super-Apps and the Exploitative Potential of Mobile Applications*. Disponible en: <https://www.privacyinternational.org/node/789> <https://www.privacyinternational.org/node/789>.



TIC Y DERECHOS HUMANOS

(...) este optimismo, tal vez ingenuo, parece haber relegado a un plano secundario la consideración de un aspecto específico de la informatización del Estado que concierne en grado sumo al ciudadano común, a saber: el uso indebido de una ingente masa de información en manos del Ejecutivo bien puede acarrear consecuencias nocivas para sus derechos en países donde todavía no existe una regulación adecuada sobre nuevas tecnologías de información como es, precisamente, el caso de Colombia.⁸⁷

El poder informático consiste en la sujeción del individuo a través de su información, posibilidad que ha realizado los distintos avances tecnológicos.⁸⁸ Por ejemplo, quien administra o usa bases de datos sobre antecedentes penales “tiene el poder de afectar diferentes libertades de las personas (circulación, trabajo, no discriminación, etc.)”.⁸⁹ El conocimiento o posesión de datos sobre alguien implica entonces tener un “poder informático” sobre ella, por lo cual es posible que se encuentre un abuso de este poder.⁹⁰

Ap

Diana López es periodista y usa Facebook activamente tanto en su vida personal como para publicar opiniones sobre la vida política del país. La periodista utilizó su cuenta para publicar una opinión que incluía su valoración de lo sucedido con un político de su región y basó sus conclusiones en información que, dijo, recibió de sus lectores.

Debido a sus comentarios fue denunciada por injuria por el político protagonista de su nota. El fiscal que conoció el caso solicitó ante el Juzgado de Control de Garantías que autorizara una búsqueda selectiva en base de datos de la cuenta de Facebook de la periodista. La solicitud fue concedida en los siguientes términos “El despacho accede a autorizar al ente fiscal emita la orden de búsqueda selectiva en base de datos de la cuenta <https://facebook.com/diana.lopez/> y para buscar datos de suscriptores, direcciones de conexiones IP, servicios utilizados, teléfono móvil o correo electrónico asociado, lista de contactos, destinatario de mensajes enviados y claves de acceso, durante el periodo comprendido entre el mes de noviembre a diciembre de 2016, dicha orden tendrá un término de 15 días”.

La periodista interpuso una tutela contra esta decisión por considerar que no solo se vulnera su derecho a la libertad de expresión sino que, además, se desconoce la jurisprudencia sobre secreto de la fuente y es desproporcional, pues una decisión de ese tipo obliga a aplicar, en lo pertinente, las normas de registro y allanamiento, que es lo que permitiría limitar el alcance de esta medida pues, el no hacerlo equivaldría, por ejemplo, a que un fiscal que pretenda conocer el contenido de una carta enviada a una persona determinada en una fecha determinada solicitara autorización a un juez para leer todas las cartas enviadas o recibidas durante toda la vida de una persona.

Usted es el juez de tutela ¿Cómo resolvería este caso? ¿Qué elementos tendría en cuenta?

87

Corte Constitucional. Sentencia T-414 de 1992. M.P. Ciro Angarita Barón.

88

Corte Constitucional. Sentencia C-1011-08. M.P. Jaime Córdoba Triviño.

89

Corte Constitucional. Sentencia SU-458 de 2012. M.P. Adriana María Guillén Arango

90

Corte Constitucional. Sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño y Sentencia T-303 de 1993, M.P. Hernando Herrera Vergara.



Ae

Autoevaluación
Lea los siguientes artículos:

1. ¿Es la acumulación de datos el petróleo del siglo XXI?... piénselo de nuevo (Publicado por Rajan Amol en El Mundo, 14 de octubre de 2017. Disponible en <http://www.bbc.com/mundo/noticias-41600755>)
2. Personalizar TuLlave es entregar un cheque en blanco (Publicado por Carolina Botero en La Silla Vacía en dos partes el 29 de noviembre de 2017, disponible en: Parte I <http://lasillavacia.com/silla-llena/red-de-la-innovacion/historia/personalizar-tullave-es-entregar-un-cheque-en-blanco-parte> y Parte II <http://lasillavacia.com/silla-llena/red-de-la-innovacion/historia/personalizar-tullave-es-entregar-un-cheque-en-blanco-0>)

En grupos de 3 a 5 personas discutan las lecturas propuestas. Reflexionen sobre la capacidad de consentimiento que tienen las personas en un mundo donde los sistemas de información son cada vez más usados en diferentes esferas. Puede usar como detonante que mientras Rajan Amol indica que "es en gran medida resultado de mis opciones que estas empresas tengan tantos de mis datos personales.", Carolina Botero habla sobre cómo se entregan datos en ocasiones porque no "hay más opción pública para viajar y el único prestador será Transmilenio".

J

- Corte Constitucional. Sentencia T-277 de 2015. M.P. María Victoria Calle Correa.
- Corte Constitucional. Sentencia T/011 de 1992. M. P. Alejandro Martínez Caballero
- Corte Constitucional. Sentencia T-343 de 1993. M.P. Fabio Morón Díaz
- Corte Constitucional. Sentencia C-179 de 1994. M.P. Carlos Gaviria Díaz.
- Corte Constitucional. Sentencia C-626 de 1996. M.P. José Gregorio Hernández Galindo.
- Corte Constitucional. Sentencia T-414 de 19-92. M.P. Ciro Angarita Barón
- Corte Constitucional. Sentencia C-1011-08. M.P. Jaime Córdoba Triviño.
- Corte Constitucional. Sentencia SU-458 de 2012. M.P. Adriana María Guillén Arango
- Corte Constitucional. Sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño
- Corte Constitucional. Sentencia T-303 de 1993, M.P. Hernando Herrera Vergara.



B

- Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 17 de abril de 2013. Documento A/HRC/23/40. Disponible en <http://undocs.org/es/A/HRC/23/40>
- Naciones Unidas. Asamblea General. El Derecho a la privacidad en la era digital. Documento A/RES/68/167. Resolución aprobada el 18 de diciembre de 2013. Disponible en <http://undocs.org/es/A/RES/68/167>
- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. Documento OEA/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Disponible en: <http://bit.ly/1WHR6cD> o en CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. Documento OEA/Ser.L/V/II. CIDH/rele/inf.11/13, 31 de diciembre de 2013. Disponible en http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf
- Naciones Unidas. Informe del Relator Especial para la promoción y protección de la libertad de expresión, 22 de mayo de 2015. Documento ONU A/HRC/29/32, Cifrado y anonimato en las comunicaciones digitales. Disponible en: <http://bit.ly/2pa0zYu>
- 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. Disponible en <http://on.unesco.org/2qwfUaS>
- CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 2014. Disponible en <http://bit.ly/1qR7bYf>
- Universidad de los Andes, Dejusticia y Open Society Foundations. Nuevos Desafíos: Libertad de en Internet. Unesco. Caja de herramientas para escuelas judiciales iberoamericanas. Formación de formadores en libertad de expresión, acceso a la información pública y seguridad de periodistas. Edición Marine González, 2017. Disponible en <http://unesdoc.unesco.org/images/0025/002515/251593S.pdf>
- Comisión Interamericana de Derechos Humanos (CIDH). Relatoría Especial para la Libertad de Expresión. Video: "Libertad de expresión e Internet". 17 de junio de 2014. Disponible en <https://www.youtube.com/watch?v=YaTvcMCrcNg>
- Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/29/32. Mayo 22 de 2015. Párr. 56. Recuperado en <http://www.globalmediapolicy.net/node/15836>



Unidad 4: FLUJOS DE INFORMACIÓN

Og

El objetivo general de la Unidad 4 es presentar algunas de las problemáticas más actuales que se derivan del uso de tecnología digital, su interacción con la infraestructura de Internet y que muestran la tensión de derechos propias de esta nueva era.

Oe

- Identificar estándares internacionales y precedentes jurisprudenciales que le permitirán resolver de forma sustentada problemas referentes a la neutralidad de la Red.
- Resolver, con base en precedentes jurisprudenciales, las disputas en torno a prácticas de los actores de Internet o a las regulaciones en las que se vea involucrado el principio de neutralidad de la Red.
- Interiorizar, reflexionar y ser consciente de las garantías constitucionales que dependen del principio de neutralidad de la red y de la necesidad de conservarla.

MAPA CONCEPTUAL

Unidad 4: Flujos de información

4.1 Neutralidad de la red

4.2 Filtrado y bloqueo

4.3 Violencia de género y entornos digitales



Co

Contenido

En esta unidad se ha querido recoger importantes y nuevos conceptos, retos y tensiones de derechos que se derivan del flujo de información que facilita Internet y que, dadas las características de esta red, deben ser analizados en forma particular. Estos temas recogen de una u otra manera lo que se ha visto en las unidades anteriores.

Las lecturas sugeridas en relación con estos temas son las siguientes:

- Fundación Karisma, “Neutralidad de la red y ofertas comerciales en Colombia, análisis de la regulación”, Juan Diego Castañeda y Laura Daniela González, Bogotá, 2017, Disponible en <https://karisma.org.co/fundacion-karisma-publica-informe-sobre-neutralidad-de-la-red-en-colombia/>
- “Curso Avanzado para Jueces y Operadores Jurídicos en las Américas”. Propuesta curricular y materiales de estudio. Elaborado por Catalina Botero, Federico Guzmán, Sofía Jaramillo y Salomé Gómez para De Justicia con el apoyo de Open Society Foundations (osf). 2017, Disponible en: <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf> <https://www.dejusticia.org/wp-content/uploads/2017/05/Gui%CC%81a-Curricular-Versi%CC%81n-Final-.pdf>

4.1 La neutralidad de la red⁹¹

El principio de neutralidad de la red es la prohibición para los intermediarios que proveen Internet a las personas de interferir con el uso que ellas hacen de Internet, siempre que este uso sea legal.

⁹¹ *El tema de neutralidad de la red se desarrolló adaptando y complementando el Tema 2 del módulo 8 del texto “El Derecho a la Libertad de Expresión. Curso Avanzado para Jueces y Operadores Jurídicos en las Américas”. Propuesta curricular y materiales de estudio. Elaborado por Catalina Botero, Federico Guzmán, Sofía Jaramillo y Salomé Gómez para De Justicia con el apoyo de Open Society Foundations (OSF). 2017, Disponible en https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf*



TIC Y DERECHOS HUMANOS

La neutralidad busca proteger la libertad de las personas para escoger y usar cualquier contenido, aplicación o servicio y, en consecuencia, conservar la naturaleza abierta de Internet, que ya discutimos y que permite a cualquier persona generar y transmitir contenidos de todo tipo.⁹²

Este principio se asocia directamente con la defensa de la libertad de expresión porque conservar la dinámica abierta de Internet es preservar una plataforma para mejorar el discurso democrático, facilitar la organización y la acción política, además de proveer un ambiente descentralizado para la interacción social, cultural y política en el cual todos pueden participar. El principio está definido en la Declaración Conjunta de los Relatores sobre Libertad de Expresión e Internet de 2011, según este principio “el tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación”.⁹³

Esto implica principalmente que “la libertad de acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet no esté condicionada, direccionada o restringida, por medio de bloqueo, filtración o interferencia”.⁹⁴

La Comisión Interamericana de Derechos Humanos (CIDH) ha reafirmado que la defensa del principio de neutralidad de la red vincula la protección de la libertad de expresión con la arquitectura original de Internet:

(...) la neutralidad de la red se desprende de su diseño original, el cual facilita el acceso y la difusión de contenidos, aplicaciones y servicios de manera libre y sin distinción alguna. Al mismo tiempo, la inexistencia de barreras desproporcionadas de entrada para ofrecer nuevos servicios y aplicaciones constituye un claro incentivo para la creatividad, la innovación y la competencia.⁹⁵

⁹² Comisión de Regulación de Comunicaciones, *Neutralidad de Internet, informe técnico (2011)*: 5. Recuperado en https://www.crc.com.gov.co/es/recursos_user/Actividades%20Regulatorias/Neutralidad_Internet/Documento_Soporte.pdf https://www.crc.com.gov.co/es/recursos_user/Actividades%20Regulatorias/Neutralidad_Internet/Documento_Soporte.pdf

⁹³ El Relator Especial para la Libertad de Opinión y de Expresión de Naciones Unidas (ONU), la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial para la Libertad de Expresión de la Organización de Estados Americanos (OEA) y la Relatora Especial para la 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, punto 5(a). Disponible en: <http://bit.ly/1eX83sn> <http://bit.ly/1eX83sn> <http://bit.ly/1eX83sn>

⁹⁴ CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de expresión e Internet. oea/Ser.L/V/II. CIDH/rele/inf.11/13. 31 de diciembre de 2013. párr. 25.* Disponible en: <http://bit.ly/1WHR6cD> <http://bit.ly/1WHR6cD>

⁹⁵ Ibídem.



TIC Y DERECHOS HUMANOS

La no discriminación se predica de particulares y de los Estados, pero es deber de los Estados adoptar las medidas legislativas, administrativas, judiciales y de otro carácter que sean necesarias para dar aplicación al principio de neutralidad de la red.

En tal sentido, en virtud del principio de neutralidad de la red, los Estados están obligados tanto a abstenerse de intervenir sobre el flujo informativo legal de Internet, sea cual sea el criterio de selección o discriminación. También deben impedir que terceros actores establezcan controles informativos con efectos semejantes de restricción del acceso a información por determinados sectores de usuarios. Para la Relatoría Especial de la CIDH:

(...) deben adoptarse medidas para evitar que el establecimiento de controles particulares genere una violación de la libertad de expresión. Como sostiene el artículo 13.3 de la Convención Americana, las restricciones indirectas a este derecho pueden también provenir de determinados actos de particulares y los Estados deben asumir un rol de garantía frente a esos abusos.⁹⁶

Ahora bien, el principio de neutralidad de la red también tiene una aplicación específica, ya no en la gestión de los contenidos, sino en la gestión del tráfico de Internet. Se ha aceptado que los proveedores de Internet tienen una potestad razonable de gestionar dicho tráfico para efectos de finalidades técnicas e infraestructurales de la red, o también para excluir determinados emisores de contenidos que son ilegales, o contenidos que han sido voluntariamente excluidos por el usuario del servicio de Internet. En palabras de la Relatoría Especial de la CIDH:

No debe haber discriminación, restricción, bloqueo o interferencia en la transmisión del tráfico de Internet, a menos que sea estrictamente necesario y proporcional para preservar la integridad y seguridad de la red, para prevenir la transmisión de contenidos no deseados por expresa solicitud —libre y no incentivada— del usuario; y para gestionar temporal y excepcionalmente la congestión de la red. En este último caso, las medidas de gestión del tráfico empleadas no deben discriminar entre tipos de aplicaciones o servicios. Además, la propuesta de la Comisión Europea para la regulación del mercado único europeo para comunicaciones electrónicas reconoce que 'la gestión razonable del tráfico incluye la prevención o impedimento de crímenes graves, incluidas las acciones voluntarias de proveedores para prevenir el acceso y la distribución de pornografía infantil'.⁹⁷

96

Ibidem. párr. 28

97

CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de expresión e Internet*. oea/Ser.L/V/II. CIDH/rele/inf.11/13. 31 de diciembre de 2013. párr. 30. Disponible en: <http://bit.ly/1WHR6cD>



Una concreción individual del principio de neutralidad de la red ha sido deducida por los Relatores Especiales para Libertad de Expresión en su Declaración Conjunta sobre el tema y planteada por la Relatoría Especial de la CIDH en su estudio especializado sobre el tema. En este trabajo, al referirse al derecho de acceso a Internet y al deber del Estado de abstenerse de manipular los contenidos comunicacionales que allí circulan, se explicó que:

(...) está prohibida la interrupción del acceso a Internet, o a parte de ésta, aplicada a poblaciones enteras o a determinados segmentos del público, la negación del derecho de acceso a Internet a modo de sanción y las medidas de reducción de la velocidad de navegación de Internet o de partes de esta con fines diferentes a la gestión razonable del tráfico. Todo lo anterior vulnera de manera radical el derecho a la libertad de expresión en Internet.⁹⁸

En Colombia la neutralidad de la red está consagrada en el artículo 56 de la Ley 1450 de 2011, “por la cual se expide el Plan Nacional de Desarrollo, 2010-2014” y fue desarrollada mediante Resolución 3502 de 2011 de la Comisión de Regulación de Comunicaciones.

La forma que adoptó el principio en Colombia es como

- a. Una prohibición de interferir con el acceso a contenidos, aplicaciones o servicios lícitos y,
- b. Una autorización a favor de los proveedores de acceso a Internet (son un tipo de intermediarios en la Red) para ofrecer planes diferenciados de acceso a Internet.

La prohibición, está relacionada con la necesidad que tienen los proveedores de acceso a Internet de gestionar el tráfico que pasa por sus redes. La autorización, en cambio, toca más el aspecto comercial del acceso a Internet a través de los planes que tienen permitido ofrecer esos intermediarios.

Adicionalmente, la Resolución 3502 de 2011 estableció una serie de principios relacionados con la neutralidad. A la fecha la autoridad (Comisión de Regulación de Comunicaciones) no ha expedido ninguna sanción por violación a la neutralidad, tampoco se ha presentado ningún debate judicial al respecto.



4.2 Filtrado y bloqueo⁹⁹

Ya en 2012 el relator especial para la libertad de expresión de la ONU en su informe mencionaba con preocupación el arbitrario uso del filtrado y bloqueo de contenidos en la red como una amenaza a la libertad de expresión.¹⁰⁰ Las órdenes de filtrado o bloqueo de información, por su carácter extremo, sólo serían admisibles en casos excepcionales en los cuales, desde una perspectiva estricta de control, estén cumplidos todos los requisitos de las limitaciones de la libertad de expresión expuestos en el capítulo correspondiente.

En palabras de la Relatoría Especial de la OEA,

(...) el bloqueo o suspensión obligatoria de sitios web enteros o generalizados, plataformas, conductos, direcciones IP, extensiones de nombre de dominios, puertos, protocolos de red o cualquier tipo de aplicación, así como medidas encaminadas a eliminar enlaces (links), datos y sitios web del servidor en el que están alojados, constituyen una restricción que solo será excepcionalmente admisible en los estrictos términos establecidos en el artículo 13 de la Convención Americana.

85. En casos excepcionales, cuando se está frente a contenidos abiertamente ilícitos o a discursos no resguardados por el derecho a la libertad de expresión, resulta admisible la adopción de medidas obligatorias de bloqueo y filtrado de contenidos específicos. En estos casos, la medida debe someterse a un estricto juicio de proporcionalidad y estar cuidadosamente diseñada y claramente limitada de forma tal que no alcance a discursos legítimos que merecen protección. En otras palabras, las medidas de filtrado o bloqueo deben diseñarse y aplicarse de modo tal que impacten, exclusivamente, el contenido reputado ilegítimo, sin afectar otros contenidos.¹⁰¹

⁹⁹ *El tema de filtrado y bloqueo se desarrolló adaptando y complementando el Tema 4 del módulo 8 del texto "El Derecho a la Libertad de Expresión. Curso Avanzado para Jueces y Operadores Jurídicos en las Américas". Propuesta curricular y materiales de estudio. Elaborado por Catalina Botero, Federico Guzmán, Sofía Jaramillo y Salomé Gómez para De Justicia con el apoyo de Open Society Foundations (OSF). 2017, Disponible en <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf> <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf>*

¹⁰⁰ Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, Frank La Rue. A/HRC/17/27. Mayo 16 de 2011, Párr. 82. Recuperado en <http://www.acnur.org/t3/fileadmin/Documentos/BDL/2015/10048.pdf?view=1> <http://www.acnur.org/t3/fileadmin/>

¹⁰¹ CIDH, Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF.11/13, 31 de diciembre de 2013, párr. 66. Ibid., párrs. 84-85.



En todo caso, cuando se establece que la medida de filtrado o bloqueo es necesaria y proporcional para evitar un daño mayor, deben establecerse salvaguardas que eviten el abuso. En el informe de 2013 la Relatoría Especial de la CIDH indicaba como ejemplos de salvaguardas: la transparencia sobre los contenidos cuya remoción ha sido ordenada, información sobre la necesidad y justificación, información sobre la forma como funciona el filtrado o bloqueo y las desventajas si la acción resulta excesiva.¹⁰²

En Colombia la única ley que permite expresamente el bloqueo o filtrado de contenidos es la ley 679 de 2001, “por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución”. Es decir, para evitar la distribución de material de explotación sexual infantil se creó un mecanismo que permite al Ministerio TIC ordenar a los proveedores de acceso a Internet el bloqueo de las páginas que estén distribuyendo este tipo de contenidos.

Como se vio arriba, la sentencia T-063A de 2017 ordenó a Google retirar un blog de su plataforma Blogger en reacción a una denuncia por “honra y buen nombre” que instauró el dueño de una empresa de muebles. En el blog, su autor anónimo acusaba a la empresa de estafar a sus clientes. Google manifestó que, dado que el contenido del blog no es inapropiado ni abiertamente ilegal no podía bloquear el blog mientras no tuviera una orden judicial. El juez de primera instancia le dio la razón a Google. Posteriormente la Corte Constitucional seleccionó la decisión y la modificó ordenando el bloqueo del blog y otras obligaciones negativas para el ejercicio de derechos humanos. La sentencia fue objeto de un incidente de nulidad que obligó a analizar no solo el tema de bloqueo y filtrado sino también la protección del anonimato y el rol de los intermediarios.¹⁰³

Ahora bien, la aprobación del Parlamento de la Unión Europea en marzo de 2019 de una Directiva que reformará el marco jurídico de derechos de autor en los países de esa región va más allá y propone un mecanismo de limitación de la forma como se comparte material protegido por derecho de autor en línea, especialmente en las plataformas de redes sociales, obligando a las empresas a crear mecanismos automatizados para filtrar los contenidos y evitar la publicación de aquellos que “puedan” ser

¹⁰² *Ibid, párrs. 87 y 89.*

¹⁰³ *Corte Constitucional, Auto 285 de 2018, M.P. José Fernando Reyes Cuartas.*



infractores del derecho de autor¹⁰⁴. Así se pasa de un instrumento que se usa y funciona sobre todo como herramienta de apoyo para los sistemas de moderación de contenidos actuales que en todo caso complementa la revisión humana y se hace después de la publicación, para pasar a un mecanismo de censura previa.

El informe del Relator para Libertad de Expresión de la ONU de 2018¹⁰⁵ incluye un análisis de los problemas que ya existen en el mecanismo de automatización como funciona actualmente. El Relator alerta sobre la preocupación de la sociedad civil, que ve cómo los filtros automatizados han sido criticados por su falta de transparencia en la forma en que trabajan y adoptan las decisiones, pide a las empresas trabajar y reforzar la "diligencia debida" en este contexto. El Relator alerta también sobre las importantes limitaciones de que adolece la automatización, como las dificultades para tener en cuenta el contexto, la amplia variación de matices idiomáticos y el significado y las particularidades lingüísticas y culturales. En sus recomendaciones a los Estados el relator sugiere, como ya dijimos, que eviten promulgar leyes o concertar acuerdos que requieran la vigilancia o el filtrado "activo" del contenido, que es incompatible con el derecho a la privacidad y puede ser equivalente a la censura previa a la publicación.

Efectivamente, la tendencia regulatoria actual obliga a ver en la censura previa a las expresiones de las personas uno de sus mayores riesgos. Sabemos que los mecanismos actuales de filtrado automatizado vinculados a la protección del derecho de autor generan numerosos «falsos positivos», especialmente cuando los algoritmos deben navegar por las complejidades de las leyes locales que tienen excepciones de derechos de autor y otros usos legítimos que son complicadas de aplicar incluso para los especialistas. El efecto para la libertad de expresión de incorporar filtros automatizados activos a internet representa importantes riesgos para la libertad de expresión y constituye un mecanismo de censura previa.

¹⁰⁴ Véase el análisis que hacen de la Directiva varias organizaciones de derechos digitales de América Latina "La Directiva Europea de Derecho de Autor y su impacto en los usuarios de América Latina y el Caribe: una perspectiva desde las organizaciones de la sociedad civil". Recuperado en <https://stats.karisma.org.co/la-directiva-europea-de-derecho-de-autor-y-su-impacto-en-los-usuarios-de-america-latina-y-el-caribe-una-perspectiva-desde-las-organizaciones-de-la-sociedad-civil/>

¹⁰⁵ Naciones Unidas. Informe del Relator Especial para la promoción y protección del derecho a la libertad de expresión, David Kaye. A/HRC/38/35. Abril 6 de 2018. Recuperado en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.



4.3 Violencia de género y entornos digitales

La violencia en los entornos digitales crece a la par con la penetración de Internet. Las características de Internet, que hacen que cualquiera pueda expresarse, llevaron en su momento al relator para libertad de expresión de la ONU, Frank La Rue, a considerarla como la nueva “plaza pública”. Pero, si no la cuidamos, no lo será para muchos.

Poblaciones especialmente vulnerables como los niños, niñas y adolescentes, las minorías étnicas o políticas, quienes profesan credos minoritarios, quienes tienen una identidad de género diferente a la normalizada, o las mujeres, suelen ser víctimas de violencias. Las violencias que se ensañan con estas poblaciones fuera de línea se están trasladando al mundo digital. Para exemplificar esto analizaremos el caso de la violencia contra las mujeres, pero es necesario pensar y analizar otras violencias.

Internet es un espacio privilegiado para dar voz y, sin embargo, la violencia del mundo fuera de línea contra las mujeres amenaza con convertirse en un mecanismo de censura para ellas.

Aunque en Colombia se reconocen los derechos de las mujeres, adicionalmente se han ratificado los tratados internacionales y regionales más importantes que garantizan sus derechos.¹⁰⁶ La Constitución Política, en su artículo 13, reconoce el derecho a la igualdad y prohíbe la discriminación por razón de género. Además, establece la obligación del Estado de fomentar la igualdad real y efectiva a través de acciones afirmativas. El artículo 43, por su parte, garantiza la igualdad de derechos y oportunidades para mujeres y hombres, además de que establece la no discriminación de las mujeres.

El Estado colombiano también ha mostrado significativos progresos en el desarrollo de normas que promueven la igualdad de género y salvaguardan los derechos de las mujeres¹⁰⁷, por su parte, la jurisprudencia colombiana ha reafirmado que no solo hay obligación de reconocer la igualdad ante la ley, sino ante el cumplimiento de los derechos.¹⁰⁸ Esa jurisprudencia ha

¹⁰⁶ Por ejemplo, la Convención para la eliminación de todas las formas de violencia contra la mujer (1979) o Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (1994), conocida como la Convención de Belém do Pará.

¹⁰⁷ Véase, por ejemplo, la ley contra la violencia hacia las mujeres, Ley No. 1257 de 4 de diciembre de 2008 y su reglamento, o la ley que crea el delito del feminicidio, Ley No. 1761 de 6 de julio de 2015.

¹⁰⁸ Véase, por ejemplo, Corte Suprema de Justicia, Sala de Casación Penal, Sentencia del 23 de septiembre de 2009, M.P. Julio Enrique Socha Salamanca; Corte Constitucional de Colombia (2008), Sentencia T-496, M.P. Jaime Córdoba Triviño; Corte Constitucional de Colombia (2011, 8 de noviembre), Sentencia T-843, M.P. Jorge Ignacio Pretelt Chaljub.



TIC Y DERECHOS HUMANOS

tenido un tratamiento normativo importante en cuanto al reconocimiento de la discriminación histórica y estructural contra la mujer en la promoción efectiva de la igualdad y la erradicación de la discriminación contra las mujeres.

Sin embargo, hay una desconexión entre las normas y la práctica, que se ve reflejada en las estadísticas. Los números muestran una violencia de origen de género muy arraigada en la sociedad colombiana.¹⁰⁹ Si esto ocurre en el mundo fuera de línea, la situación en el mundo en línea no es mejor. El problema todavía no se puede medir con números, no hay estadísticas que lo evidencien, tampoco hay estrategias ni mecanismos de control para enfrentarla.

Sin embargo, puede afirmarse que la violencia digital contra la mujer en entornos digitales replica las dinámicas y repertorios de violencias del mundo fuera de línea. A esto se suma que sus impactos pueden ser más graves dada la naturaleza misma de Internet: los contenidos violentos son fácil y ampliamente difundidos y compartidos entre muchas personas, además de que permanecen accesibles durante mucho más tiempo después del incidente inicial.¹¹⁰

Manifestaciones de las violencias digitales contra las mujeres son, por ejemplo, el ciberacoso exhibido a través la difusión de rumores, la publicación de mensajes denigrantes, entre otros. La divulgación sin consentimiento de fotos con contenido íntimo sexual, la revelación de información personal como ubicación, contactos, etc. (doxxing), la sextorsión o chantaje con una imagen de contenido sexual de la víctima, amenazas de violencia física o de muerte, etc. Y su objetivo no es otro que afectar el buen nombre, credibilidad y reputación de la mujer, desestabilizarla y crear miedo, dominio, control, vigilancia o censura, etc.

En este contexto el anonimato que Internet facilita y que sirve de escudo protector para la libertad de expresión de muchos --como ya vimos en otra parte de este documento--, representa un problema para estas mujeres.

¹⁰⁹ Según el Instituto Nacional de Medicina Legal y Ciencias Forenses en 2016 de los 26,473 casos de violencia en el contexto familiar, el 59% de las víctimas fueron mujeres y en los casos de la violencia entre pareja o por expareja, las estadísticas también demuestran que es la mujer la que se lleva la peor parte: es la víctima en el 86% de los más de medio millón de casos reportados ese año. *Forensis 2016. Datos para la vida. Bogotá, Colombia, 2017.* Disponible en <http://www.medicinallegal.gov.co/documents/88730/4023454/Forensis+2016+-+Datos+para+la+Vida.pdf/af636ef3-0e84-46d4-bc1b-a5ec7lac9fc1> <http://www.medicinallegal.gov.co/documents/88730/4023454/Forensis+2016+-+Datos+para+la+Vida.pdf/af636ef3-0e84-46d4-bc1b-a5ec7lac9fc1>

¹¹⁰ Dickinson, J., Levin, E. & Pettalia, J.L. (2013). *Cyberbullying: Eliciting harm without consequence. Computers in Human Behavior.* 29(6), pp. 2758-2765. DOI: 10.1016/j.chb.2013.07.020.



Aunque tampoco es que ese anonimato sea requisito indispensable para que una mujer sea víctima de violencia digital, sobre todo, si se piensa en el contexto de la violencia doméstica en entornos digitales, donde el victimario suele ser una persona conocida, sí es una característica que puede potenciar su vulnerabilidad. Ahora bien, pensar que acabar con el anonimato en la red sería la solución para evitar la violencia contra las mujeres sería una conclusión errónea.

La Convención Americana sobre derechos humanos en su artículo 13.5 prohíbe “toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional”. Cuando se trata de casos de violencia contra una persona en razón a su género el juez puede usar instrumentos como el bloqueo y filtrado, e incluso herramientas para tomar medidas razonables que le permita identificar a la persona que incurre en las acciones prohibidas y aplicarle el castigo previsto en el ordenamiento legal.

Así, por ejemplo, en el informe sobre «Discurso de odio y la incitación a la violencia contra las personas lesbianas, gays, bisexuales, trans e intersex en América»¹¹¹, la Relatoría Especial para la Libertad de Expresión hizo una revisión general del marco jurídico interamericano relativo al discurso de odio y la incitación a la violencia que puede ayudar y dar parámetros sobre la forma de aplicar este marco en general a poblaciones vulnerables.

¹¹¹ CIDH, *Relatoría Especial para la Libertad de Expresión. Informe Anual 2014. Capítulo IV (Discurso de odio y la incitación a la violencia contra las personas lesbianas, gays, bisexuales, trans e intersex en América). OEA/Ser.L/V/II. Doc.48/15, 31 diciembre 2015. Recuperado en http://www.oas.org/es/cidh/expresion/docs/informes/odio/Discurso_de_odio_incitacion_violencia_LGTBI.pdf. http://www.oas.org/es/cidh/expresion/docs/informes/odio/Discurso_de_odio_incitacion_violencia_LGTBI.pdf*



Ap

Conservar la dinámica abierta de Internet es preservar una plataforma para mejorar el discurso democrático, facilitar la organización y la acción política, además de proveer un ambiente descentralizado para la interacción social, cultural y política en el cual todos pueden participar. La neutralidad de la red aporta a este propósito al preservar la infraestructura abierta donde hay competencia entre proveedores y libertad de elección para las personas. En ese contexto analice los siguientes planes de acceso a Internet:

1. Sobre las ofertas de Whatsapp, Facebook o Twitter gratis, que son comunes en los planes de acceso a Internet móvil en Colombia, analice si el ofrecer cierto tráfico gratuito constituye un trato diferencial respecto a otro tráfico no favorecido y si ese trato es legítimo o constituye una violación a la neutralidad de la red. Recuerde que el tráfico no favorecido no es bloqueado o ralentizado.
2. Analice a la luz de la neutralidad de la red, los siguientes dos planes de acceso a Internet por celular de dos empresas diferentes: (1) Un plan de "beneficios premium" para sus clientes en postpago que incluye "música ilimitada" de donde se puede elegir entre 5 aplicativos seleccionados por esa empresa y el consumo de la aplicación seleccionada no afectará el consumo de datos del plan. (2) Un plan de que ofrece gratis a sus clientes el uso de aplicaciones de música en streaming. El plan ofrece 30 opciones para elegir y está abierta a incluir cualquiera que cumpla una serie de requisitos.



Lea el siguiente caso y resuelva las preguntas al final.

Hostallnn es un servicio que permite a las personas encontrar alojamiento a un menor precio que los hoteles convencionales. El alojamiento es ofrecido por otras personas particulares. Hostallnn se queda con un margen del precio pagado por el huésped y su plataforma está disponible en Internet como una aplicación para Android y iOS, así como en un sitio web. Hostallnn no tiene una oficina en Colombia.

El gremio hotelero se ha estado manifestando en contra de la plataforma y solicita a las autoridades tomar acciones contra Hostallnn. El Ministerio de Industria, Cultura y Turismo considera que el servicio ofrecido por Hostallnn no cumple con los requisitos que imponen las leyes y reglamentos vigentes sobre el servicio de hotelería y turismo en el país y solicita el bloqueo de la plataforma en el país.

El Ministerio de las Tecnologías de la Información y las Comunicaciones afirma que no es posible tomar acciones respecto a la plataforma puesto que el principio de neutralidad de la red, tal y como está consagrado en la normativa vigente, sólo permite el bloqueo de contenido ilegal.

Teniendo en cuenta esta situación, responda las siguientes preguntas:

Desde el punto de vista del Ministerio de Comercio, Industria y Turismo ¿qué tipo de acción presentaría y ante qué juez, para solicitar el bloqueo de Hostallnn? ¿Cómo argumentaría la petición? Concretamente, ¿cómo argumentaría que la plataforma de un servicio de intermediación hotelera ilegal debe ser considerado ilegal también en Internet?

Desde el punto de vista del Ministerio de las TIC, ¿cómo defiende la legalidad de la plataforma, independientemente del cumplimiento de los requisitos legales para el servicio que presta Hostallnn?

Desde el punto de vista del juez que recibe la causa, ¿accedería a la petición de bloqueo o cualquier otra relacionada con el tráfico de Internet? ¿A quién dirige la orden, en caso de acceder a alguna solicitud? ¿Considera necesario que la legislación vigente establezca expresamente que un servicio que no cumple con la reglamentación correspondiente es ilegal, para efectos de la legislación sobre neutralidad de la red?

Independientemente de la posición de los distintos actores en este caso:

¿Considera que una empresa como Hostallnn es un simple intermediario de Internet o presta el servicio de hotelería y turismo? Como simple intermediario ¿estaría sujeto a la regulación de la actividad que intermedia o estas reglas no aplicarían a la empresa?

¿Qué papel considera que juegan las tiendas de aplicaciones (Google Play de Google o App Store de Apple)? ¿Podrían también ellas ser objeto de una orden judicial de retirada de la plataforma ilegal?



J

Jurisprudencia

- Corte Constitucional, Sentencia T-063A de 2017. MP. Jorge Iván Palacio Palacio. Salvamento de Voto Aquiles Arrieta Gómez
- Sala de Casación Penal, Sentencia del 23 de septiembre de 2009, M.P. Julio Enrique Socha Salamanca;
- Corte Constitucional de Colombia (2008), Sentencia T-496, M.P. Jaime Córdoba Triviño;
- Corte Constitucional de Colombia (2011, 8 de noviembre), Sentencia T-843, M.P. Jorge Ignacio Pretelt Chaljub.

B

- CASTAÑEDA, J.D. y GONZÁLES, L. Fundación Karisma, "Neutralidad de la red y ofertas comerciales en Colombia, análisis de la regulación", Bogotá, 2017, Disponible en: <https://karisma.org.co/fundacion-karisma-publica-informe-sobre-neutralidad-de-la-red-en-colombia/> Curso Avanzado para Jueces y Operadores Jurídicos en las Américas". Propuesta curricular y materiales de estudio. Elaborado por Catalina Botero, Federico Guzmán, Sofía Jaramillo y Salomé Gómez para De Justicia con el apoyo de Open Society Foundations (osf). 2017, Disponible en: <https://www.dejusticia.org/wp-content/uploads/2017/05/Gui%CC%81a-Curricular-Versio%CC%81n-Final.pdf> <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf>
- BOTERO, C., GUZMÁN. F., JARAMILLO, S., y GÓMEZ, S. "El Derecho a la Libertad de Expresión. Curso Avanzado para Jueces y Operadores Jurídicos en las Américas". Propuesta curricular y materiales de estudio. Elaborado para De Justicia con el apoyo de Open Society Foundations (OSF). 2017, Disponible en: <https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf>
- Comisión de Regulación de Comunicaciones, Neutralidad de Internet, informe técnico (2011): 5, https://www.crcom.gov.co/es/recursos_user/Actividades%20Regulatorias/Neutralidad_Internet/Documento_Soporte.pdf
- DICKINSON, J., LEVIN, E. & PETTALIA, J.L. (2013). Cyberbullying: Eliciting harm without consequence. Computers in Human Behavior. 29(6), pp. 2758–2765. DOI: 10.1016/j.chb.2013.07.020



5. CASO INTEGRADO INTEGRADOR

Teniendo como fundamento la sentencia T-227 de 2015 de la Corte Constitucional, se propone el siguiente caso integrado-integrador, que ejemplifica la importancia de la comprensión de algunas características técnicas del funcionamiento de Internet para los operadores de justicia, las tensiones de derechos y de estos frente a las potestades estatales, así como el reto de pensar las competencias jurisdiccionales nacionales en relación con una red de comunicación que opera de modo descentralizado y cuyos elementos y capas se encuentran diseminados globalmente.

El señor Rafael María Castro era propietario de una próspera agencia de viajes. El mejor cliente de la agencia le compraba habitualmente pasajes aéreos para viajes intercontinentales que, ordinariamente, eran emitidos a nombre de mujeres, según requerimiento del comprador.

En el año 1999 varios medios de prensa nacionales e internacionales registraron la captura tanto del comprador habitual como del señor Castro, quienes fueron vinculados por la Fiscalía a un proceso penal imputados de pertenecer a una red de tráfico de personas.

El proceso al que fue vinculado culminó por prescripción de la acción penal.

Quince años luego de la ocurrencia de los hechos, el registro de la noticia sigue disponible en Internet, sin que haya alguna nota posterior que informe sobre la prescripción de la acción penal, lo cual afecta al señor Castro en la medida en que, al ingresar su nombre completo en el motor de búsqueda Google, su nombre aparece todavía como primera entrada en la noticia publicada por el diario *El Tiempo* y, en segundo lugar, por el diario *La Vanguardia*, de España, sin que haya seguimiento alguno posterior a la noticia que lo afecta, lo cual perjudica enormemente su reputación ante entidades financieras y en la búsqueda de trabajo.

El señor Castro ya se puso en contacto con el periódico *El Tiempo*, al que mediante derecho de petición le solicitó la eliminación del contenido, sin haber obtenido respuesta satisfactoria, pues el medio sostiene que la noticia es veraz e imparcial. El diario *La Vanguardia* ha guardado silencio ante similar petición por vía electrónica.



Con base en los hechos narrados, el señor Castro instauró una acción de tutela en la que le solicita a la jurisdicción constitucional que le ordene al diario El Tiempo y a La Vanguardia borrar la noticia. De igual manera, le solicitó a Google la desindexación de la noticia. La empresa respondió que su solicitud debía elevarla ante la sede de la empresa en el Estado de California, en los Estados Unidos de América.

Con base en el caso hipotético planteado:

- ¿Cuál es la jurisdicción competente para conocer de las pretensiones del señor Castro? ¿Por qué?
- ¿Cómo resolvería la tensión existente entre el derecho al buen nombre del accionante y las garantías constitucionales a la libertad de prensa?
- ¿Cuáles son las implicaciones del caso, si las hay, en materia de habeas data?
- ¿Cuáles son las implicaciones del caso, si las hay, en relación con la neutralidad de la red?
- Si decide el que el caso amerita la restricción a la libertad de expresión, ¿qué tipo de medidas considera que son proporcionales al tiempo que conservan la neutralidad de la red?
- Si decide que el caso amerita el bloqueo o filtrado de contenido, ¿cómo y a quién impartiría la orden?



6. BIBLIOGRAFÍA GENERAL

- Blum, A. (2013). Tubos en busca de la geografía física de Internet. (E. Mercado, Trad.).
- Castañeda, J.D. (2016) “¿Es legítima la retención de datos en Colombia?, análisis comparativo de una herramienta de vigilancia masiva que restringe los derechos humanos”. Fundación Karisma. Disponible en <https://karisma.org.co/es-legitima-la-retencion-de-datos-en-colombia-2/>
- Castañeda, J.D. (2017) “Un rastreador en tu bolsillo”, Fundación Karisma. Disponible en: <https://homascelusvigilados.karisma.org.co/>
- CIDH, Informe No. 11/96. Caso No. 11.230. Francisco Martorell vs. Chile. 1996.
- Consejo de Derechos Humanos de las Naciones Unidas (2012, 29 de julio). *Promoción, protección y disfrute de los derechos humanos en Internet*. A/HRC/20/L.13. Recuperado en http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf
- Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. A/HRC/32/38. 11 de mayo de 2016
- Cortés, C. Vigilancia de las comunicaciones en Colombia, Bogotá, De justicia. Disponible en: <https://www.dejusticia.org/publication/vigilancia-de-las-comunicaciones-en-colombia-el-abismo-entre-la-capacidad-tecnologica-y-los-controles-legales/>
- Dickinson, J., Levin, E. & Pettalia, J.L. (2013). Cyberbullying: Eliciting harm without consequence. *Computers in Human Behavior*. 29(6), pp. 2758–2765. DOI: 10.1016/j.chb.2013.07.020.
- Doria, A. (2014). Use [and Abuse] of Multistakeholderism in the Internet. In *The Evolution of Global Internet Governance* (pp. 115-138). Springer, Berlin, Heidelberg.
- EDRI (s.f.). ¿Cómo funciona Internet? *The EDRI Paper*. 3a. edición, p. 3. Recuperado de http://www.edri.org/files/paper03_20120725_02_esp.pdf http://www.edri.org/files/paper03_20120725_02_esp.pdf
- Grupo de Trabajo sobre la Sociedad de la Información (2013). *Declaración Conjunta sobre la Agenda para el Desarrollo Post-2015*. Recuperado en <http://www.ungis.org/Portals/0/documents/JointInitiatives/UNGIS.Joint.Statement.pdf> <http://www.ungis.org/Portals/0/documents/JointInitiatives/UNGIS.Joint.Statement.pdf>



TIC Y DERECHOS HUMANOS

- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 mayo 2016.
- La Rue, Frank, "Report of the Special Rapporteur on freedom of opinion and expression", (2011, 6 May). A/HRC/17/27. Recuperado en http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Lessig, Lawrence, (2009) *El código 2.0*, Madrid, Traficantes de sueños.
- Malcolm, J. (2008). Multi-stakeholder governance and the Internet Governance Forum. Terminus Press
- Mueller, M. (2010). Networks and states: the global politics of Internet governance. Cambridge, Mass: MIT Press.
- OECD (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing. Recuperado en <http://dx.doi.org/10.1787/9789264115644-en>
- Peña Ochoa, P. (2013), ¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. *Guía para periodistas*, Santiago, ONG Derechos Digitales.
- Privacy International. Case Study: Super-Apps and the Exploitative Potential of Mobile Applications. Disponible en: <https://www.privacyinternational.org/node/789>
- RedPaTodos, "Sobre la gobernanza en Internet". Recuperado en https://www.youtube.com/watch?v=HU2Vbo_SxIs
- Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos CIDH; "Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión", 30 de diciembre de 2009. Disponible en <http://www.oas.org/es/cidh/expresion>
- Rodríguez, Katitza, "Análisis comparativo de las leyes y prácticas de vigilancia en Latinoamérica", disponible en <https://necessaryandproportionate.org/es/an%C3%A1lisis-comparado-de-las-leyes-y-pr%C3%ADcticas-de-vigilancia-en-latinoam%C3%A9rica> <https://necessaryandproportionate.org/es/an%C3%A1lisis-comparado-de-las-leyes-y-pr%C3%ADcticas-de-vigilancia-en-latinoam%C3%A9rica>
- Savage, J. E., & McConnell, B. W. (2015). Exploring Multi-Stakeholder Internet Governance. Brown University Bruce W. McConnell, EastWest Institute
- Wagstaff, Keith, "You are not an IP address, rules judge", TIME, Mayo 7 de 2012. Recuperado de: <http://techland.time.com/2012/05/07/you-are-not-an-ip-address-rules-judge/> <http://techland.time.com/2012/05/07/you-are-not-an-ip-address-rules-judge/>



Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Escuela Judicial
"Rodrigo Lara Bonilla"



@escuelajudicialrlb



@Ejrlbnet



@EJRLB



@escuelajudicial_rlb

<https://escuelajudicial.ramajudicial.gov.co/>