EXAMINANDO LOS DERECHOS Y LAS LIBERTADES EN INTERNET EN LATINOAMÉRICA (EXLILA)

INFORME NACIONAL COLOMBIA

Juan Diego Castañeda y Amalia Toledo
FUNDACIÓN KARISMA*

RESUMEN EJECUTIVO

Aunque Colombia tiene retos para garantizar el acceso a internet a toda la población, este medio se ha convertido en una herramienta esencial para el desarrollo de muchas actividades y el ejercicio de derechos fundamentales como la libertad de expresión y el acceso al conocimiento.

La legislación y jurisprudencia aplicable a internet no ha sido sistemática y muchas veces tiene importantes consecuencias para que internet siga siendo una herramienta libre y abierta. El principio de neutralidad de la red, por ejemplo, está desarrollado de tal manera que permite la creación de planes diferenciados según el mercado,

* En un esfuerzo para que todas las personas tengan acceso al conocimiento, la Fundación Karisma está trabajando para que sus documentos sean accesibles, es decir, tengan un formato electrónico diseñado para que su contenido pueda ser leído por el mayor número de personas posible, incluidas las que tienen algún tipo de discapacidad o de dificultad para la lectura y comprensión. Más información sobre el tema: www.documentoaccesible.com/#que-es

APC
ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

Este informe se ha elaborado como parte del proyecto Examinando los derechos y las libertades en internet en Latinoamérica (EXLILA) de la Asociación para el Progreso de las Comunicaciones (APC).
El proyecto está financiado por Open Society Institute (OSI) y APC y está coordinado por la ONG Derechos Digitales.

lo que en la práctica puede implicar el desconocimiento de este principio. Las normas sobre vigilancia de las comunicaciones, por otro lado, aunque importantes para la investigación criminal, no cuentan con los debidos contrapesos y controles judiciales, ni obedecen a un análisis serio de necesidad y proporcionalidad, como es el caso de las facultades que tienen los organismos de inteligencia. Finalmente, aunque no hay sistemas de filtrado de internet, existe un régimen de bloqueo de pornografía infantil que, a pesar de perseguir fines enteramente necesarios, carece de controles y de la posibilidad de ejercer el derecho a la defensa.

Los casos problemáticos demuestran que todavía falta mucho camino por recorrer en la aplicación de las normas existentes a situaciones ocurridas en la red. En un caso, un comentarista de una noticia en línea es condenado a prisión y multa por el delito de injuria. En otro, un estudiante está siendo procesado por violación a derechos de autor por compartir en una plataforma digital un material académico previamente publicado en internet.

Sin embargo, los casos más relevantes tienen que ver con el uso ilegítimo de herramientas de vigilancia. Se han producido condenas contra ex funcionarios del gobierno y de organismos de seguridad por interceptar ilegalmente comunicaciones de magistrados de altas cortes, líderes de oposición y periodistas. Un asesor de una campaña para las elecciones presidenciales aceptó cargos por interceptación ilegal de comunicaciones de funcionarios y demás actores involucrados en los diálogos de paz con la guerrilla de las Fuerzas Armadas Revolucionarias de Colombia (FARC). Finalmente, investigaciones de organizaciones internacionales descubren sistemas de vigilancia de las comunicaciones y hackeo previamente ocultos a la opinión pública.

Ante este panorama, es cada vez más apremiante la necesidad de considerar normas internacionales de derechos humanos para los entornos digitales; fortalecer las capacidades judiciales, especialmente en lo relacionado con la comprensión de internet; desarrollar e implementar modelos de participación en la construcción de políticas y normas en torno a internet, que garanticen el involucramiento de la sociedad civil, la academia y la comunidad técnica por igual; y promover el seguimiento por parte de la sociedad civil de desarrollos legislativos, judiciales y administrativos que afecten a la red.

En este informe hacemos un rápido recorrido a través de la normativa vigente y los casos –judiciales y mediáticos– más relevantes que afectan, tanto positiva como negativamente, el ejercicio de los derechos humanos de la ciudadanía colombiana. En este sentido, revisamos normativas sobre la neutralidad de la red, delitos informáticos, protección de la infancia, actividades de investigación criminal y de inteligencia, de retención de datos y anonimato, destacando los problemas que muchas de estas normas presentan frente a la protección de los derechos fundamentales. También vemos algunos de los casos judiciales o reportados en medios de comunicación más emblemáticos, que servirán de testimonio para mostrar que aún falta mucho por recorrer para el reconocimiento y protección de internet como un espacio de ejercicios de derechos y libertades. Finalmente, presentaremos algunas recomendaciones que tienen como fin impulsar el potencial democratizador y de empoderamiento de la ciudadanía a través del acceso y uso de la red.

INTRODUCCIÓN

La primera experiencia de internet en Colombia se remonta al año 1988 con la creación de un red interna montada por la Universidad de los Andes[1]. Ya para el inicio de la década de los 90, se consiguió la primera interconexión de entre varias universidades colombianas con la Universidad de Columbia en los Estados Unidos. A partir de ahí, la expansión de internet en el territorio ha sido imparable y constante.

Hoy día, internet se ha convertido en una herramienta indispensable para la sociedad colombiana. Si bien siguen existiendo retos de conectividad de acceso a esta red en el territorio nacional, es indiscutible que la vida cotidiana depende, en gran medida, de la interacción y actividades en línea que nos permiten tener una voz muchas veces vedada en espacios físicos, aumentar nuestros ingresos, conectarnos con amistades, familiares, colegas y hasta con el gobierno, adquirir bienes y servicios en línea, convertirnos en generadores de contenidos, y un gran etcétera. El ciberespacio se ha convertido en un lugar para la participación política y ciudadana, para el ejercicio de derechos humanos jamás antes visto.

Esta evolución no ha estado exenta de retos sociales, tecnológicos, legales y judiciales. Abordar estos desafíos, en múltiples ocasiones, ha puesto en peligro el ejercicio mismo de los derechos humanos. Estamos ante una herramienta que todos los días nos permite crear nuevas formas de interactuar en todas las fases de nuestra vida y eso, de una parte, requiere de un proceso de prueba y error. También demanda una actualización y revisión continua de nuestro conocimiento y entendimiento de las prácticas emergentes, de las tecnologías y aplicaciones que se están desarrollando incesantemente, y la adecuación de normas y doctrinas jurídicas que son obsoletas ante esta nueva realidad.

En este informe hacemos un rápido recorrido a través de la normativa vigente y los casos –judiciales y mediáticos– más relevantes que afectan, tanto positiva como negativamente, el ejercicio de los derechos humanos de la ciudadanía colombiana. En este sentido, revisamos normativas sobre la neutralidad de la red, delitos informáticos, protección de la infancia, actividades de investigación criminal y de inteligencia, de retención de datos y anonimato, destacando los problemas que muchas de estas normas presentan frente a la protección de los derechos fundamentales. También vemos algunos de los casos judiciales o reportados en medios de comunicación más emblemáticos, que servirán de testimonio para mostrar que aún falta mucho por recorrer para el reconocimiento y protección de internet como un espacio de ejerciciosde derechos y libertades. Por último, presentaremos algunas recomendaciones que tienen como fin impulsar el potencial democratizador y de empoderamiento de la ciudadanía a través del acceso y uso de la red.

1 Cobos, T. (2010, 12 enero). Historia de internet en el mundo y su llegada a Colombia. *Tania Lu, mi blog*. tanialu.co/2010/01/12/historia-de-internet-en-el-mundo-y-su-llegada-a-colombia/#sthash.h2jz9Z8t.dpuf

MARCO NORMATIVO GENERAL

En Colombia se reconoce el derecho de cualquier persona a la libertad de expresión y a la protección de su intimidad personal y familiar y el derecho a la autodeterminación informativa, o *habeas data*[2]. Algunos instrumentos internacionales de derechos humanos relevantes que ha suscrito Colombia son:

- Declaración americana de los derechos y deberes del hombre de 1948
- Declaración universal de los derechos humanos
- Pacto internacional de derechos civiles y políticos
- Convención americana sobre derechos humanos – Pacto de San José de Costa Rica
- Convención sobre los derechos del niño
- Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares
- Convención internacional sobre los derechos de las personas con discapacidad
- Convención para la eliminación de todas la formas de discriminación contra las mujeres y su protocolo opcional.

La jurisprudencia constitucional ha analizado en incontables ocasiones conflictos entre el derecho a la libertad de expresión y otros derechos fundamentales como la honra y el buen nombre, así como violaciones al derecho a la intimidad. En general, se reconoce la aplicación de los derechos fundamentales en el entorno digital, en las mismas condiciones que por fuera de él.

NEUTRALIDAD DE LA RED

No existe en Colombia una regulación integral de internet. Se puede destacar, en todo caso, la existencia del Plan Nacional de Desarrollo, que en su artículo 56, establece que los prestadores de servicios de internet (PSI) "no podrán bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario [sic] de internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de internet"[3]. Sin embargo, al final del inciso, se permite a los prestadores "hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios [sic] de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación".

Esa excepción fue llevada al extremo en la Resolución No. 3502 de 2011[4] de la Comisión de Regulación de Comunicaciones, ente regulador de las telecomunicaciones. En ella se dice que se "podrán ofrecer planes de acceso a internet donde se limite el acceso a tipos genéricos de servicios, contenidos o aplicaciones". El resultado es la proliferación de planes de internet que acogen la modalidad de *zero-rating*[5], siendo el más famoso de ellos, Internet.org de Facebook, hoy conocido como FreeBasic.org (véase la sección Casos problemáticos).

DELITOS INFORMÁTICOS

Existen precedentes sobre la aplicación de varios tipos penales a conductas a través de internet (véase la sección Casos problemáticos). También la legislación penal establece algunos delitos específicamente relacionados con tecnologías de información y comunicación, que fueron introducidos en 2009[6]. La reforma incluyó varios delitos en el Código Penal, tales como el acceso abusivo a un sistema informático, la interceptación de datos informáticos o el uso de software malicioso.

BLOQUEO DE PORNOGRAFÍA INFANTIL

Colombia no ha implementado ninguna regulación específica sobre bloqueos o filtrado de contenidos en internet, siendo la única excepción la pornografía infantil. La Ley No. 679 de 2001[7] y el Decreto No. 1524 de 2002[8] establecen que una división de la Policía Nacional está facultada para revisar contenido digital denunciado por pornografía infantil y determina si califica o no para ser bloqueado. En caso de serlo, las URL son notificadas al Ministerio de las Tecnologías de la Información y las Comunicaciones, que

2 Constitución Política. (1991). Artículos 15, 16 y 20. www.constitucioncolombia.com/titulo-2/capitulo-1

3 Ley No. 1450. (2011). *Plan Nacional de Desarrollo 2010-2014*. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101

4 www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45061

5 https://es.wikipedia.org/wiki/Zero-rating

6 Ley No. 1273. (2009). *Ley de delitos informáticos.* www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

7 www.mintic.gov.co/portal/604/articles-3685_documento.pdf

8 www.mintic.gov.co/portal/604/articles-3554_documento.pdf

a su vez notifica a los PSI, quienes proceden a ejecutar el bloqueo. Los criterios de bloqueo de pornografía infantil son fijados por una comisión compuesta por el Instituto Colombiano de Bienestar Familiar, la Defensoría del Pueblo, la Fiscalía General de la Nación y representantes de UNICEF.

No hay norma alguna que obligue a las autoridades a avisar a la persona afectada. Esta medida tampoco se ejecuta bajo supervisión judicial. La página bloqueada debe llevar a un aviso sobre el hecho mismo del bloqueo por contenido de pornografía infantil y debe notar la existencia de la Ley No. 679 de 2001.

VIGILANCIA DE LAS COMUNICACIONES

El régimen de vigilancia de las comunicaciones en Colombia abarca la interceptación, la retención de datos de tráfico y la situación legal de uso del cifrado. Veamos.

Interceptación

La interceptación de comunicaciones solo puede efectuarse cuando hay una ley que la permite, siguiendo las reglas que ella establezca y con control judicial[9]. En Colombia, el único organismo autorizado para ordenar la interceptación es la Fiscalía General de la Nación, que es la encargada de la investigación criminal y de acusar ante la justicia a quienes puedan ser señalados de cometer un crimen. En el artículo 250 de la Constitución se lee que

> La Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento […y deberá] 2. Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis horas siguientes[10].

Las mismas atribuciones aparecen en el Código de Procedimiento Penal (CPP). Específicamente, la Fiscalía puede retener, inspeccionar y devolver correspondencia, interceptar comunicaciones que transiten por cualquier medio, retener y aprehender dispositivos para recuperar información dejada al navegar por internet u otros medios tecnológicos y hacer búsquedas selectivas en bases de datos[11]. De todas estas actividades, solo la búsqueda selectiva en bases de datos requiere autorización previa del Juez de Control de Garantías. Las demás actividades se realizan bajo órdenes de la Fiscalía y, posteriormente, son revisadas por el mismo Juez de Control de Garantías bajo criterios de legalidad, necesidad y proporcionalidad. En caso de que el juez declare la legalidad de las actividades, la información recuperada puede ser usada en el proceso penal.

La Corte Constitucional ha entendido que la interceptación de comunicaciones y similares tienen un componente de urgencia que justifica el hecho de que la audiencia de control de garantías tenga lugar después de efectuada la actividad[12]. Por ejemplo, la búsqueda selectiva en bases de datos requiere audiencia previa de autorización porque, como los datos no están bajo control de la persona investigada, no hay urgencia.

Ninguna de las normas que rige el procedimiento penal requiere que la persona sujeta a una medida probatoria que afecta el derecho a su intimidad sea notificada. Sin embargo, la audiencia de control de garantías (donde se legaliza la medida y sus resultados) no es secreta y la persona investigada no tiene ninguna restricción para asistir a ella. En todo caso, es posible entender que estas notificaciones son necesarias a partir de la existencia del principio y derecho fundamental al debido proceso[13].

Inteligencia

Aunque no tienen facultades expresas para interceptar comunicaciones, los organismos de inteligencia pueden, según el artículo 17 de la Ley de actividades de inteligencia y contrainteligencia[14], "monitorear el espectro electromagnético". La Corte Constitucional, al examinar este punto, entendió que

> el monitoreo del espectro electromagnético, como actividad comprendida dentro del ámbito de la inteligencia y contrainteligencia, consiste en llevar a cabo una labor de rastreo de forma aleatoria e indiscriminada. Ello implica la captación incidental de comunicaciones en las que se revelan

9 Constitución Política. (1991). Artículo 15. www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

10 Constitución Política. (1991). Artículo 250. www.constitucioncolombia.com/titulo-8/capitulo-6/articulo-250

11 Código de Procedimiento Penal. Artículos 233-236 y 244. perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf

12 Corte Constitucional de Colombia. (2007). Sentencia C-336. www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

13 Constitución Política. (1991). Artículo 29. www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-29

14 Ley No. 1621. (2012). *Ley de actividades de inteligencia y contrainteligencia*. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=52706

> circunstancias que permiten evitar atentados y controlar riesgos para la defensa y seguridad de la Nación. Técnicamente se estaría ante una especie de rastreo de sombras, imágenes y sonidos representados en frecuencias de radiación electromagnética y ondas radioeléctricas. Monitorear no es interceptar[15].

Aún así, no está claro por qué monitorear no implica interceptar comunicaciones si en cualquier caso ellas son "captadas" y del monitoreo puede llegar a conocerse "circunstancias que permiten evitar atentados y controlar riesgos". Tampoco está claro si internet puede ser monitoreado en estos mismos términos. Todavía no se han presentado casos ante las autoridades judiciales donde se haya interpretado el alcance de esta facultad.

Retención

Existe la retención obligatoria de datos de tráfico de comunicaciones establecida para servir en la investigación criminal y el desarrollo de actividades de inteligencia. Para la investigación criminal, el Decreto No. 1704 de 2012 obliga a los proveedores de redes y servicios de telecomunicaciones a retener y entregar a la fiscalía, cuando lo solicite, los datos del suscriptor y los datos de ubicación de los dispositivos[16]. La Ley de inteligencia y contrainteligencia, por su parte, obliga a los proveedores a retener y entregar a los organismos de inteligencia "el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores", así como toda la información que permita la localización de los dispositivos[17].

Ninguna de las dos formas de retención tiene control judicial y no está claro si opera solo sobre telefonía móvil y fija, o si también aplica para datos de internet. Tampoco hay un catálogo de delitos cuya investigación amerite usar la medida.

Cifrado y anonimato

No hay una prohibición general para la expresión anónima. Sin embargo, hay que hacer dos precisiones. Primero, en la Resolución No. 3067 de 2011[18] de la Comisión de Regulación de Comunicaciones se definieron los principios que los proveedores deben cumplir en lo relacionado a la seguridad de sus redes, siguiendo las recomendaciones pertenecientes a las series X.800[19] de la Unión Internacional de Telecomunicaciones. En el mismo sentido, las entidades bancarias tienen el deber de asegurar sus comunicaciones.

Segundo, a pesar de lo anterior, la Ley No. 418 de 1997[20], en su artículo 102, prohíbe "enviar mensajes en lenguaje cifrado o ininteligible" a las personas usuarias de "equipos de comunicaciones que utilizan el espectro electromagnético". El alcance de esta norma no es claro y no conocemos de la existencia de casos donde haya sido sancionado alguien, de alguna forma, por haber usado métodos de cifrado de comunicaciones o de información.

15 Corte Constitucional de Colombia. (2012). Sentencia C-540. www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

16 Decreto 1704. (2014). Artículos 4 y 5. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=48863

17 Ley No. 1621. (2012). Ley de actividades de inteligencia y contrainteligencia, artículo 44. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=52706

18 www.asomovil.org/wp-content/uploads/2015/02/Resoluci%C3%B3n-No.-3067-de-2011-Indicadores-de-calidad-en-Telecomunicaciones.pdf

19 https://es.wikipedia.org/wiki/X.800

20 www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6372

CASOS PROBLEMÁTICOS

VIGILANCIA DE LAS COMUNICACIONES

En 2009 se conoció que el antiguo organismo de inteligencia del Estado –el Departamento Administrativo de Seguridad (DAS)– siguió ilegítimamente las comunicaciones privadas de magistrados de altas cortes, periodistas y líderes de oposición[21]. El caso, conocido como "Chuzadas", fue investigado penalmente y la justicia condenó, entre otros, a la ex directora del DAS y al ex secretario del ex presidente Álvaro Uribe por el delito de interceptación ilegal de comunicaciones[22]. Se desconoce con exactitud el papel que jugó internet en todo el asunto, pero es posible que las comunicaciones digitales de las víctimas hayan sido interceptadas, porque los organismos de seguridad cuentan con las capacidades técnicas para hacerlo.

En febrero de 2014 se conoció la existencia de una fachada de inteligencia militar desde la que, presuntamente, se interceptaron los correos electrónicos de las personas representantes del gobierno y las FARC que hacen parte de los diálogos de paz que tienen lugar actualmente en La Habana, Cuba[23]. El nombre de la operación encubierta era "Andrómeda" y por ese mismo nombre se conoce el escándalo en los medios. Luego de conocido el caso, 20 miembros de las fuerzas militares fueron relevados y 5 fueron destituidos[24]. Hasta ahora solo se ha capturado a algunos efectivos, pero no hay condenas y el fondo del caso aún está por establecerse[25].

A mediados de 2014, y en medio de la campaña electoral presidencial, se conoció que el ex candidato Óscar Iván Zuluaga había contratado los servicios de un supuesto experto en informática que le proveía información confidencial sobre el proceso de paz con el fin de hacer más efectiva su campaña[26]. Andrés Sepúlveda, el supuesto experto, aceptó finalmente los cargos por el delito de interceptación de comunicaciones personales, entre otros[27]. Las investigaciones contra otras personas involucradas por este hecho avanzan lentamente.

A mediados de 2015 se filtró una gran cantidad de información de la empresa italiana *Hacking Team*[28], que permitió descubrir que la Dirección Nacional de la Policía de Colombia (DIPON) había tenido acercamientos con la empresa y había adquirido algunos de sus productos, específicamente el programa "Galileo", un software malicioso con la capacidad de infectar equipos y obtener información de ellos, así como encender remotamente el micrófono o la cámara web[29]. Aunque no hay pruebas concretas que indiquen casos donde haya sido usado este software, recientemente algunos periodistas denunciaron seguimientos ilegales en su contra, cuyo objetivo, supuestamente, era alejarlos de las investigaciones sobre corrupción dentro de la Policía que estaban adelantando[30]. Uno de los periodistas contó que de su computador personal se borraba información sobre la que estaba trabajando, e incluso en una ocasión el puntero del ratón empezó a moverse solo[31]. Al respecto, el gobierno creó

21 Revista Semana. (2009, 21 febrero). El DAS sigue grabando. Revista Semana. www.semana.com/nacion/articulo/el-das-sigue-grabando/100370-3

22 El Tiempo. (2015, 30 abril). Condena de 14 años para Hurtado y 8 para Bernardo Moreno por chuzadas. *El Tiempo*. www.eltiempo.com/politica/justicia/caso-chuzadas-del-das-condena-a-maria-del-pilar-hurtado-y-bernardo-moreno/15660280

23 Revista Semana. (2014, 8 febrero). ¿Alguien espió a los negociadores de La Habana? *Revista Semana*. www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

24 Blu Radio. (2015, 23 enero). Purga en inteligencia de las Fuerzas Militares por escándalo de Andrómeda. *Blu Radio*. www.bluradio.com/88548/purga-en-inteligencia-de-las-fuerzas-militares-por-escandalo-de-andromeda

25 El Espectador. (2014, 5 octubre). Legalizan captura de tres uniformados del Ejército por caso Hacker. *El Espectador*. www.elespectador.com/noticias/judicial/legalizan-captura-de-tres-uniformados-del-ejercito-caso-articulo-520717

26 Revista Semana. (2014, 17 mayo). El video del 'hacker' y Zuluaga. *Revista Semana*. www.semana.com/nacion/articulo/el-video-del-hacker-con-oscar-ivan-zuluaga/388438-3

27 Revista Semana. (2015, 123 febrero). Juez avaló preacuerdo entre Fiscalía y el hacker Sepúlveda. *Revista Semana*. www.semana.com/nacion/articulo/caso-hacker-juez-avalo-preacuerdo-con-andres-sepulveda/417779-3

28 Hern, A. (2015, 6 julio). Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. *The Guardian*. www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

29 Botero, C., & Sáenz, P. (2015, 24 agosto). En Colombia, el PUMA no es como lo pintan. *Digital Rights Latin America and the Caribbean*. www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan

30 Jiménez Herrera, J. (2015, 4 diciembre). "No hay duda de los seguimientos": Vicky Dávila. *El Espectador*. www.elespectador.com/noticias/judicial/no-hay-duda-de-los-seguimientos-vicky-davila-articulo-603572

31 Vélez, L. (2015, 6 diciembre). El precio de denunciar. *El Espectador*. www.elespectador.com/opinion/el-precio-de-denunciar

una comisión para la investigación del caso[32] y la Fiscalía General de la Nación abrió formalmente una investigación que aún está en desarrollo[33].

INVESTIGACIONES DE *PRIVACY INTERNATIONAL*

En agosto de 2015 la organización británica *Privacy International* publicó dos reportes sobre el estado de los sistemas de vigilancia de las comunicaciones en Colombia[34]. La conclusión general es que existen sistemas de vigilancia con distintos grados de supervisión y control. La Fiscalía General de la Nación controla un sistema llamado Esperanza, que supuestamente solo tiene capacidad para interceptar un número limitado de líneas de celular. Hacia 2007, se conoció que la Policía Nacional estaba adquiriendo equipos de vigilancia de las comunicaciones dentro de un programa llamado Plataforma Única de Monitoreo y Análisis (PUMA), cuyas capacidades de vigilancia no estaban del todo claras aunque, de un modo u otro, incluirían internet. A mediados de 2014, la Fiscalía General declaró públicamente que estaba tomando control de los equipos que conformarían el sistema PUMA porque no encontraba las garantías suficientes para que esos equipos no fueran usados abusivamente y porque es el único organismo autorizado para interceptar comunicaciones privadas[35]. A pesar de la falta de controles al uso de sistemas de interceptación, la Policía anunció que empezaría pruebas para el uso de los equipos de PUMA en octubre de 2015[36].

El último sistema de vigilancia es el Sistema Integrado de Grabación Digital (SIGD), a cargo de la Dirección de Inteligencia de la Policía Nacional (DIPOL) y con capacidad para interceptar y monitorear comunicaciones a través de teléfonos celulares y mensajes de texto. No está claro si a través de este sistema las autoridades tienen capacidades tecnológicas para monitorear el tráfico de internet.

Finalmente, y gracias a la revelación de datos de la empresa italiana *Hacking Team*, se está conociendo que la Policía Nacional podría haber contratado la adquisición de herramientas que tendrían la capacidad de interceptar comunicaciones privadas digitales[37]. Sin embargo, esto aún es materia de investigación.

LIBERTAD DE EXPRESIÓN Y NEUTRALIDAD DE LA RED

'Derecho al olvido'

Otro caso relevante está relacionado con una tutela que presentó una ciudadana contra el periódico El Tiempo y Google, pues al hacer una búsqueda de su nombre, encontraba un resultado donde aparecía relacionada con la comisión de un delito. La Corte Constitucional decidió proteger el derecho al buen nombre y honra de la ciudadana y ordenar al periódico a mantener actualizadas las noticias judiciales, pero también dificultar la búsqueda del enlace de la nota donde aparece el nombre de la persona en motores de búsqueda como Google[38]. De otra parte, la Corte entendió que Google no tenía responsabilidad por el contenido generado por el periódico, argumentando que esta exoneración es necesaria para proteger la neutralidad de la red, que está garantizada como parte del derecho fundamental a la libertad de expresión. La Corte, finalmente, ordenó al periódico mantener actualizadas las noticias que mencionen a una persona en relación con la ocurrencia de delitos.

Internet.org

A principios de 2015, Colombia se convirtió en el primer país latinoamericano donde entraba la polémica iniciativa Internet.org, hoy conocida como FreeBasic.org, impulsada por Facebook[39]. La iniciativa fue anunciada conjuntamente por el gobierno, el creador y dueño de Facebook, Mark Zuckerberg, y Tigo, el operador que implementaría la iniciativa. Si bien el proyecto es un acuerdo puramente privado entre Facebook y Tigo, se presentó en el país como una estrategia importante de política pública para cerrar la brecha digital y conectar a la población que

32 El Tiempo. (2015, 7 diciembre). "No vamos a tolerar persecuciones": Santos. *El Tiempo*. www.eltiempo.com/politica/gobierno/no-vamos-a-tolerar-persecuciones-santos/16451813

33 El Espectador. (2015, 3 diciembre). Fiscalía abrió investigación por seguimientos ilegales a Vicky Dávila. *El Espectador*. www.elespectador.com/noticias/judicial/fiscalia-abrio-investigacion-seguimientos-ilegales-vick-articulo-603160

34 Privacy International. (2015). *Un estado en la sombra: vigilancia y orden público en Colombia y Demanda y oferta: la industria de la vigilancia al descubierto*. www.privacyinternational.org/reports

35 El Tiempo. (2014, 30 agosto). Fiscalía le dice "no" a sistema de interceptación "Puma" de la Policía. *El Tiempo*. www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

36 El Tiempo. (2014, 30 septiembre). Plataforma Puma de la Policía entrará en operación, pero limitada. *El Tiempo*. www.eltiempo.com/politica/justicia/plataforma-unica-de-monitoreo-y-analisis-comienzan-pruebas/16390794

37 Botero, C., & Sáenz, P. (2015, 24 agosto). Op. cit.

38 Corte Constitucional de Colombia. (2015). Sentencia T-277. https://karisma.org.co/wp-content/uploads/2015/07/TUTELA-EL-TIEMPO.pdf

39 El Tiempo. (2015, 14 enero). Internet.org llega al país de la mano de Facebook. *El Tiempo*. www.eltiempo.com/archivo/documento/CMS-15093976

aún no tiene acceso a internet. Al cierre de este informe, todavía no se han conocido datos por parte del operador de telecomunicaciones que demuestren que Internet.org esté alcanzando su objetivo de servir como un estímulo para que más personas puedan adquirir un servicio de internet propiamente dicho.

En septiembre de 2015, Facebook lanzó la plataforma *Free Basics* para la implementación de Internet.org, adoptando nuevas guías para desarrolladores y el uso de https por defecto[40]. Esta nueva movida de Facebook fue una respuesta a muchas de las críticas que recibió la iniciativa[41].

Injuria

Gonzalo Hernán López

En un caso de aplicación desproporcionada del derecho penal a internet, Gonzalo Hernán López fue condenado a 18 meses de cárcel y multa por insultar a una funcionaria pública en un foro de comentarios del sitio web de un periódico tras una noticia que informaba sobre casos de corrupción política. Se ha entendido, por lo menos en su caso, que las expresiones injuriosas a través de internet tienen una consideración mayor si se comete a través de medios de comunicación social o de divulgación colectiva[42].

DERECHO DE AUTOR

Diego Gómez

Diego Gómez es un estudiante de biología que podría recibir hasta ocho años de cárcel por compartir en internet una tesis de maestría, que ya se encontraba digitalizada y disponible en diversos sitios web[43]. Se le acusa de violar el derecho de autor, pese a que solo compartió la tesis con el ánimo de dar a conocer ese recurso académico a otras personas y sin ningún interés económico detrás. El caso se encuentra actualmente en etapa judicial, por lo que aún se desconoce el desenlace. No obstante, a partir de una campaña desarrollada por la Fundación Karisma, conocida como #CompartirNoEsDelito, Diego se ha convertido en una figura internacional clave para la defensa del acceso abierto[44].

Este caso demuestra que las prácticas que han emergido en la era digital y que han supuesto un cambio de paradigma, aún chocan con normas legales –en este caso, el régimen legal de derecho de autor– anticuadas y desactualizadas.

40 Internet.org. (2015, 24 septiembre). Update to Internet.org Free Basic Services. *Internet.org by Facebook*. press.internet.org/2015/09/24/update-to-internet-org-free-basic-services

41 Open letter to Mark Zuckerberg regarding Internet.org, net neutrality, privacy, and security. www.accessnow.org/pages/open-letter-mark-zuckerberg-regarding-internetorg

42 Código de Procedimiento Penal, Artículo 223. perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf

43 El Espectador. (2014, 20 agosto). Estudiante podría ir a la cárcel por divulgar tesis en una plataforma virtual. *El Espectador*. www.elespectador.com/noticias/judicial/estudiante-podria-ir-carcel-divulgar-tesis-una-platafor-articulo-511647

44 Fundación Karisma. (s.f). Compartir no es delito. www.karisma.org.co/compartirnoesdelito. Archivo de prensa. www.karisma.org.co/compartirnoesdelito/?page_id=239

CONCLUSIONES Y RECOMENDACIONES

Internet es una herramienta con inigualables capacidades para permitir el ejercicio de derechos como la libertad de expresión y el acceso al conocimiento que, sin embargo, puede verse afectada por el desarrollo de políticas que no tienen en cuenta sus características particulares y el punto de vista de los múltiples grupos interesados.

Desafortunadamente, el gobierno colombiano no es consistente respecto del respeto de derechos fundamentales en la implementación de sus políticas y programas para internet, como se puede ver en el desarrollo de los sistemas de vigilancia de las comunicaciones. Difícilmente, la falta de control y supervisión evidente de herramientas como PUMA o SIGD puede generar un clima de confianza en el que internet pueda destacarse como una plataforma para el ejercicio de derechos fundamentales. Por otro lado, casos como el de Gonzalo Hernán López o Diego Gómez permiten concluir que el poder judicial aún tiene mucho camino por recorrer en la compresión de las características de la red. Aunque son pocas las ocasiones en que internet es objeto central de una decisión judicial, el precedente que sientan estas decisiones riñe con la necesidad de aplicar de forma adecuada y proporcionada la legislación diseñada para un mundo sin internet.

En ese contexto, se pueden formular las siguientes recomendaciones:

- En general, se debe tener en cuenta la existencia de estándares internacionales de derechos humanos tales como la Declaración conjunta sobre libertad de expresión e internet[45], la Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión[46], o los Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones[47], entre otros, al desarrollar medidas de restricción de derechos fundamentales.
- Se debe fortalecer las capacidades judiciales, especialmente en lo relacionado con la comprensión de internet, de forma que se desarrolle una línea de interpretación judicial consistente con los estándares internacionales de derechos humanos aplicables a la red.
- Las autoridades deben desarrollar e implementar modelos de participación que tomen en cuenta los puntos de vista de los diferentes grupos interesados en internet tales como la sociedad civil, la academia y la comunidad técnica. La ampliación de la discusión a estos grupos aumentará la legitimidad de las políticas que se quiera implementar para regular internet. Vale anotar que, en este sentido, ya ha habido avances positivos en el tema de la gobernanza de internet.
- La sociedad civil debe estar atenta a los desarrollos legislativos, judiciales y administrativos que afectan internet, con el fin de buscar una participación efectiva y consolidar su lugar como interlocutor ante las autoridades relevantes en la creación e implementación de políticas que afecten internet. Esto, a su vez, debe ir de la mano de acciones de incidencia basadas en investigación y acorde con las necesidades locales y los debates internacionales en torno a internet.
- La sociedad civil, además, debe impulsar y ampliar las redes de apoyo locales, regionales e internacionales para amplificar su voz en la defensa de los derechos humanos en espacios digitales y aunar esfuerzos y conocimiento en cuestiones compartidas entre los países.

45 Relator Especial de las Naciones Unidas para la promoción y protección del derecho a la libertad de opinión y de expresión, Representante para la libertad de los medios de comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos para la libertad de expresión, y Relatora Especial sobre libertad de expresión y acceso a la información de la Comisión Africana de Derechos Humanos y de los Pueblos. (2011, 1 junio). *Declaración conjunta sobre libertad de expresión e internet*.

46 Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de opinión y de expresión y Relatora Especial de la Organización de Estados Americanos para la libertad de expresión. (2013, 21 junio). *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*.

47 https://es.necessaryandproportionate.org/text

APC
ASOCIACIÓN PARA
EL PROGRESO DE
LAS COMUNICACIONES

Internet y TIC para la justicia social y el desarrollo

APC es una red internacional de organizaciones de la sociedad civil fundada en 1990 que empodera y asiste a gente que trabaja por la paz, los derechos humanos, el desarrollo y la protección del medio ambiente, a través del uso estratégico de las tecnologías de información y comunicación (TIC).

APC trabaja para construir un mundo en donde todas las personas tengan un acceso fácil, equitativo y accesible al potencial creativo de las tecnologías de información y comunicación para mejorar sus vidas y crear sociedades más igualitarias y democráticas.

www.apc.org info@apc.org

Diseño gráfico: MONOCROMO

Escrito por Juan Diego Castañeda y Amalia Toledo

Encargado por la Fundación Karisma

ESTE INFORME SE HA ELABORADO COMO PARTE DEL PROYECTO EXAMINANDO LOS DERECHOS Y LAS LIBERTADES EN INTERNET EN LATINOAMÉRICA (EXLILA) DE LA ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES (APC).

EL PROYECTO ESTÁ FINANCIADO POR OPEN SOCIETY INSTITUTE (OSI) Y APC Y ESTÁ COORDINADO POR LA ONG DERECHOS DIGITALES.

INFORME NACIONAL COLOMBIA
Marzo 2016

ISBN 978-92-95102-52-1 APC-201603-CIPP-R-ES-DIGITAL-243