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

INFORME CONSOLIDADO DE INVESTIGACIÓN

Paula Jaramillo

DERECHOS DIGITALES

INTRODUCCIÓN

El presente informe consolidado forma parte del proyecto Examinando los derechos y las libertades en internet en Latinoamérica, también denominado EXLILA, de la Asociación para el Progreso de las Comunicaciones (APC), coordinado por Derechos Digitales.

Este informe registra los principales hallazgos emanados de los informes nacionales de México, Costa Rica, Colombia y Paraguay, elaborados en base al Marco APC-La Rue de monitoreo de derechos humanos en internet (*APC-La Rue Framework for Assessing Freedom of Expression and Related Rights on the Internet*, en adelante Marco APC-La Rue). Dicho documento marco gira sobre tres grandes ejes: libertad de expresión, restricciones aplicadas sobre contenidos en línea (bloqueos, ciberataques, protección de la privacidad y datos personales, entre otros puntos), y acceso a internet para diferentes grupos (grupos marginales, menores de edad).

Adicionalmente, se elaboró un extenso cuestionario sobre derechos humanos e internet que también tuvo

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.

como origen el Marco APC-La Rue y que sirvió para confeccionar los informes nacionales referidos en este documento.

El cuestionario desarrolló los tres tópicos principales planteados por el Marco APC-La Rue, con el objetivo de generar preguntas de respuesta afirmativa o negativa. Las preguntas se agruparon en torno a algunos de los principales derechos fundamentales que se ejercen usualmente en internet: privacidad, libertad de expresión, honra, libertad de conciencia y religión, asociación, reunión y no discriminación. Por último, se agregó una sección de preguntas sobre el comportamiento del sector privado respecto del ejercicio de derechos humanos en internet.

El informe resultante presenta los temas que forman parte de la agenda de los países involucrados en el proyecto e identifica los puntos en común. También muestra las áreas en las que se registran los mayores avances en materia de protección de derechos humanos e internet, y aquéllas en las que se detectan riesgos o amenazas, con el fin de facilitar una adecuada labor de contención en un futuro cercano.

Todos los informes nacionales generados para esta investigación tienen una estructura común, basada en la confección de un resumen ejecutivo sobre la situación de cada país y una introducción referida a la historia y al contexto general. A continuación, se exponen la normativa y las regulaciones más importantes que tiene el país en relación a internet, y se hace referencia a casos problemáticos en relación a la libertad y los derechos en internet – ya sean de naturaleza judicial o no. Por último, se presentan conclusiones y recomendaciones.

Un análisis de estas características, basado además en el enfoque propuesto por el Marco APC-La Rue, pone en evidencia la necesidad de mayor investigación en el área de los derechos humanos y su ejercicio en el entorno en línea. Valdría la pena ampliar la investigación para incluir otras temáticas pendientes que el propio Marco reconoce en situación de desarrollo (derechos sexuales y de las mujeres, derechos económicos, sociales y culturales) y cubrir también otros países del continente.

SITUACIÓN GENERAL DE LOS PAÍSES EXAMINADOS

Al analizar los cuatro informes generados en el marco del presente proyecto, se puede afirmar que el ejercicio de derechos en internet ha surgido como un asunto de cierta relevancia últimamente para los sistemas jurídicos nacionales, incluso al margen de la mayor o menor tasa de conectividad existente en cada país.

La prueba fehaciente de la importancia de este fenómeno está dada por la existencia de una serie de casos a raíz de los que se discute sobre el ejercicio de derechos en internet, o la imposibilidad de ejercer tales derechos. Ante esta nueva realidad, los gobiernos han tomado diversos caminos en lo legislativo, ya sea interpretando la legislación disponible como aplicable al ambiente en línea, o generando nueva regulación específica para dicho entorno.

Como consecuencia, han surgido proyectos de ley que plantean riesgos para los derechos fundamentales en internet y que, si bien pueden tener objetivos atendibles, desconocen los reales usos y potencialidades de la red. Así, se terminan afectando derechos ciudadanos ajenos a las conductas que se pretende evitar.

Esto sucede en el contexto de la regulación internacional para internet, que consiste en una serie de tratados y convenios conocidos hoy como *soft law* debido a su falta de poder vinculante, lo que nos lleva a preguntarnos si existe una perspectiva de derechos humanos adecuada en dicha normativa.

Para responder a esa pregunta, el Marco APC-La Rue y el cuestionario generado a partir de él resultan aún más valiosos, ya que brindan un conjunto de herramientas precisas y de fácil comprensión para determinar en qué áreas se han de reconocer avances positivos y en cuáles se han de reforzar el análisis, el estudio y la incidencia con el objetivo de encontrar soluciones afines a los principios consignados en los instrumentos de derechos humanos. Para ello, es imprescindible el desarrollo de políticas públicas, legislación y, en general, regulación que refuerce el ejercicio de derechos y prevenga su vulneración.

MAYORES AVANCES REGISTRADOS

El *reconocimiento constitucional* de garantías relacionadas con los derechos humanos e internet, elemento considerado relevante para el Marco APC-La Rue y el cuestionario, es ya un hecho en varios de los países estudiados. Este es un aspecto innegablemente positivo.

En México, por ejemplo, se reconoce el deber del Estado de garantizar el derecho de acceso a las tecnologías de información y comunicación, incluido el servicio de internet[1]. También se establece que las telecomunicaciones son servicios públicos de interés general que se deben prestar en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias[2].

Existe el mismo reconocimiento constitucional en Costa Rica a propósito del derecho a la privacidad, vinculado con la protección de los datos personales, resultando plenamente aplicable a internet. También existen proyectos de ley para declarar fundamental el derecho a internet. La declaración sostiene que el acceso a las tecnologías es básico para facilitar el ejercicio de los derechos fundamentales de las personas e impulsa al Estado a promover y garantizar el acceso universal a las nuevas tecnologías.

Paraguay, por su parte, reconoce constitucionalmente el derecho a la intimidad[3] y la privacidad de las comunicaciones[4].

Dicho reconocimiento constitucional, ya sea más o menos específicamente orientado hacia lo que sucede en internet, se complementa con la regulación que viene desarrollándose sobre el tema tanto en lo nacional, como en lo internacional.

A nivel nacional, se han elaborado proyectos de ley que, en muchos casos, carecen de una perspectiva de derechos humanos y terminan restringiendo o violando derechos fundamentales.

En lo internacional, los países han ido adhiriendo progresivamente a la regulación existente. Si bien la principal crítica a este fenómeno es su ya mencionado carácter no vinculante, denota un esfuerzo para aunar criterios y marca una tendencia orientadora en cuanto a reglas y principios.

Como parte de este mismo proceso de integración legislativa ha de considerarse la invitación a formar parte del Convenio de Ciberseguridad (Convenio de Budapest)

1 Artículo 6 de la Constitución de México
2 Fracción II, apartado B del mismo artículo
3 Artículo 33
4 Artículo 36

que recibieron Costa Rica y Paraguay. Dicho convenio apunta a generar una mayor cooperación internacional en cuestión de delitos informáticos y protección de privacidad y datos personales, pero cuenta también con contenidos polémicos en materia de retención de datos.

En cuanto a la *protección de datos,* elemento de privacidad destacado en el Marco APC-La Rue y el cuestionario, los países estudiados cuentan con normativa específica y aplicable a internet. Costa Rica contempla la obligación de los proveedores de servicios de internet (PSI) de tomar las medidas necesarias para garantizar que los datos se conserven de conformidad con lo dispuesto en el Reglamento sobre medidas de protección de la privacidad de las comunicaciones. Para ello establece que todos los datos deben ser confidenciales y no pueden hacerse públicos, ni ser entregados a persona física o jurídica alguna, a menos que haya autorización expresa del/a abonado/a o su representante; o por orden judicial conforme a la legislación vigente. Además, los datos deben ser conservados únicamente por el tiempo necesario y luego se deben procesar para volverlos anónimos.

La *neutralidad de la red*, otro elemento importante en aras de la privacidad, ha surgido como tema en varios de los países analizados (México, Colombia y Paraguay), lo que denota una cierta preocupación sobre la materia. Sin embargo, la regulación creada ha sido de irregulares características y cuenta con excepciones que en la práctica y por diferentes vías, han tornado irrelevante o inaplicable dicho principio, tal como se indicará con más detalle en la siguiente sección sobre "Principales amenazas detectadas".

Otro tema delicado es el de la vigilancia, en particular la *interceptación de comunicaciones*, incluidas aquellas que tienen lugar en internet. Ejemplos de ello son la retención de correspondencia, 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. Es frecuente que, en las legislaciones analizadas, dicha intervención se encuentre sujeta al requisito de autorización judicial, lo que representa un aspecto positivo y alineado con la salvaguarda de garantías fundamentales. Tal es el caso de Paraguay y Colombia.

En Paraguay, el Ministerio Público puede acceder a las comunicaciones intervenidas siempre y cuando un juez lo autorice, lo que constituye una excepción al principio de inviolabilidad y secreto de las telecomunicaciones[5].

En Colombia, ello solo puede efectuarse cuando existe autorización legal, siguiendo las reglas establecidas y sujeto a control judicial *ex ante* (en el caso de la búsqueda selectiva en bases de datos), y *ex post* en los demás. La Fiscalía General de la Nación es el único organismo autorizado para ordenar la interceptación.

La *protección de menores* ante la pornografía infantil como justificación del bloqueo de contenidos se da en el caso colombiano bajo una modalidad excepcional[6]. Esta normativa faculta a una división de la Policía Nacional para revisar contenido digital denunciado y determinar si califica o no para ser bloqueado; se sigue luego un protocolo de notificación que involucra al Ministerio de las Tecnologías de la Información y las Comunicaciones y los PSI. La entidad a cargo de establecer los criterios de bloqueo de pornografía infantil es una comisión compuesta por el Instituto Colombiano de Bienestar Familiar, la Defensoría del Pueblo, la Fiscalía General de la Nación y representantes de UNICEF. Este es un aspecto positivo, ya que determina estándares que buscan objetivar dichos bloqueos, alejándolos así de la posibilidad de constituirse en una herramienta de censura.

En Paraguay existe actualmente el denominado Proyecto de ley para la protección de niños y adolescentes contra contenidos nocivos de internet. Se teme que la Ley afecte derechos fundamentales, ya que pretende regular el filtrado de contenidos en redes inalámbricas públicas e incluso a nivel de los PSI.

En otro ámbito, en los países estudiados se ha verificado la existencia de regímenes que regulan el *derecho de autor* y su protección. Tal derecho ha quedado claramente desactualizado y todavía no se ha producido el cambio de paradigma requerido para su adaptación, lo que amenaza derechos fundamentales. El actual movimiento en pro del acceso abierto a contenidos ha adquirido mayor fuerza, considerando sobre todo que internet facilita el acceso y la circulación de información y conocimiento.

Finalmente, en materia de *ciberseguridad*, merece ser mencionado como un aspecto positivo el Plan Nacional de Ciberseguridad paraguayo, que se terminó de redactar en junio de 2015 con apoyo del equipo técnico de la Organización de Estados Americanos (OEA). En este programa contribuyen Canadá, Estados Unidos, Estonia y Reino Unido. Además, Paraguay ejerce ahora la presidencia del Comité Interamericano contra el Terrorismo. Sin embargo, el informe reconoce que se precisa mayor debate y discusión pública sobre la elaboración e implementación desde la perspectiva de los derechos fundamentales.

5 Establecido en la Ley de telecomunicaciones 642/95 y el Decreto del Poder Ejecutivo 14135/96

6 Ley 679 de 2001 y el Decreto 1524 de 2002

PRINCIPALES AMENAZAS DETECTADAS

La *deficiente implementación de los principios constitucionalmente reconocidos* a nivel de legislación secundaria en algunos países surge como un tópico de cuidado derivado de uno de los aspectos positivos registrados.

Tal es el caso de México donde, aunque existe un amplio reconocimiento constitucional de internet como servicio público de interés general que debe ser garantizado por el Estado, respetando condiciones de acceso libre, universal y sin injerencias arbitrarias, la legislación secundaria no siempre se encuentra acorde a ello.

En esta situación se encuentra la Ley federal de telecomunicaciones y radiodifusión mexicana, norma que:

- pretende implementar las obligaciones constitucionales respecto de internet y establece principios sobre neutralidad de la red que deben regir el servicio de acceso, aunque aún no se ha implementado, es decir, no hay lineamientos del Instituto Federal de Telecomunicaciones para la gestión de tráfico;
- establece diversas medidas, como la conservación masiva de metadatos de comunicaciones por dos años, que permiten la vigilancia de las comunicaciones por parte de las autoridades; y,
- establece obligaciones de colaboración con instancias de seguridad y justicia, tanto para empresas de telecomunicaciones como para aquellas que proveen aplicaciones, contenidos o servicios en internet. Dichas obligaciones incluyen la entrega de metadatos, la intervención de comunicaciones privadas y la localización geográfica en tiempo real de dispositivos de comunicación, sin señalar de forma clara, precisa y detallada qué autoridades pueden solicitar dicha colaboración o bajo qué circunstancias, y sin establecer de manera explícita la necesidad de autorización judicial u otras medidas de transparencia y rendición de cuentas para prevenir el abuso de vigilancia.

En cuanto a la *neutralidad de la red*, y tal como ya se anunciara a propósito de los avances, si bien se ha introducido como tema relevante en materia regulatoria, lo ha sido de forma tal que el principio ha quedado sin mayor aplicación práctica.

Así ha sucedido en México, donde aún está pendiente la emisión de normativa destinada a su implementación, en un contexto de prácticas contrarias a la neutralidad de la red promovidas tanto por proveedores de acceso a internet, como por proveedores de aplicaciones y servicios, e incluso con colaboración del gobierno federal. Tal es el caso de las ofertas de *zero rating* o del programa Internet.org o Free Basics, de Facebook.

En Colombia, el Plan Nacional de Desarrollo establece el principio de neutralidad de la red (artículo 56), pero al final hace una excepción, permitiendo a los PSI "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"[7]. A principios de 2015, Colombia se convirtió en el primer país latinoamericano donde entró la polémica iniciativa Internet.org, hoy conocida como Free Basics, impulsada por Facebook. Si bien el proyecto es un acuerdo puramente privado entre Facebook y Tigo –el operador a cargo de implementar la iniciativa–, se presentó en el país como una estrategia importante de política pública para cerrar la brecha digital y conectar a la población que aún no tiene acceso a internet. Sin embargo, el operador de telecomunicaciones aún no ha brindado datos que demuestren que Internet.org esté alcanzando su objetivo de democratizar el acceso a la red.

En Paraguay, la Resolución 190/2009 de la Comisión Nacional de Telecomunicaciones (CONATEL) protege el principio de neutralidad de la red y existe un proyecto para otorgarle rango legal. Pero no existen sanciones punitivas o administrativas en caso de faltas.

También se ha presentado en Paraguay el asunto del acceso gratuito a las redes sociales. Tigo es el proveedor desde 2013, lo que ha sido objeto de diversas declaraciones públicas de Mark Zuckerberg en el marco del proyecto Internet.org. CONATEL no se ha pronunciado con relación a esta infracción del principio de neutralidad, aunque sí lo hizo en el caso del bloqueo de llamadas de WhatsApp.

En materia de *vigilancia estatal* también se presentan varias amenazas, en particular para el derecho a la privacidad. En México, el Código Nacional de Procedimientos Penales otorga facultades a las procuradurías de justicia y fiscalías de investigación del país para intervenir comunicaciones privadas y tener acceso a metadatos, previa autorización judicial. Sin embargo, cuando se trata de la facultad de requerir la localización geográfica en tiempo real de dispositivos de comunicación, no se establece control judicial.

La vaguedad del lenguaje utilizado en la Ley de seguridad nacional mexicana para justificar este tipo de medidas, al otorgarle facultades al Centro de Investigación y Seguridad Nacional para intervenir comunicaciones privadas, también constituye una amenaza.

7 Dicha situación no hizo más que verse agravada por la Resolución 3502 de 2011 de la Comisión de Regulación de Comunicaciones, que llevó a la proliferación de planes de internet que acogen la modalidad de *zero rating*.

En el caso de Paraguay, la legislación[8] contempla un plazo obligatorio de seis meses para la conservación de un registro de llamadas del servicio de telefonía celular móvil o el sistema de comunicación personal, sin que se hayan contemplado penas administrativas y restrictivas, o multas, en caso de difusión pública o privada del contenido de esas señales. También hay normas que establecen que las empresas proveedoras de internet y de servicios de alojamiento de datos deben almacenar los datos de tráfico o "relativos a la comunicaciones electrónicas" por el mismo plazo de seis meses.

Paraguay cuenta, desde 2014, con un Sistema Nacional de Inteligencia (SINAI) según el cual solo la Secretaría Nacional de Inteligencia (SIN) tiene autoridad para "recopilar y procesar" información con el objetivo de salvaguardar la seguridad nacional, así como para la producción de inteligencia –concepto que no define. Sin embargo, no se mencionan ni sus actividades, ni sus atribuciones, aunque sí se señala su carácter excepcional y sujeto a autorización judicial, la cual contempla excepciones que abren flancos difíciles de cerrar. Existe preocupación debido a la vaguedad de las definiciones legales y respecto de la posible desproporción de esta vigilancia con relación a la afectación de derechos, sobre todo de aquellos individuos que incomoden o se opongan al gobierno.

Además, existe un proyecto de ley de delito organizado que establece, como parte de las investigaciones de este tipo de delitos, la posibilidad de realizar vigilancia electrónica. Este proyecto de ley está siendo observado atentamente ante el peligro de que atente contra derechos fundamentales.

En Colombia, la retención de datos de tráfico de comunicaciones también existe, tanto para la investigación criminal, como para el desarrollo de actividades de inteligencia. Para el primer fin, se obliga a los proveedores de redes y servicios de telecomunicaciones a retener y entregar a la fiscalía, cuando lo solicite, los datos del/a suscriptor/a y los datos de ubicación de los dispositivos[9]. La Ley de inteligencia y contrainteligencia 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" y toda la información que permita localizar los dispositivos, sin establecer paralelamente ninguna salvaguarda.

Ninguna de las formas de retención mencionadas tiene control judicial y no está claro si operan solo sobre telefonía móvil y fija, o si se aplican también a internet.

Existen varios casos documentados en Colombia sobre vigilancia de las comunicaciones que han afectado incluso a miembros del gobierno y el poder judicial[10]. En 2007 se supo que la Policía Nacional estaba adquiriendo equipos de vigilancia de las comunicaciones en el marco del programa Plataforma Única de Monitoreo y Análisis (PUMA), cuyas capacidades de vigilancia no estaban del todo claras aunque parecía que incluían internet. A mediados de 2014, la Fiscalía General declaró públicamente tener el control de los equipos que conformarían el sistema PUMA, pero la Policía anunció el inicio de pruebas para el uso de los equipos en octubre de 2015.

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. La adquisición por parte de la Policía Nacional de herramientas que tendrían la capacidad de interceptar comunicaciones privadas digitales aún se está investigando.

Por otra parte, a mediados de 2015 se empezó a extender por el continente americano la empresa privada italiana Hacking Team, que suministra servicios y software de vigilancia a los gobiernos del mundo. México –el mejor cliente de Hacking Team– concentra la mayor cantidad de clientes vigentes o potenciales y representa las mayores ganancias para la empresa vendedora. Varias autoridades mexicanas, muchas de las cuales no se encuentran legalmente facultadas para la vigilancia de comunicaciones, adquirieron software malicioso. Hay quienes lo han usado incluso en contra de opositores políticos y es posible que estas prácticas se hayan extendido a la intervención de comunicaciones de la población civil.

En Colombia, si bien no se pudo demostrar la utilización de Hacking Team[11], se supo que la Dirección Nacional de la Policía de Colombia (DIPON) tuvo acercamientos con la empresa y adquirió el programa "Galileo", un software malicioso con capacidad de infectar equipos y obtener información de ellos, además de encender remotamente el micrófono o la cámara web.

Paraguay también se vio involucrado en el escándalo de Hacking Team, pero las conversaciones tendientes a la compra del denominado Sistema de Control Remoto no se concretaron. Sin embargo, han existido otros casos

8 Reglamento de CONATEL 1350/2002

9 Decreto 1704 de 2012

10 Se han monitoreado conversaciones sostenidas en el contexto de los diálogos de paz entre representantes del Ejecutivo y las FARC.

11 Aunque aún hay una investigación en curso, y los principales afectados son un grupo de periodistas.

relacionados con software de seguridad para la interceptación de comunicaciones que han suscitado la atención pública (y uno de ellos es FinFisher, similar al de la mencionada empresa italiana).

Respecto de la *protección de los datos personales*, también se presentan situaciones de riesgo.

La Ley federal de protección de datos personales en posesión de los particulares de México ofrece protección a los usuarios y usuarias de internet, pero el Instituto Nacional de Acceso a la Información y Protección de Datos (INAI) la ha interpretado de maneras que comprometen el derecho a la libertad de expresión en internet. Un ejemplo de ello es la consideración de que el derecho de rectificación y cancelación de datos personales implica el derecho a exigir que intermediarios de internet remuevan enlaces a pedido de una persona que considere que el contenido enlazado daña su reputación o constituye un uso no autorizado de datos personales.

Existe un caso documentado en este sentido, en que el INAI ordenó a Google la remoción de tres enlaces a páginas de internet que mencionan el nombre de un empresario, siguiendo la doctrina elaborada por el Tribunal de Justicia de la Unión Europea conocida popularmente como "derecho al olvido". Esto ha generado incentivos perversos para el mercado de las empresas de manejo de reputación.

Otro caso relevante ocurrió en Colombia, a raíz de la queja presentada por una ciudadana contra el periódico El Tiempo y Google, pues al hacer una búsqueda su nombre aparecía ligado a un delito. La Corte Constitucional ordenó al periódico 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. 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, garantía que forma parte del derecho a la libertad de expresión. Finalmente, la Corte ordenó al periódico mantener actualizadas las noticias que mencionan a una persona en relación con la ocurrencia de delitos.

La Ley paraguaya sobre protección de datos personales[12] cuenta con grandes limitaciones, conceptos vagos e imprecisos y deficiencias en general. Las falencias alcanzan a la acción de *habeas data* y a la protección de los datos sensibles tales como "condición médica", ya que no impone sanción alguna por violaciones en el manejo de información sobre la salud personal. Un ejemplo de esto último fue la violación de la confidencialidad y privacidad ocurrida en mayo de 2015 cuando el embarazo de una niña de 10 años se hizo público y estuvo presente en los medios, incluyendo el parto.

Las amenazas a la *libertad de expresión* en internet constituyen otro de los temas sensibles. En México no se han documentado controles, filtros o bloqueos de información generalizados en internet. Pero el derecho a la libertad de expresión en internet se ve amenazado por el contexto de violencia generalizada, sobre todo contra los y las periodistas. Igualmente, algunas interpretaciones del derecho a la protección de los datos personales han derivado en órdenes de censura de enlaces a información de interés público sobre casos de corrupción y han sugerido esquemas amplios de responsabilidad de intermediarios.

En Colombia se prohíbe el envío de mensajes "en lenguaje cifrado o ininteligible" a las personas usuarias de "equipos de comunicaciones que utilizan el espectro electromagnético"[13]. El alcance de dicha disposición no resulta claro y se desconoce la existencia de casos en los que se haya aplicado.

El concepto tradicional de *protección del derecho de autor*, aplicado a internet, ha devenido en situaciones que incluso rayan en lo irracional. Así, en Colombia se registró el caso de un estudiante de biología que podría tener que cumplir hasta ocho años de cárcel por compartir en internet una tesis de maestría que ya estaba digitalizada y disponible en diversos sitios web.

En Paraguay se establece pena privativa de libertad de hasta tres años o multa para quien, sin autorización del titular, divulgue, promocione, reproduzca o represente públicamente una obra protegida por la ley de derecho de autor. Esta ley se aplica en el entorno en línea, lo que trae aparejadas muchas complejidades. Por ejemplo, la información sobre la violación cometida se obtiene a través de vigilancia previa, es decir, se consigue la IP de la descarga ilegal o se incauta la computadora o teléfono celular, con lo que se violan derechos fundamentales.

Existe un antecedente en Paraguay que pudo haber influido en lo anterior. Se trata de un proyecto de ley para la retención de datos de tráfico con el fin de perseguir cualquier hecho punible, también conocido como Pyrawebs. La polémica suscitada fue tan fuerte que el proyecto no se aprobó.

En internet no es raro encontrar leyes de *delitos informáticos* que criminalizan usos legítimos de la tecnología. Así sucedió en Costa Rica, donde se proponían penas de cárcel ante la publicación, por cualquier medio, de informaciones secretas políticas, o para el tratamiento no autorizado de imágenes, datos de una persona física

12 Ley 1682/01, posteriormente modificada por la Ley 1962/02

13 Ley 418 de 1997, artículo 102

o jurídica almacenados en sistemas o redes informáticas, telemáticas, en contenedores electrónicos, ópticos o magnéticos[14]. Afortunadamente, la reforma al código penal fue declarada inconstitucional y hoy existe una regulación de delitos informáticos que no violenta derechos fundamentales.

En México se presentó una iniciativa legal carente de suficiente rigor técnico y jurídico, que establecía severas sanciones para una amplia gama de conductas y amenazaba la privacidad de los usuarios y usuarias de internet obligando a toda empresa de telecomunicaciones e internet a conservar datos sobre el uso que hicieran sus clientes de la red, y entregar dichos datos a las autoridades. La polémica suscitada fue tal que el proyecto se retiró prontamente.

En Colombia se produjo una aplicación desproporcionada del *derecho penal* a internet cuando se condenó a una persona a 18 meses de cárcel y multa por insultar a una funcionaria pública en un foro de comentarios del sitio web de un periódico. El argumento para justificar la pena fue que las expresiones injuriosas tienen mayor incidencia si se cometen a través de medios de comunicación social o de divulgación colectiva.

Por su parte, el Código Procesal Penal de Paraguay establece la necesidad de una orden judicial al referirse a la interceptación e incautación de la correspondencia, telégrafo o cualquier otro tipo de correspondencia, además de la posibilidad de vigilancia de las comunicaciones con carácter excepcional. Sin embargo, no quedan claros los límites para el tipo de tecnología que debe ser utilizada.

14 Ley de delitos informáticos 9048, de 2012

CONCLUSIONES

Los derechos fundamentales en internet se ven amenazados en los cuatro países analizados.

Si bien se detectan algunos avances o aspectos positivos, muchos se convierten en la práctica en situaciones de cuidado para el ejercicio de derechos, ya sea por la implementación deficiente de normas bien intencionadas, o por no cumplirse las garantías que se pensaba salvaguardar.

En este sentido, hay que insistir en la necesidad de una regulación con perspectiva de derechos humanos, que garantice un equilibrio adecuado de intereses también al momento de su implementación. De lo contrario, el peligro es que se multipliquen las declaraciones de intenciones con casi nulo efecto práctico, tal como parece haber sucedido en los países observados en materia de neutralidad de la red.

Por ese motivo, los esfuerzos no deben concluir cuando se logra una normativa respetuosa de los derechos humanos, sino que hay que realizar un seguimiento luego de su implementación con el fin de garantizar el cumplimiento de lo establecido, o denunciar su incumplimiento.

En los cuatro países estudiados según los lineamientos del Marco APC-La Rue y el cuestionario derivado quedan tópicos claves por abordar, sobre todo en lo referido al derecho de reunión, de no discriminación, y las libertades de conciencia, religión y asociación. Se trata de países donde es preciso garantizar el derecho a la privacidad y la libertad de expresión para fortalecer la democracia, la participación ciudadana y la libertad de información.

Para ello es clave desarrollar la confianza suficiente a fin de aprovechar una herramienta con tantas capacidades como internet que, mal utilizada, puede convertirse en un arma de persecución, represión, censura y abuso. Prueba de ello fue el mencionado escándalo de Hacking Team en América Latina, que puso en evidencia la disposición de los gobiernos para invertir fuertes sumas de dinero con el fin de monitorear a la ciudadanía a sus espaldas.

Se necesitan políticas que atiendan a las particulares características de internet, potenciándola y no restringiéndola de manera innecesaria; y que en ese proceso puedan tener participación todos los grupos de la sociedad interesados en manifestar su opinión, lo que brindará no solo una perspectiva más amplia, sino que también dotará de legitimidad al proceso.

Por supuesto, ello requerirá de la acción de una sociedad civil empoderada e informada en la que se desarrolle más investigación para llevar a cabo acciones de incidencia basadas en evidencia, y que sea capaz de efectuar análisis comparativos sobre los últimos avances a nivel nacional e internacional. Este esfuerzo permitirá unir fuerzas a nivel regional para potenciar un discurso que vele por mejores políticas públicas para el ejercicio de derechos en internet, que efectivamente se enfoquen en la regulación dotada de una perspectiva respetuosa de los derechos humanos.

Paralelamente, el Estado debe promover iniciativas legales para proteger los derechos de toda la población y evitar que el propio aparato administrativo se transforme en un celador indeseado de la ciudadanía, a sus espaldas y a expensas de sus propios recursos, mientras el Poder Judicial debe ejercer un control independiente, razonable, proporcionado y transparente.

Las organizaciones de la sociedad civil latinoamericana que trabajan en defensa de los derechos fundamentales tienen la posibilidad de asumir un importante rol, aprovechando herramientas como el Marco APC-La Rue y el cuestionario surgido a partir de él para realizar diagnósticos y estudios comparativos, y proponer soluciones.

La investigación realizada propone un excelente punto de partida, que puede extenderse a las áreas no abordadas, guiándose para ello en el detallado cuestionario propuesto. Aún cuando el resultado de dicho ejercicio lleve a concluir que se trata de áreas que carecen en absoluto de tratamiento, o que solo se han tratado en muy escasa medida, se dejarán sentadas las bases del desafío pendiente.

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

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 CONSOLIDADO DE INVESTIGACIÓN

MARZO 2016

ISBN 978-92-95102-56-9 APC-201603-CIPP-R-ES-DIGITAL-247