

Hacia una Internet libre de censura

Propuestas para América Latina

Eduardo Bertoni

COMPILADOR

Facultad de Derecho
Centro de Estudios en Libertad de
Expresión y Acceso a la Información



Hacia una Internet
libre de censura

Hacia una Internet libre de censura

Propuestas para América Latina

Eduardo Bertoni

COMPILADOR

Facultad de Derecho

Centro de Estudios en Libertad de
Expresión y Acceso a la Información



Hacia una internet libre de censura : propuestas para América Latina / compilado por Eduardo Andrés Bertoni. - 1a ed. - Buenos Aires : Universidad de Palermo - UP, 2012.
352 p. ; 23x16 cm.

ISBN 978-987-1716-54-8

1. Políticas Públicas. 2. Internet. I. Bertoni, Eduardo Andrés, comp.
CDD 320.6

Compilador:
Eduardo Bertoni

Diseño gráfico:
Patricia Fiuza

Diseño original de tapa:
Departamento de Diseño Institucional
- Universidad de Palermo

Corrección:
Julieta Botto

Editado por la Universidad
de Palermo, enero de 2012,
Buenos Aires, Argentina

© 2012 Fundación Universidad
de Palermo

ISBN: 978-987-1716-54-8

Hecho el depósito que marca la
ley 11.723

Esta edición, de 500 ejemplares,
se terminó de imprimir en el mes
de enero de 2012 en BRAPACK
Industria Gráfica, Saraza 1354,
Ciudad de Buenos Aires.

Impreso en la Argentina / Printed
in Argentina

Universidad de Palermo
Rector
Ing. Ricardo H. Popovsky

Facultad de Derecho
Decano
Roberto Saba

Centro de Estudios en Libertad de Expresión
y Acceso a la Información (CELE)

Director
Eduardo Bertoni

Mario Bravo 1050
(C1175ABW) Ciudad de Buenos Aires
Argentina
Tel.: (54 11) 5199-4500 | Fax: (54 11) 4963-1560
cele@palermo.edu | www.palermo.edu/cele

La reproducción total o parcial de este
libro, en cualquier forma que sea, idéntica
o modificada, no autorizada por los editores,
viola derechos reservados; cualquier
utilización debe ser previamente solicitada.

Este libro se publica gracias al apoyo financiero
de la Fundación Open Society Institute.

Índice

- 7 Presentación
Eduardo Bertoni
- 11 Introducción
Preservar la libertad en Internet en las Américas
Dawn Carla Nunziato
- 45 Capítulo uno
Responsabilidad de los proveedores de servicios de Internet (ISPs) en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica
Claudio Ruiz Gallardo y Juan Carlos Lara Gálvez
- 109 Capítulo dos
Intermediarios y libertad de expresión: apuntes para una conversación
Hiram A. Meléndez Juarbe
- 125 Capítulo tres
Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet
Lorenzo Villegas Carrasquilla

- 165 Capítulo cuatro
Protección de datos personales y prestación
de servicios en línea en América Latina
Alberto J. Cerda Silva
- 181 Capítulo cinco
Filtrado de contenido en América Latina:
razones e impacto en la libertad de expresión
*Joana Varon Ferraz, Carlos Affonso Pereira de Souza,
Bruno Magrani, Walter Britto*
- 259 Capítulo seis
La determinación de la jurisdicción en litigios
por difamación por contenidos en Internet:
algunas observaciones para América Latina
Eduardo Bertoni
- 313 Capítulo siete
Desarrollando políticas de Internet en Latinoamérica:
una perspectiva global
*Cynthia M. Wong, James Dempsey y Ellery Roberts
Biddle*
- 341 Epílogo
Conclusiones y recomendaciones para América Latina
Eduardo Bertoni
- 347 Sobre los autores y autoras

Presentación

Eduardo Bertoni

El debate global sobre la regulación en Internet ha evolucionado desde la pregunta de si la regulación de Internet es deseable a las preguntas, cuyas respuestas dependen del contexto y ubicación geográfica en que sean hechas, de qué áreas del derecho requieren regulación de la actividad en Internet; qué tipo de regulación es preferible y efectiva, y para qué fines.

Los países de América Latina han dado algunos pasos tímidos hacia la regulación de Internet. Las iniciativas han mirado hacia los Estados Unidos y Europa, donde Internet está más regulada, y los debates legislativos y públicos sobre el tema reflejan las discusiones que se dan a nivel internacional, gobernadas por los intereses, a veces en conflicto, de usuarios, compañías que operan en el espacio de Internet y encargados del diseño de políticas públicas. Los debates reflejan también la historia, principios y valores culturales que subyacen a las legislaciones en América Latina.

¿Qué políticas debe adoptar la región para promover el acceso a Internet? ¿Qué nivel de responsabilidad deben tener los proveedores de servicios de Internet en monitorear y evitar actos ilícitos cometidos a través de Internet? ¿Cómo debe responder el derecho de autor y derechos vinculados a las nuevas prácticas de publicación y acceso a contenidos en Internet? ¿En qué medida debe ajustarse el derecho penal a algunos comportamientos en Internet? ¿Cómo afectan las políticas gubernamentales y privadas originadas en otros países el acceso a Internet, la privacidad en línea y el desarrollo económico de América Latina?

En los últimos años, los países de América Latina han comenzado a desarrollar algunas respuestas a estas preguntas. En la región, se han

adoptado leyes y presentado proyectos de ley en las áreas de protección a la minoridad, discriminación, propiedad intelectual, telecomunicaciones, difamación, protección de datos personales, neutralidad de la red, regulación de contenidos en Internet, regulación de los espacios de acceso a Internet y responsabilidad de proveedores de servicios de Internet, entre otros.

Desde el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo, las preguntas que nos hemos formulado son: ¿de qué modo afectan estas políticas el ejercicio de la libertad de expresión en Internet? ¿Cuál es el vínculo entre la responsabilidad de los proveedores de servicios de Internet y la libertad de expresión? ¿Qué incentivos genera, en relación con la posibilidad de ejercitar plenamente la libertad de expresión, para usuarios y empresas la adopción de un sistema u otro de responsabilidad civil y penal? ¿Cuál es el vínculo entre la protección de datos personales y el derecho a la privacidad con la libertad de expresión? ¿En qué casos debería permitirse el filtrado, por parte de Gobiernos o de empresas privadas, de ciertos tipos de expresiones en línea? y ¿es esta actividad equiparable a la censura previa prohibida por el artículo 13 de la Convención Americana sobre Derechos Humanos? ¿Qué criterio sobre jurisdicción territorial deberían adoptar los tribunales en casos de difamación por contenido en línea?

Los artículos de esta publicación abordan algunos de estos temas, no con la idea de arribar a soluciones últimas, sino con la intención de plantear algunas de las cuestiones legales involucradas en estos temas y pensar acerca del efecto en torno de la libertad de expresión sobre las políticas posibles. Este libro pretende ser una guía que ayude a académicos, profesionales y encargados de la formulación de políticas públicas a pensar estas cuestiones.

Este trabajo es el resultado del proyecto del CELE sobre Libertad de Expresión e Internet, desarrollado durante 2011, que tuvo el objetivo de explorar cuál es el impacto sobre la libertad de expresión de la legislación, casos judiciales y políticas sobre Internet en algunos países de América Latina en relación con estos temas.

Desde 2010, el CELE ha estudiado temas de libertad de expresión e Internet. En octubre de 2010, la Universidad de Palermo fue sede de la *Consulta latinoamericana de expertos sobre libertad de expresión en Internet*, organizada por Frank La Rue, Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión. Las cuestiones debatidas en esa oportunidad indicaron la necesidad de un estudio más profundo

sobre estos temas en nuestra región. Nuestro proyecto de 2011 fue guiado por la intención de obtener un mayor conocimiento sobre estos temas, que hemos procurado adquirir mediante la realización de consultas a expertos, el estrechamiento de vínculos con organizaciones locales e internacionales dedicadas a estos temas y la participación en conferencias regionales e internacionales.

Los artículos contenidos en esta publicación han sido elaborados por prestigiosos académicos tanto de América Latina como de otras regiones, entre los que se encuentran expertos en derecho de las nuevas tecnologías, derecho de Internet, telecomunicaciones, derecho penal, derecho de propiedad intelectual y derecho a la libertad de expresión de Brasil, Colombia, Chile, la Argentina, Puerto Rico y los Estados Unidos.

Como complemento de los estudios desarrollados en el marco del proyecto, el 12 y 13 de septiembre de 2011, el CELE organizó el taller regional *Libertad de expresión e Internet: aspectos regulatorios en América Latina*, en el que fueron presentados algunos de los trabajos aquí publicados. Las conclusiones que el CELE ha recogido en esas discusiones están incluidas en esta publicación. Este taller fue posible gracias al apoyo de Google Inc.

Finalmente, el CELE agradece profundamente el apoyo del Open Society Institute para la realización de este proyecto. Agradecemos, también, a quienes elaboraron artículos para esta publicación y al personal y a los colaboradores de nuestro Centro de Estudios por su valiosa contribución para con esta actividad. Especial mención merece Andrea de la Fuente, investigadora del CELE, en este proyecto.

Esperamos que los lectores encuentren tan enriquecedor el debate como nosotros.

Preservar la libertad en Internet en las Américas

Dawn Carla Nunziato¹

Introducción

El taller Libertad de Expresión e Internet: aspectos regulatorios en América Latina, organizado por el profesor Eduardo Bertoni, contó con la presencia de expertos en derecho del hemisferio occidental, que fueron invitados a debatir sobre posibles vías para facilitar la libertad de expresión en Internet. Se examinaron alternativas para alcanzar un equilibrio entre los perjuicios que puede causar la libertad de expresión (como daños a la privacidad, el honor, la propiedad intelectual y el bienestar general) y sus beneficios, además del rol que desempeñan los proveedores de servicios de Internet como intermediarios en la protección y facilitación de la libertad de expresión en Internet. Durante el taller, se analizó el rol que corresponde a los Gobiernos en la protección de la libertad de expresión en Internet y en la sanción de expresiones nocivas, tanto en forma directa como mediante la regulación de los intermediarios. También se evaluó la función que desempeñan los Gobiernos en la regulación de los proveedores de servicios de Internet para facilitar el libre flujo de información. A continuación,

1. Quisiera expresar mi enorme agradecimiento a Eduardo Bertoni, director del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, por haberme invitado a participar en el taller Libertad de Expresión e Internet: aspectos regulatorios en América Latina, así como a todas las personas que intervinieron en el taller, por su destacado trabajo en el ámbito de la libertad de expresión en Internet en la región de América.

expondré algunas observaciones y recomendaciones preliminares destinadas a resguardar la libertad en este medio, y para ello me centraré especialmente en el modo en que los proveedores de servicios de Internet y los Gobiernos facilitan la libertad de expresión en América.

Actualmente, ciudadanos en toda América utilizan Internet como foro de expresión y comunicación, con una frecuencia sin precedentes. La presencia de Internet en América Latina aumenta rápidamente a medida que los países advierten la importancia de Internet para su economía y para la participación ciudadana en foros de expresión globales. En este período de cambios veloces, algunos países de América Latina se han posicionado como líderes en la protección de la libertad de expresión en Internet. Chile, por ejemplo, fue el primer país del mundo en sancionar una ley sobre neutralidad en la red, y garantizó de este modo que sus proveedores de servicios de Internet (PSI) no puedan discriminar contenidos o aplicaciones transmitidos a sus ciudadanos. Por el contrario, otros países de América Latina están adoptando medidas claramente menos respetuosas de la libertad de expresión en Internet. Venezuela, por ejemplo, tiene previsto establecer un punto único de acceso a Internet para impedir que sus ciudadanos tengan acceso a expresiones que «fomenten zozobra en la ciudadanía o alteren el orden público»². En los últimos años, los tribunales de Brasil han ordenado un bloqueo excesivamente amplio de contenidos de Internet, y en una oportunidad, llegaron, incluso, a exigir el bloqueo de *todo* tipo de acceso a YouTube en el país³. Los avances en tecnología de filtrado han alcanzado un punto en el cual es posible para los Gobiernos censurar expresiones que no gocen de la aprobación de las autoridades o de ciertas personas. En vista de estos cambios, es un momento oportuno para formular recomendaciones a Gobiernos de América Latina, a fin de que puedan preservar a Internet como foro para la libre expresión y no cedan a la tentación de apoderarse de Internet y convertirla en una herramienta de control gubernamental y manipulación. En las siguientes secciones, me propongo reflexionar sobre las iniciativas de los Estados Unidos y otros países en esta materia y formular recomendaciones para proteger la libertad de expresión en Internet en la región de América.

2. Véase *infra* Varon Ferraz, Joana, Carlos Affonso Sousa, Bruno Magrani y Walter Britto, «Filtrado de contenido en América Latina: razones e impacto en la libertad de expresión», capítulo 5 del presente volumen.

3. *Íd.*

I. Reglamentación gubernamental de proveedores de servicios de Internet

Los proveedores de servicios de Internet custodian el acceso a la totalidad de los contenidos en Internet y, como tales, tienen amplio poder de control sobre qué información reciben y comunican sus suscriptores. La existencia de este poder genera el interrogante de en qué circunstancias se debe exigir o permitir a los PSI que lo ejerzan para prohibir a sus suscriptores el acceso a contenidos presuntamente nocivos, ilícitos o que las autoridades desapruében. Es decir, ¿deberían los Gobiernos regular a los PSI para *exigirles* que restrinjan el acceso a contenidos que el Gobierno o terceros afirman que son lesivos? Por otra parte, los Gobiernos podrían sancionar leyes sobre neutralidad en la red a fin de *prohibir* que los PSI utilicen esta potestad para controlar el acceso a contenidos lícitos por parte de sus suscriptores. Como ejemplo del primer caso, los Gobiernos podrían exigir a los PSI que prohíban a sus suscriptores acceder a contenidos que las autoridades consideran lesivos, como ha intentado hacerlo Venezuela. O bien, podrían exigir a los PSI que impidan todo tipo de acceso a contenidos que son señalados como agraviantes por una persona, tal como ha ocurrido en Brasil. Los propios PSI podrían optar por impedir a sus suscriptores el acceso a materiales que ellos estimen no convenientes, como aplicaciones o contenidos ofrecidos por un competidor, o contenidos que adhieran a una determinada opinión política o social con la cual no esté de acuerdo el PSI. En la sección siguiente, sugiero en primer lugar que los PSI deberían estar exentos de cualquier responsabilidad por alojar contenidos lesivos y, en segundo lugar, que se debería exigir legalmente a los PSI que faciliten el acceso a todos los contenidos lícitos, sin discriminación ni censura.

I.A. Los proveedores de servicios de Internet en general deberían estar exentos de responsabilidad por facilitar el acceso a contenidos nocivos

Los Gobiernos deben adoptar decisiones difíciles respecto de si corresponde atribuir responsabilidad –y de qué manera– a los PSI por facilitar el acceso a contenidos nocivos, ya sea al alojar este tipo de material, como en el caso de YouTube; o al proporcionar enlaces a dichos contenidos, como en el caso de Google. En un régimen que proteja al máximo las expresiones, los PSI estarían exentos de cualquier tipo de responsabilidad como intermediarios y no se les exigiría eliminar contenidos lesivos ni deshabilitar su acceso si

no existe una resolución judicial específica que determine que se trata de un contenido ilícito. Contrariamente, en un régimen que sea lo más restrictivo posible, los PSI serían directamente responsables por contenidos nocivos de terceros, con independencia de si conocen en forma real o presunta dicho contenido. Y entre estos dos extremos, las posibilidades son numerosas.

La imposición de responsabilidad objetiva a proveedores de servicios de Internet por haber facilitado contenidos presuntamente nocivos publicados por suscriptores trae aparejadas graves consecuencias para la libertad de expresión, puesto que exige que los PSI lleven a cabo un control enérgico y minucioso de todo el contenido y podrían incentivarlos a eliminar cualquier material cuyo carácter nocivo o ilícito sea apenas cuestionable. La mayoría de los países de la región finalmente no han implementado un sistema de este tipo. No obstante, incluso la imposición a estos proveedores de un sistema de responsabilidad supeditado al envío de notificaciones tiene consecuencias negativas para la libertad de expresión. En un sistema de esta índole, si se reconoce a una persona afectada el derecho a exigir que el PSI elimine contenidos que esta señala como nocivos o ilícitos, la obligación del PSI de quitar dicho contenido, o los incentivos que tenga para hacerlo –cuando no medie una determinación judicial sobre su ilicitud–, tendrán efectos perniciosos para la libertad de expresión. En palabras de un tribunal:

La imposición de responsabilidad a los PSI sobre la base de la recepción de notificaciones proporcionaría a terceros una vía para interponer demandas en el futuro sin costo alguno. Cuando a una persona le desagraden las expresiones manifestadas por otra a través de un servicio informático interactivo, la parte agraviada no tendrá más que «notificar» al proveedor de servicios pertinente y afirmar que la información es difamatoria para la ley. A la luz de la enorme cantidad de expresiones que se comunican a través de servicios informáticos interactivos, estas notificaciones podrían resultar excesivamente engorrosas para los proveedores de servicios, que continuamente deberían optar entre censurar expresiones controvertidas o afrontar una responsabilidad limitativa. [Esta situación debilitaría] el carácter dinámico de las expresiones vertidas a través de Internet...⁴

4. *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997).

Los Estados Unidos se han mantenido al margen de este tipo de sistemas desfavorables para la libertad de expresión en casos en que el perjuicio invocado es el de difamación o violación de la privacidad. El artículo 230 de la Ley de Decencia en las Comunicaciones (Communications Decency Act)⁵ exime, en general, a los PSI de responsabilidad objetiva y responsabilidad basada en la notificación por parte de la persona afectada acerca del contenido supuestamente nocivo y libera, asimismo, a dichos proveedores de cualquier responsabilidad por facilitar el acceso a expresiones supuestamente nocivas. Esta inmunidad se extiende a casos en que los PSI editen, examinen previamente o contraten a terceros para que generen o publiquen los contenidos presuntamente nocivos. Si bien esta inmunidad otorga una amplia protección, ha sido extendida en forma bastante generalizada, incluso a casos donde el PSI interviene activamente en la creación del contenido, y realmente no podría afirmarse que este haya sido proporcionado por «otro» proveedor de contenidos informativos. La justicia estadounidense, al interpretar el artículo 230, debería examinar más minuciosamente si el PSI ha tenido un rol activo en la generación de contenidos nocivos, y no debería extender esta exención de responsabilidad a casos de esta naturaleza. Así, se conseguiría un equilibrio entre la protección de los intermediarios y el derecho a reparación adecuada de las partes agraviadas por dicho contenido. La postura de los Estados Unidos frente a las denuncias de violación de derechos de autor ha conseguido resultados mucho menos proteccionistas de la libertad de expresión (y el uso justo). Conforme a la Ley Estadounidense sobre Derechos de Autor en la Era Digital (United States's Digital Millennium Copyright Act, DMCA)⁶, el titular de derechos de autor básicamente puede obligar al PSI a quitar contenidos que considere nocivos, sin una determinación judicial sobre la naturaleza lesiva del material. El artículo 512 de la DMCA reconoce en los proveedores de servicios una forma segura de limitar su responsabilidad por violaciones directas e indirectas de derechos de autor si se comprometen a quitar contenidos que el titular del derecho en cuestión *afirma* que son violatorios⁷. Conforme a

5. Pub. L. No. 104-104, 110 Stat. 133 (codificado según reforma en 47 u.s.c. § 223 [2000]). El artículo 230 establece que «[n]ingún proveedor... de servicios informáticos interactivos será tratado como editor o vocero de información proporcionada por otro proveedor de contenidos informativos».

6. 17 u.s.c. art. 512 (2000).

7. 17 u.s.c. art. 512 (c)(1)(c).

las disposiciones del artículo 512 sobre notificación y retiro, el titular de derechos de autor podría notificar al proveedor de Internet que considera que está alojando contenidos lesivos o que incluye enlaces a contenidos de este tipo⁸. Al recibir esta notificación, el proveedor deberá rápidamente interrumpir el alojamiento o cancelar el enlace al contenido supuestamente lesivo para, así, beneficiarse con la limitación de responsabilidad establecida en la ley. Si bien la ley también contempla un mecanismo para que el usuario de Internet que publicó dicho contenido defienda el uso (a través de una «contranotificación»)⁹, este mecanismo resulta problemático, pocas veces se aplica y ha tenido impacto limitado en la censura de contenidos permitida por el artículo 512. Hoy en día, los titulares de derechos de autor, respaldados por la DMCA, solamente necesitan enviar una notificación al PSI solicitando que elimine un determinado contenido, y el PSI, para conseguir la limitación de responsabilidad establecida en el artículo 512, dará curso inmediatamente a este pedido, y quitará «con prontitud» el contenido o deshabilitará el acceso¹⁰. De hecho, esta disposición permite al titular de derechos de autor obtener una medida equivalente a una prohibición temporal –un mandamiento judicial que ordena quitar el contenido presuntamente violatorio– sin ningún proceso judicial. Miles de titulares de derechos de autor han logrado persuadir a los PSI de que censuren cualquier uso crítico o desfavorable del contenido tutelado por derechos de autor, incluso en casos donde estos usos no serían considerados violatorios, sino usos legítimos, conforme a la Ley de Derechos de Autor. El análisis de miles de usos diversos del artículo 512 revela una «alta incidencia de usos cuestionables del proceso... con el fin de conseguir ventajas en un mercado competitivo, proteger derechos no tutelados como derechos de autor... y disuadir la crítica, los comentarios y el uso legítimo, lo cual [redunda en] efectos continuos y posiblemente incalculables para las expresiones públicas»¹¹. La atribución de responsabilidad a los PSI, mediante un sistema de notificaciones, por alojar contenidos presuntamente lesivos o proporcionar enlaces a estos, genera resultados desfavorables para la libertad

8. 17 u.s.c. art. 512 (c)(3).

9. 17 u.s.c. art. 512 (g)(3)(c).

10. Véase art. 512 (c)(1)(c).

11. Véase Urban, Jennifer M y Laura Quilter, «Efficient Process or “Chilling Effects”? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act», en *Santa Clara Computer and High Tech L.J.*, 22 (2006), p. 621.

de expresión. Permitir que titulares de derechos de autor consigan cancelar contenidos supuestamente violatorios sin una resolución judicial acerca de la ilicitud del contenido no protege de manera suficiente los derechos de libertad de expresión y uso legítimo de los usuarios de Internet ni constituye un modelo que merezca ser replicado por otros países de América.

Como hemos visto, las leyes que instan a los PSI a quitar contenidos supuestamente nocivos sin intervención de un proceso judicial son sumamente problemáticas. No obstante, también la imposición *judicial* de la obligación de retirar contenidos a los PSI puede tener consecuencias desfavorables para la libertad de expresión. En los casos de la Argentina y Brasil, que serán analizados por otros comentaristas, la Justicia exigió a los PSI que quitaran enlaces a sitios web que contenían nombres famosos como Cicarelli y Maradona. En estos casos, la Justicia no definió sus resoluciones con la suficiente especificidad para proteger los derechos de libertad de expresión, e impuso una obligación de retiro amplia a los PSI. Las órdenes judiciales de retiro excesivamente amplias, así como la implementación indiscriminada de estas órdenes por los PSI, han tenido graves consecuencias para el derecho de expresión.

A fin de evitar resultados desfavorables para la libertad de expresión al regular Internet, los Gobiernos deberían abstenerse de sancionar leyes que atribuyan responsabilidad de intermediarios –ya sea objetiva o basada en la notificación– a los PSI por facilitar contenidos que agravan a terceros. Si bien la Justicia debería conservar la facultad de imponer obligaciones de retiro en casos específicos en que los PSI publican contenidos ilícitos, tales órdenes deberían ser formuladas por los tribunales e implementadas por los PSI con la mayor especificidad y precisión posible, para, así, evitar inhibir en forma excesiva las expresiones protegidas.

I.B. Los Gobiernos deberían imponer obligaciones sobre neutralidad en la red a proveedores de servicios de banda ancha

Como se indica en la parte I.A., para proteger el libre flujo de información en Internet, los Gobiernos deberían sancionar leyes que eximan en términos generales a los PSI de responsabilidad por alojar contenidos nocivos o ilícitos. Contrariamente, los Gobiernos deberían imponer a los proveedores de servicios de banda ancha la obligación jurídica de facilitar a los usuarios de Internet el acceso a todos los contenidos lícitos, y exigirles que actúen como conductores neutrales de tales contenidos, sin discriminación ni

censura. Dado que Internet se ha convertido en el medio más importante para expresarse y comunicarse con los demás, en América y el resto del mundo por igual, es imprescindible que los usuarios de Internet gocen de la garantía de libre circulación de información y comunicación de ideas, sin censura ni discriminación por parte del Gobierno ni de los PSI responsables de facilitar tales comunicaciones. Del mismo modo que desde hace tiempo se exige legalmente a las empresas de telefonía, en los Estados Unidos y en otros países, que conecten las llamadas de los usuarios y que faciliten las comunicaciones sin censura ni discriminación, también se debería obligar a los proveedores de servicios de banda ancha a facilitar la comunicación y el intercambio de información sin discriminación ni censura. Esta libertad de comunicación es, desde hace tiempo, un aspecto esencial de nuestro estilo de vida democrático y liberal, y debe continuar siendo protegida en la era de Internet¹².

En los Estados Unidos, el Gobierno, históricamente, ha impuesto obligaciones positivas a entidades que intervienen en transporte, telecomunicaciones y otras importantes funciones vinculadas con los servicios públicos para facilitar el libre flujo de la información y el comercio, sin censura ni discriminación. A través de la doctrina del «uso compartido de la infraestructura» (*common carriage doctrine*), el Gobierno de los Estados Unidos ha impuesto obligaciones positivas a entidades que desempeñan importantes funciones de comunicación y transporte en beneficio del público. En vez de conceder a los canales de comunicación la facultad discrecional de regular las expresiones del modo que les parezca conveniente, la doctrina del uso compartido de la infraestructura implementada por el poder judicial y legislativo en los Estados Unidos exige que estas entidades pongan a disposición todos los contenidos lícitos en las mismas condiciones.

Al regular a proveedores de banda ancha, los Gobiernos deberían guiarse por el principio que subyace al derecho moderno de las comunicaciones y la doctrina de uso compartido de la infraestructura: que las democracias liberales requieren una ciudadanía debidamente informada, y que esto, a su vez, exige que los ciudadanos gocen de la libertad de comunicarse y de

12. Para un análisis más detallado de la doctrina de uso compartido de la infraestructura (*common carriage*) y su aplicación respecto de los proveedores de servicios de Internet, véase Nunziato, Dawn C., *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*; Stanford, Stanford University Press, 2009.

tener acceso a comunicaciones de distintas fuentes. Los mismos principios que justifican la regulación de las empresas de telefonía bajo el régimen de uso compartido de la infraestructura (*common carriers*), sujetas a requisitos de no discriminación, con el fin de «proteger el derecho a comunicarse de los ciudadanos comunes»¹³, son relevantes a efectos de las comunicaciones a través de Internet.

Permitir que los proveedores de banda ancha discriminen contenidos o aplicaciones arbitrariamente es incompatible con la evolución histórica del reconocimiento de la libertad de comunicación de las personas. Admitir que proveedores de banda ancha restrinjan el libre flujo de información e ideas permite que estos custodios de la libertad de expresión frustren el «debate público y la deliberación informada... que constituyen un presupuesto de los Gobiernos democráticos y a los cuales aspira la Primera Enmienda»¹⁴. A falta de regulación, los proveedores de banda ancha tendrán facultades discrecionales para discriminar contenidos o aplicaciones, y los ciudadanos no tendrán garantías de acceso a una multiplicidad de opiniones de fuentes diversas y antagónicas exentas de censura, lo cual es necesario para que puedan tener una participación relevante en el Gobierno democrático. En vez de eso, los ciudadanos se verán constreñidos progresivamente a formas de expresión aprobadas (o al menos no desaprobadas) por uno o dos proveedores de banda ancha que actúan como custodios de sus comunicaciones en Internet.

Por lo tanto, los proveedores de banda ancha deberían estar sujetos a reglamentaciones sobre neutralidad en la red que exigen que asuman, al menos, la obligación de no discriminar, que fue tradicionalmente impuesta a otros servicios de comunicaciones, es decir, la obligación de facilitar y transmitir sin discriminación todos los contenidos y aplicaciones lícitos, sin excepción.

Las reglamentaciones sobre neutralidad en la red que prohíben a proveedores de banda ancha bloquear contenidos o aplicaciones lícitas deberían, además, exigir *transparencia* en estos bloqueos, y que tales proveedores informen a sus suscriptores sobre cualquier aplicación o contenidos (ilícitos) que hayan sido bloqueados, con indicación de los

13. Pool, Ithiel de Sola, *Technologies of Freedom*, 1983, p. 106.

14. *Id.*

motivos (*e.g.*, el proveedor afirma que el contenido era ilícito debido a que incluía pornografía infantil o algún tipo de material que se considera ilícito en ese país). Exigir esta transparencia en las medidas de bloqueo permitirá a los usuarios controlar estas decisiones de los proveedores de banda ancha y asegurar que no encubran una discriminación ilegítima basada en el contenido. Los usuarios de Internet gozan del derecho a la transparencia de las decisiones que inciden en qué contenido pueden consultar, así como a ser informados sobre la cancelación de contenidos y aplicaciones y a conocer los motivos, para, así, poder contrarrestar las acciones discriminatorias de los proveedores de banda ancha. En resumen, los Gobiernos deberían sancionar leyes que prohíban a proveedores de banda ancha bloquear aplicaciones o contenidos lícitos y priorizarlos o degradarlos en función de criterios discriminatorios. Este tipo de legislación debería, además, exigir transparencia en el bloqueo o la degradación, para lo cual los proveedores de banda ancha deberán informar a los usuarios de Internet sobre contenidos o aplicaciones que fueron bloqueados o degradados y los correspondientes motivos, y así los usuarios podrán aplicar controles genuinos a estas decisiones de los proveedores y asegurar que tales acciones no encubran actos de discriminación ilegítima. Varios países de América Latina han sido pioneros en materia de neutralidad en la red. Como se analiza en este volumen, Chile fue el primer país del mundo en sancionar una ley sobre neutralidad en la red y dispuso que los PSI «no podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red»¹⁵. Sin embargo, este mandato admite una excepción y dispone que «los proveedores de acceso a Internet podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red...». Colombia ha aprobado una ley similar sobre neutralidad en la red, pero no prevé una excepción sobre administración de red de este tipo. La ley colombiana establece que los «prestadores de servicios de Internet no podrán... bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de Internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio

15. Véase *supra* nota 2.

lícito a través de Internet [ni] disting[uir] arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos...». Las leyes sobre neutralidad en la red sancionadas en Chile y Colombia deberían servir como modelo a otros países del hemisferio para la protección del derecho de los usuarios de Internet a comunicarse por este medio, sin discriminación ni censura¹⁶. A fin de que Internet cumpla la promesa de que se trata del «mercado más participativo de expresiones masivas que haya conocido este país –y el mundo en general–»¹⁷, quienes actúan como custodios de las expresiones vertidas en Internet deberían ser regulados, para, así, garantizar que su rol de guardianes sea positivo para este mercado, sin discriminación ni censura, y se respeten los valores de libertad de expresión que son necesarios para facilitar el debate público y la deliberación informada que supone un gobierno democrático y que exige la libertad de expresión.

II. Los Gobiernos deberían sancionar garantías para las expresiones anónimas en Internet

Uno de los aspectos de Internet que más favorecen la libertad de expresión es la capacidad de los interlocutores de manifestarse en forma crítica, sin temor a represalias, acerca de los más diversos temas, incluidos sus Gobiernos y otros aspectos de relevancia política y social. Un elemento clave de este aspecto de la libertad de expresión en Internet es la capacidad

16. La Comisión Federal de Comunicaciones de los Estados Unidos (United States's Federal Communications Commission), tras años de incertidumbre y vacilación, finalmente ha publicado normas sobre neutralidad en la red que entrarán en vigor en noviembre de 2011. Tales normas sobre neutralidad en la red: (1) prohíben a los proveedores de servicios de Internet mediante tecnologías alámbricas o conexiones fijas a banda ancha bloquear contenidos, aplicaciones o servicios lícitos, salvo excepciones razonables sobre administración de redes, y prohíben que estos proveedores discriminen de manera irrazonable al gestionar el tráfico; (2) prohíben a los proveedores de servicios de banda ancha inalámbrica o móvil bloquear aplicaciones o contenidos lícitos que compiten con los propios servicios de voz o video de estos proveedores, si bien contemplan excepciones razonables sobre administración de redes. Véase *Preserving the Open Internet*, 76 Fed. Reg. 59192 (23 de septiembre de 2011) (codificado en 47 C.F.R. pt. 8). No obstante, estas normas pueden ser objeto de recurso judicial y no hay certeza acerca de si serán implementadas, ni cuándo.

17. 929 F. Supp. en 844.

de expresarse en forma anónima o con seudónimos. Sin embargo, varios países de América han sancionado medidas destinadas a restringir o prohibir expresiones anónimas, tanto en el espacio real como en el ciberespacio. La Constitución de Venezuela, por ejemplo, prohíbe las expresiones anónimas en cualquier medio¹⁸. La Constitución de Brasil contiene una prohibición similar sobre expresiones anónimas¹⁹. Este tipo de restricciones a la capacidad de las personas de expresarse en forma anónima (o con seudónimos), en Internet y otros medios, son contrarias a la garantía de libertad de expresión y deberían ser reconsideradas. Los países deberían brindar garantías genuinas para proteger el derecho de las personas a comunicarse y expresarse en forma anónima en Internet y en el espacio real.

La experiencia de los Estados Unidos, desde su fundación, demuestra la importancia de las garantías gubernamentales para el derecho a expresarse en forma anónima. La protección de expresiones anónimas ha sido un aspecto importante de la jurisprudencia estadounidense sobre libertad de expresión desde que se fundó el país. A lo largo de la historia de los Estados Unidos, y especialmente durante su formación y su evolución como democracia liberal, el derecho de los editores y autores a preservar el anonimato ha sido un componente importante del derecho de libertad de expresión y de prensa consagrado en la primera enmienda. Clarence Thomas, magistrado de la Corte Suprema de los Estados Unidos, resumió algunos aspectos relevantes de la historia de la nación en estos términos:

No hay dudas de que la literatura política creada por los Padres Fundadores se generó en forma anónima. Los ensayos que integran *El Federalista*, publicados con el seudónimo Publius, son uno de los ejemplos más famosos de la producción de literatura política anónima que tuvo lugar durante la ratificación de la Constitución... La primera y la más famosa experiencia estadounidense sobre libertad de prensa fue el juicio de Zenger en 1735, un caso sobre panfletos anónimos de contenido político.

18. Véase Freedom House, *Freedom on the Internet 2011*, 366 y n. 69, disponible [en línea]: <<http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf>>. [Nota del editor: consultada el 26/10/11.]

19. El artículo 5, inciso IV, de la Constitución de Brasil establece que: «Todas las personas son iguales ante la ley, sin distinción de cualquier naturaleza, y se garantiza a los brasileños y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, la libertad, la igualdad, la seguridad y la propiedad, en los siguientes términos:... es libre la manifestación del pensamiento, quedando prohibido el anonimato».

John Peter Zenger, dueño de la imprenta, se negó a revelar la identidad de los autores anónimos que, en sus panfletos, cuestionaban al gobernador de Nueva York, representante de la Corona... El caso... mostró, en una etapa temprana, la estrecha vinculación que reconocían entre anonimato y libertad de prensa los primeros pensadores estadounidenses²⁰.

Proteger el anonimato de autores y editores persigue dos objetivos fundamentales: en primer lugar, preservar el anonimato de quienes expresan ideas permite que el contenido del mensaje sea evaluado en función de su mérito y no de la identidad o reputación del autor²¹. En segundo lugar, proteger el anonimato permite a quienes expresan posturas o defienden causas que no son mayoritarias poder hacerlo sin temor a represalias personales²². En este sentido, la protección de expresiones anónimas es clave para lograr la función contramayoritaria de la primera enmienda, al resguardar a los emisores de mensajes controvertidos frente a posibles riesgos de represalias. Como lo expresó la Corte Suprema de los Estados Unidos en *McIntyre c/ Ohio Elections Commission*²³, al basarse en la teoría de la libertad de expresión formulada por John Stuart Mill en *Sobre la Libertad*²⁴:

El discurso anónimo no es una práctica perniciosa ni fraudulenta, sino un ejercicio honesto de defensa de ideas y disenso. El anonimato es un resguardo frente a la tiranía de la mayoría. Es un ejemplo de la finalidad perseguida por la Declaración Constitucional sobre Derechos y Garantías, en particular la primera enmienda, y que consiste en proteger a personas impopulares frente a represalias y evitar que se censuren sus ideas en una sociedad intolerante²⁵.

20. *McIntyre v. Ohio Elections Comm'n*, 514 u.s. 334, 350 (1995).

21. *Íd.* en 334 («El anonimato brinda a aquellos autores que no gozan de aceptación la posibilidad de que los lectores no prejuzguen su mensaje simplemente porque les desagrada la persona que lo propone»). Véase, también, Tien, Lee, «Who's Afraid of Anonymous Speech? McIntyre and The Internet», en *Or. L. Rev.*, 75 (1996), pp. 117, 144.

22. Véanse *McIntyre*, 514 u.s. en 374; *Talley v. California*, 362 u.s. 60, 64 (1960); Tien, *íd.* nota 21, p. 144 (donde se observa que «uno de los costos evidentes de regular el anonimato sería las posibles represalias contra los autores»).

23. 514 u.s. 334 (1995).

24. Stuart Mill, John, *On Liberty*; 1859.

25. 514 u.s. en 347.

Si no se protege el anonimato, quienes defienden ideas impopulares a menudo se abstendrán de hablar, y esto empobrecerá el intercambio de ideas. Como lo explicó Hugo Black, magistrado de la Corte Suprema de los Estados Unidos, en *Talley c/ California*²⁶, «la única forma en que aquellos grupos y sectas que fueron perseguidos a lo largo de la historia pudieron criticar prácticas y leyes opresivas fue en forma anónima»²⁷. La protección de expresiones anónimas será, por ende, un componente clave de cualquier foro público de expresión donde las personas puedan intercambiar su opinión sin represalias personales y conseguir que sus ideas se aprecien en razón de su mérito.

Si bien estas justificaciones de la defensa de las expresiones anónimas son más persuasivas en el caso del discurso político, las garantías reconocidas en la primera enmienda a las manifestaciones anónimas también se extienden a otros tipos de expresiones. Como lo expresó la Corte Suprema de los Estados Unidos en *McIntyre*:

Los panfletos, volantes, folletos e, incluso, libros anónimos han tenido un rol trascendental en el desarrollo de la humanidad... La decisión del autor de mantener el anonimato puede deberse al temor a sufrir represalias económicas u oficiales, al temor al ostracismo social o simplemente al deseo de preservar, en la mayor medida posible, su privacidad. Independientemente de las razones... las ventajas de que ingresen al mercado de ideas obras anónimas superan indudablemente cualquier interés público que se pueda preservar al exigir la divulgación del autor como condición de acceso. Por consiguiente, la decisión de un autor de mantener el anonimato, al igual que otras decisiones relativas a la omisión o incorporación de contenidos en una publicación, es un aspecto de la libertad de expresión amparada en la primera enmienda²⁸.

Entonces, el anonimato protege la prerrogativa que corresponde al autor de determinar cómo desea presentar sus ideas al resto del mundo.

26. 362 u.s. 60 (1960).

27. 362 u.s. en 64. Véase Tien, *supra* nota 21, pp. 128-29 (donde se explica que McIntyre tiene que ver con el «temor a la discriminación de opiniones, puesto que el anonimato ha estado vinculado históricamente con la posibilidad de que las personas perseguidas o impopulares critiquen prácticas y leyes opresivas»).

28. 514 u.s. en 340.

En este sentido, el anonimato «protege la capacidad de elegir en forma independiente la propia identidad, que constituye un aspecto central de cualquier concepto de libertad»²⁹.

Pese a la importancia de preservar las expresiones anónimas, los Gobiernos de América han intentado debilitar esta protección y exigir que se revele la identidad de los autores y editores, y para ello se han invocado diversos intereses opuestos. Por ejemplo, en *McIntyre*, el poder legislativo intentó justificar una norma que prohibía la distribución anónima de material de campaña, en razón de que, entre otras cosas, conocer la identidad de los autores era necesario para prevenir el fraude y la difamación³⁰. Pese a reconocer la importancia de estos intereses del estado, la Corte Suprema de los Estados Unidos determinó que el estado contaba con medios suficientes para evitar de manera *directa* actos de fraude y difamación en los contextos relevantes, y que la prohibición estatal sobre materiales de campaña anónimos constituía una modalidad indirecta y poco específica de defender estos importantes intereses del estado³¹. Si bien el interés del estado en prevenir el fraude y la difamación podrían justificar la imposición de una obligación de divulgación más limitada³², la Corte Suprema concluyó que la prohibición total de distribución de panfletos anónimos era injustificada³³.

El derecho consagrado en la primera enmienda a expresarse en forma anónima también ha sido reconocido específicamente en el contexto de las comunicaciones a través de Internet. En un caso en el cual se debatió

29. Tien, *supra* nota 21, p. 123.

30. 514 u.s. en 342.

31. *Íd.* en 344.

32. *Íd.*

33. *Íd.* Véase, también, *Watchtower Bible and Tract Society of New York v. Village of Stratton*, 536 u.s. 150 (2002). En *Watchtower*, la Corte Suprema rechazó la justificación invocada por la localidad al exigir que se revelara la identidad y la filiación política de quienes hacían campaña puerta a puerta. La localidad de Stratton, Ohio, intentó justificar esta exigencia al afirmar que se buscaba prevenir el fraude y el delito. La Corte Suprema resolvió que la prohibición total de anonimato en las campañas puerta a puerta que establecía la reglamentación –que se aplicaba no solo a transacciones comerciales y la recaudación de fondos, sino, también, a promotores con fines religiosos o políticos y otras personas que intentaran sumar adeptos a su causa– no era lo suficientemente específica como para impulsar los importantes intereses de la localidad. Por consiguiente, la Corte concluyó que la prohibición total de anonimato en campañas puerta a puerta resultaba injustificada, y se dejó sin efecto la obligación de revelar la identidad de quienes intervenían en estas prácticas.

el derecho a expresarse en forma anónima en el contexto concreto de las comunicaciones en Internet, se determinó que el estado de Georgia había violado la primera enmienda al intentar prohibir todo tipo de comunicaciones anónimas o con seudónimos en Internet. En *Zell c/ Miller*³⁴, Georgia había previsto penas para quienes dieran un nombre falso (y, por consiguiente, se comunicaran en forma anónima o con seudónimos) durante la transmisión electrónica de datos, tales como el envío de mensajes de correo electrónico. La Corte, basándose en *McIntyre*, invalidó esta ley y sostuvo que conculcaba de manera inadmisiblemente el «derecho a comunicarse en forma anónima y con seudónimos a través de Internet», reconocido constitucionalmente³⁵. Si bien reconoció el interés superior del Estado en prevenir el fraude en las comunicaciones a través de Internet, la Corte determinó que la prohibición indiscriminada contenida en la norma de cualquier expresión anónima o bajo seudónimo en Internet no era lo suficientemente específica como para favorecer este interés.

Ciertamente, habrá casos en que un demandante deberá conocer finalmente la identidad de un autor cuyo contenido se señale como ilícito o nocivo para el reclamante. Las garantías de expresión anónima no son absolutas y pueden ser suspendidas, pero siempre en el marco de un procedimiento judicial que tenga en cuenta los intereses tanto del demandante que exige una reparación genuina, como de los demandados que pretenden continuar resguardando sus derechos de libertad de expresión en la mayor medida posible. Admitir el reclamo de una parte que se considera agraviada por un demandado anónimo y permitir que el juez determine si corresponde obligar al intermediario de Internet a que revele la identidad del autor anónimo parecería ofrecer un equilibrio adecuado entre los intereses de ambas partes.

En este sentido, resultan instructivos los esfuerzos de la Justicia estadounidense por buscar un equilibrio entre el derecho de los usuarios de Internet a comunicarse en forma anónima y el derecho a la propiedad, la reputación y la privacidad de terceros. En varios casos recientes en que los demandantes afirmaron haber sido difamados a través de publicaciones anónimas en Internet e intentaron que los proveedores de servicios de

34. Véase *Zell v. Miller*, 977 F. Supp. 1228 (N. D. Ga. 1997). Véase, también, *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 831 (1996) (donde se reconoce la importancia de asegurar el anonimato en línea a interlocutores que intentan acceder a información sensible), ratificada, 521 U.S. 844 (1997).

35. *Zell v. Miller*, 977 F. Supp. 1228.

Internet correspondientes revelaran la identidad de los responsables, la Justicia impuso requisitos estrictos a la pretensión de los demandantes de conocer la identidad de estas personas. Por ejemplo, en *Doe c/2TheMart.com*, la demandante afirmaba haber sido difamada a través de una publicación anónima y exigía que el PSI diera a conocer la identidad del autor del mensaje presuntamente difamatorio. El tribunal aplicó estándares rigurosos a la posibilidad de la demandante de conocer la identidad del autor con el fin de proteger el derecho de este a expresarse en forma anónima. El tribunal estableció que «los pedidos que exigen la identificación de usuarios anónimos de Internet deben ser objeto de un cuidadoso escrutinio por parte de los tribunales», y creó de este modo una exigente prueba que considera múltiples factores para evaluar si la necesidad del actor de conocer esta información prevalece sobre el derecho del autor a expresarse en forma anónima³⁶. Solamente cuando se supere esta prueba estricta, se considerará que el interés del demandante en tener acceso a dicha información para interponer una acción por calumnias supera el derecho del demandado a expresarse en forma anónima. De manera similar, en una decisión reciente en el caso *Independent Newspapers, Inc. c/ Brodie*³⁷, el tribunal formuló los siguientes estándares estrictos, que deberán ser aplicados por los jueces al determinar si corresponde exigir la divulgación de la identidad de quien publica contenidos en forma anónima en Internet:

Quando un tribunal de primera instancia debe resolver una acción por calumnias en la cual intervienen autores anónimos o con seudónimos, debería: (1) exigir al demandante que adopte medidas para notificar a quienes publican contenidos anónimos que han sido objeto de un requerimiento o solicitud tendiente a que se libre una orden de divulgación...; (2) abstenerse de dictar medidas, a fin de conceder al autor anónimo una posibilidad razonable de presentar y notificar su contestación a la solicitud; (3) exigir al demandante que identifique e indique las manifestaciones exactas

36. Véase 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001). Esta prueba cuádruple exige que el tribunal averigüe los siguientes factores al considerar la conveniencia de hacer lugar a un requerimiento para conocer la identidad de personas que publican contenidos en Internet y que no sean parte en un procedimiento: «(1) ¿El requerimiento se presentó de buena fe? (2) ¿La información se vincula con un reclamo o defensa central? (3) ¿La información identificatoria resulta relevante en forma directa y sustancial para el reclamo o la defensa? (4) ¿La información está disponible a través de otras fuentes?»

37. 966 A.2d 432 (Md. Ct. App. 2009).

efectuadas por cada autor anónimo y que supuestamente dan sustento a la acción; (4) determinar si la demanda establece una acción por difamación *prima facie*... contra los autores anónimos y (5), si se cumplen todas las demás condiciones, ponderar el derecho de libertad de expresión del autor anónimo consagrado en la primera enmienda con el valor persuasivo del argumento *prima facie* de difamación presentado por el demandante y la necesidad de dar a conocer la identidad del autor anónimo antes de ordenar que se revelen estos datos.

Es decir, desde su fundación, los Estados Unidos ha reconocido garantías concretas a las expresiones anónimas. La protección del anonimato de quienes expresan ideas es un elemento fundamental del derecho de libertad de expresión consagrado en la primera enmienda. Esta protección también se ha ampliado a las expresiones vertidas en Internet y ha sido resguardada celosamente por la Justicia al sopesar los intereses de las partes agraviadas por estas expresiones con el interés de los autores en preservar el anonimato. El enfoque de los Estados Unidos debería servir como modelo para que otros países de América extiendan la protección al derecho de las personas a expresarse en forma anónima o con seudónimos en Internet.

III. Se debería restringir la capacidad de los Gobiernos de filtrar contenidos de Internet

Además de asegurar que los proveedores de servicios no restrinjan el libre flujo de información en Internet, es crucial que se limite la capacidad de los propios Gobiernos de censurar contenidos en Internet, incluso aquellos que se consideran ilícitos en un determinado país. Cada vez son más los países que filtran las expresiones vertidas en Internet a través de diversos mecanismos, y este tipo de censura se ha convertido en una herramienta poderosa empleada por numerosos Gobiernos –democracias y dictaduras por igual– para controlar las ideas y la información que pueden consultar sus ciudadanos³⁸. Venezuela parece encaminada a sumarse a este grupo

38. Véase Nunziato, Dawn C., «How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide», en *Geo. J. Int'l L.* 42 (2011), p. 1123. Algunos de los contenidos de esta sección han sido extraídos de este artículo.

cada vez más amplio de países. En vista de la magnitud y la efectividad de las medidas implementadas en todo el mundo para censurar la difusión de información a través de Internet, los defensores de la libertad de expresión ya no pueden confiar en la convicción de John Gilmore, uno de los pioneros de Internet, manifestada dos décadas atrás, de que «la red interpreta la censura como un error y encuentra formas de eludirla»³⁹. Las prácticas de censura generalizada en Internet se han extendido más allá de los países que las han aplicado tradicionalmente, tales como China, Arabia Saudita y Corea del Norte, a otros que hasta ahora no habían sido señalados, como el Reino Unido, Canadá y Australia. Si bien los defensores de la libertad de expresión denuncian abiertamente este tipo de censura, es posible que muchos países que han aprovechado estas poderosas herramientas de filtrado continúen limitando los contenidos de Internet y prohíban a los ciudadanos el acceso a contenidos que se consideran nocivos o ilícitos dentro de su territorio. Frente a este tipo de censura, hay dos tipos de respuestas posibles: (1) continuar denunciando abiertamente todo tipo de censura en Internet o (2) instar a que los países, como mínimo, tengan en cuenta ciertas restricciones al limitar las ideas expresadas en Internet, de modo de ser lo más específicos posible y actuar en consonancia con los principios aceptados de debido proceso. En la sección siguiente, me propongo exponer el segundo enfoque. Si bien no es sorprendente que distintos países, en función de sus diferencias históricas y su experiencia nacional, adopten valores sustantivos diversos respecto de qué expresiones desean restringir (*e.g.*, cómo definir y si conviene restringir las expresiones de odio, incitación, negación del Holocausto, pornografía, pornografía infantil, etcétera)⁴⁰, considero que, al implementar prohibiciones a estas categorías de expresión, los países deberían cumplir rigurosamente los requisitos fundamentales de debido proceso para asegurar que los

39. Elmer-Dewitt, Philip, «First Nation in Cyberspace», en *Time International*, 6 de diciembre de 1993.

40. La Convención Americana sobre Derechos Humanos, por ejemplo, protege el «derecho a la libertad de pensamiento y de expresión», y dispone que este derecho no excluye la posterior atribución de responsabilidad cuando sea necesario para asegurar el «respeto a los derechos o a la reputación de los demás» o «la protección de la seguridad nacional, el orden público o la salud o la moral públicas». La Convención establece, asimismo, que «estará prohibida por la ley 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».

ciudadanos que sean objeto de tales restricciones (1) reciban la pertinente notificación, (2) que se definan con precisión y claridad las categorías de expresión prohibidas, de modo que (3) quienes estén alcanzados por tales restricciones tengan una oportunidad genuina de conseguir el control judicial de cualquier decisión que pretenda restringir expresiones.

Las garantías de libertad de expresión no solo tienen una dimensión sustantiva, que se refiere a qué categorías de expresión conviene proteger y cuáles deben ser restringidas –y que varían de un país a otro–, sino que, además, tales protecciones tienen importantes consecuencias procesales que exigen, en los términos de la Corte Suprema de los Estados Unidos, que se implementen «herramientas sensibles» para distinguir las expresiones protegidas de aquellas que no tienen este carácter⁴¹. Tales procedimientos y herramientas sensibles para la protección de la libertad de expresión son tan importantes como las protecciones sustantivas. El juez Frankfurter de la Corte Suprema de los Estados Unidos señaló que «la historia de la libertad estadounidense es, en gran medida, la historia del procedimiento»⁴². Concretamente, los tribunales de los Estados Unidos, al desarrollar los valores sustantivos de libertad de expresión, han aplicado estrictas garantías procesales al escrutinio de las *restricciones previas a la expresión de ideas* –impuestas antes de una resolución judicial sobre la legalidad de la expresión– y han desalentado con firmeza tales restricciones. Esta fuerte presunción de ilegalidad de cualquier restricción previa es compartida también por los países de América Latina que ratificaron la Convención Americana sobre Derechos Humanos, que dispone que el «derecho a la libertad de pensamiento y de expresión... no puede estar sujeto a previa censura...»⁴³.

41. *Bantam Books v. Sullivan*, 372 u.s. 58 (1963).

42. *Malinski v. New York*, 324 u.s. 401, 414 (1945) (voto concurrente del juez Frankfurter).

43. El texto completo del artículo 13 de la Convención Americana sobre Derechos Humanos establece:

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura, sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
 - a) el respeto a los derechos o a la reputación de los demás, o
 - b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

Los sistemas nacionales de filtrado aplican «restricciones previas», es decir, restringen las expresiones antes de que exista una determinación judicial sobre su legalidad. En vez de castigar estas expresiones una vez que han sido publicadas y la Justicia ha determinado su ilegalidad, estos sistemas regulan la expresión de ideas antes de que los tribunales se pronuncien sobre su legalidad. El marco procesal adoptado en los Estados Unidos para evaluar la legalidad de las restricciones previas ofrece un punto de partida a los países que pretenden limitar la potestad gubernamental de bloquear o filtrar contenidos en Internet. En el contexto de medidas de filtrado o bloqueo de alcance nacional de expresiones en Internet, estas garantías requieren, en primer lugar, que toda medida de filtrado que se aplique esté sujeta a *definiciones claras y precisas de las expresiones reguladas*; en segundo lugar, que la estrategia de filtrado *se ponga en práctica de manera abierta y transparente*, de modo que los usuarios de Internet y proveedores de contenidos afectados sean *notificados* sobre el bloqueo y las razones correspondientes; y en tercer lugar, que la estrategia de filtrado conceda a usuarios de Internet y proveedores de contenidos la *posibilidad de apelar tales decisiones sobre bloqueo ante un órgano judicial, de manera expeditiva*. Estos procedimientos por sí solos no indican qué tipo de categorías de expresión deben ser restringidas ni cuáles se consideran nocivas. En lugar de ello, prevén garantías genuinas, de tipo procesal, para la implementación de restricciones a cualquier tipo de categorías de expresiones que un Gobierno considere peligrosas.

A fin de comprender cuáles son los factores en juego en un sistema de esta naturaleza y de qué modo la falta de transparencia y apertura afecta los derechos de usuarios de Internet, consideremos el funcionamiento de

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley 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.

un sistema de filtrado aplicado en un contexto real. Imaginemos un amplio espacio físico real en el cual millones de autores presentan sus obras y las ponen a disposición de miles de millones de potenciales lectores. Los autores dejan sus obras en las estanterías de este foro y luego se retiran. Varios miles de millones de lectores también se acercan al foro para buscar libros que puedan interesarles. Sin que los autores ni los lectores lo sepan, antes de que los libros puedan ser consultados por los lectores —o en algún momento luego de que son colocados en las estanterías—, son controlados por censores ocultos y desconocidos, quienes determinan si el contenido es «permisible» de acuerdo con una serie de criterios que no han sido formulados y no pueden conocerse. Si estos censores determinan que un libro o parte de su contenido es inadmisibles, será incluido en una lista negra y sacado de circulación. Cuando los lectores ingresen al foro para elegir libros que les interesen, no sabrán cuáles han sido quitados, ni los autores de las obras prohibidas se enterarán jamás si sus libros fueron eliminados (ni por qué). Este escenario reproduce en un espacio físico real lo que ocurre en el ciberespacio cuando, mediante sistemas de filtrado, se censuran sitios web y se prohíbe a los usuarios de Internet de un país el acceso a tales contenidos.

En la descripción anterior sobre el espacio físico real, es importante comprender que independientemente de si las restricciones impuestas por el sistema de licencias se producen *ex ante* —es decir, antes de que *cualquier* lector pueda consultar el contenido de los libros— o en algún momento después de la primera circulación de las obras, ambos tipos de restricciones supondrían, en principio, una restricción previa inconstitucional. Las restricciones previas o *ex ante* incluyen aquellas impuestas por comités de censura responsables de examinar contenidos (*e.g.*, películas) antes de su distribución pública,⁴⁴ y los sistemas de filtrado impuestos *ex ante*, como filtros aplicados por Gobiernos (China es un ejemplo) a frases o términos específicos que se consideran nocivos. Por el contrario, las restricciones previas *a mitad de ciclo* incluyen aquellas aplicadas a expresiones luego

44. Véase *Freedman v. Maryland* (comité de censura cinematográfica del estado); Corte I.D.H., caso *La última tentación de Cristo* (*Olmedo Bustos y otros c/ Chile*), sentencia del 5 de febrero de 2001, Serie C, Nº 73 (en la cual el Consejo Nacional de Calificación Cinematográfica de Chile consideró y rechazó la exhibición de la película *La última tentación de Cristo*).

de su circulación inicial, pero antes de una determinación judicial acerca de su ilicitud. Dado que las restricciones previas a mitad de ciclo se aplican antes de que haya un pronunciamiento judicial sobre la ilicitud de los contenidos, existe una presunción constitucional de que se trata de restricciones *ex ante*. Las restricciones previas a mitad de ciclo incluyen sistemas de filtrado que funcionan a partir de listas de sitios web prohibidos, que se renuevan continuamente y que se mantienen en función de datos o denuncias aportados por usuarios de la red.

La Corte Suprema de los Estados Unidos evaluó un caso de restricciones previas a mitad de ciclo en *Bantam Books c/ Sullivan*⁴⁵. En *Bantam Books*, se encargó a la Comisión de Rhode Island de Fomento de la Ética Juvenil (Rhode Island Commission to Encourage Morality in Youth) que investigara a distribuidores de obras impresas obscenas o indecentes y recomendara iniciar acciones penales en su contra. La Comisión examinó diversos libros y revistas que ya se encontraban en circulación y asumió la responsabilidad de notificar a los distribuidores en casos en que se hubieran distribuido libros o revistas que la Comisión considerara objetables. Al examinar la constitucionalidad de este sistema, la Corte Suprema determinó que, aun cuando las restricciones a la publicación se aplicaran después de la circulación y distribución inicial, los actos de la Comisión constituían de todos modos una restricción previa inconstitucional. La Corte explicó que «la distinción entre expresiones legítimas e ilegítimas requiere... herramientas sensibles» y reiteró su exigencia de que la regulación de expresiones debía «respetar celosamente las garantías procesales más rigurosas»⁴⁶. La Corte observó que, en el sistema de Rhode Island, «el editor o distribuidor no tiene derecho siquiera a una *notificación ni audiencia* antes de que su publicación sea calificada como objetable por la Comisión» y que no existía «ninguna disposición sobre *contralor judicial* antes de la emisión de la notificación ni tampoco sobre *revisión judicial* de las determinaciones de la Comisión relativas al carácter objetable de una expresión». Por consiguiente, la Corte concluyó que, en el marco de este sistema de restricción previa a mitad de ciclo, los «procedimientos de la Comisión resultan netamente deficientes e inconstitucionales».

45. 372 U.S. 58 (1963).

46. *Id.* en 66.

III. A. Apertura y transparencia de los sistemas de filtrado

Bantam Books, al igual que otros casos donde se invalidaron sistemas de restricción previa, nos enseña que para que un sistema de este tipo refleje las garantías procesales necesarias, las partes afectadas deben, como mínimo, ser informadas sobre la decisión de censurar el material, de modo que puedan tener una posibilidad real de impugnar la decisión. Esto, a su vez, presupone que las partes afectadas sean *notificadas* sobre cualquier acto de censura, a fin de que tengan una *oportunidad genuina de impugnar* la decisión inicial de censura ante la Justicia. Los sistemas de filtrado que no prevén la obligación de informar a las partes afectadas sobre la censura de contenidos no cumplen este requisito mínimo. Llamativamente, en esta comparación entre apertura/transparencia y secreto/opacidad en el funcionamiento de los sistemas de filtrado, algunos de los países menos proclives a reconocer la libertad de expresión tienen un desempeño más efectivo que el de algunas democracias liberales. En Arabia Saudita, por ejemplo, pese a que el Gobierno aplica un sistema sumamente restrictivo de filtrado de contenidos de Internet, propio de una sociedad estrictamente religiosa, el sistema de filtrado se aplica de manera transparente y abierta, y pareciera notificar suficientemente a los usuarios de ese país que el acceso a Internet está sujeto a restricciones en general, así como sobre los actos de filtrado específicos. Si bien las restricciones a Internet en Arabia Saudita cercenan el derecho a la libertad de expresión desde numerosos ángulos⁴⁷, esas restricciones funcionan de manera transparente y abierta e informan claramente a los ciudadanos sobre qué expresiones han sido suprimidas de Internet y las correspondientes justificaciones. Cuando un contenido es bloqueado en Arabia Saudita (y esto ocurre habitualmente), el Gobierno describe claramente el mecanismo empleado para efectuar el filtrado. Explica a los usuarios de Internet que

47. Por ejemplo, una ley de 2008, de Arabia Saudita, sobre el uso de tecnología establece graves sanciones (que van de multas hasta cinco años de prisión) para el uso de Internet destinado a distribuir contenidos como pornografía u otros materiales que contravengan el derecho público, los valores religiosos o los estándares sociales del Reino. Véase *Access Controlled*, capítulo sobre Arabia Saudita. Se han bloqueado todos los sitios webs sobre religiones alternativas (como aquellos donde se analiza la conversión del islamismo al cristianismo); los sitios web donde se expresan opiniones críticas del islam; los sitios web sobre minorías chiitas; los sitios de defensores globales de la libertad de expresión; los sitios sobre cuestiones relativas a gays y lesbianas y los de educación sexual y planificación familiar. Véase *íd.* en 566-67.

«la Ciudad Rey Abdulaziz para la Ciencia y la Tecnología (King Abdulaziz City for Science & Technology, KACST) mantiene un registro central y un equipo proxy especializado que procesa todas las solicitudes de páginas y las compara con un listado de sitios web prohibidos. Si la página web está incluida entre la lista de páginas prohibidas, se rechaza el pedido»⁴⁸. Con respecto a las justificaciones del filtrado, el Gobierno explica lo siguiente en su página web oficial sobre filtrado:

«Dios Todopoderoso iluminó a la humanidad en el Noble Corán, a través de las palabras del profeta José: Dijo él: “¡Señor! Prefiero la cárcel a acceder a lo que ellas me piden. Pero, si no apartas de mí su astucia cederé a ellas y seré de los ignorantes”. Su Señor lo escuchó y apartó de él su astucia. Él es Quien todo lo oye, Quien todo lo sabe». José (12): 33-34⁴⁹.

Cuando un usuario de Internet en Arabia Saudita intenta acceder a un sitio web incluido en la lista de sitios prohibidos, recibe una notificación en inglés y árabe que indica que «no se permite el acceso al URL solicitado»⁵⁰. A su vez, a cualquier usuario de Internet que recibe este mensaje e intenta apelar la decisión de bloqueo se le indica que puede enviar un pedido de desbloqueo «utilizando los formularios especiales creados para tal fin en la página web de ISU»⁵¹.

De manera similar, en Finlandia, los usuarios que intentan acceder a contenidos que han sido bloqueados por el sistema de filtrado de Internet de alcance nacional reciben el siguiente mensaje, donde se les notifica que el sitio web al cual intentan acceder ha sido bloqueado:

POLICÍA.

ACCESO DENEGADO. Su navegador ha intentado acceder a un sitio que no puede ser visitado en virtud de la ley sobre medidas de prevención de distribución de pornografía infantil. La policía mantiene y actualiza una lista de estos sitios de pornografía infantil⁵².

48. *Íd.*

49. *Íd.*

50. *Íd.*

51. *Íd.*

52. Véase *EFFI, Finnish Internet Censorship*, disponible [en línea] en: <<http://www.ffi.org/blog/kai-2008-02-18.html#how-the-censorship-works>>. [Nota del editor: consultada el 28/10/11.]

Por el contrario, otros países son mucho menos transparentes en la implementación de sistemas de filtrado y operan de modo tal que no se informa a los usuarios de Internet que el sitio web que solicitan ha sido bloqueado, ni tampoco que el país aplica un sistema de filtrado de Internet de alcance nacional. En el Reino Unido, por ejemplo, donde en general existen garantías genuinas para la libertad de expresión, durante los últimos siete años los PSI han implementado un programa de filtrado en Internet de alcance nacional que funciona de manera no transparente. La gran mayoría de los PSI británicos implementan un sistema denominado Cleanfeed para bloquear el acceso a sitios web considerados potencialmente ilícitos por la Internet Watch Foundation (IWF), una organización privada que mantiene una lista de URLs sospechados de alojar contenidos ilícitos que se encuadran en una de las categorías (flexibles) de abuso sexual infantil, incitación al odio racial o contenidos adultos obscenos de tipo delictivos⁵³. Aparentemente, la gran mayoría de usuarios de Internet del Reino Unido desconocen que sus búsquedas en Internet están siendo filtradas de este modo⁵⁴. Asimismo, la implementación de Cleanfeed por los PSI no informa a los usuarios de Internet cuando los sitios que solicitan han sido filtrados o bloqueados. Cuando un usuario del Reino Unido intenta acceder a un sitio web prohibido por la IWF, el usuario (al menos algunas veces) recibe un mensaje de error genérico que indica «404/“archivo no encontrado”», que no transmite ninguna información al usuario de Internet acerca de que el sitio web ha sido excluido⁵⁵. En palabras de la comentarista Lilian Edwards, el sistema Cleanfeed del Reino Unido «podría ser el mecanismo de censura más invisible que jamás se haya inventado»⁵⁶.

El modelo de filtrado silencioso y poco transparente del Reino Unido ha tenido influencia en otros países europeos y también fue adoptado en

53. Véase [en línea]: <<http://www.iwf.org.uk/about-iwf/remit-and-role>>. [Nota del editor: consultada el 28/10/11.]

54. Véase Koumartzis, Nikolaos, *BT's Cleanfeed and Online Censorship in the UK: Improvements for a More Secure and Ethically Correct System*.

55. Véase *op. cit.*, Koumartzis, Nikolaos, *BT's Cleanfeed and Online Censorship in the UK: Improvements for a More Secure and Ethically Correct System*, p. 34 («Cuando se recibe una solicitud de acceso a un URL [prohibido por la IWF], se envía al usuario una respuesta de tipo «404», con el mensaje «página no disponible»).

56. Edwards, Lilian, *From Child Porn to China, in One Cleanfeed* (DOI: 10.2966/scrp.030306.174), disponible [en línea] en: <<http://www.law.ed.ac.uk/ahrc/script-ed/vol3-3/editorial.asp>>. [Nota del editor: consultada el 28/10/11.]

Canadá. En 2006, el PSI más importante de Canadá puso en marcha Project Cleanfeed Canada, un proyecto que se formuló sobre la base del modelo Cleanfeed del Reino Unido, junto con Cybertip.ca, una organización policial canadiense. Al igual que en el Reino Unido, los analistas de Cybertip.ca adoptan decisiones sobre contenidos potencialmente ilícitos e incluyen los URL sospechosos en la lista de distribución Cleanfeed. Luego, los PSI canadienses bloquean los URL que fueron incluidos en la lista de distribución Cleanfeed⁵⁷. Y, como en el Reino Unido, no se informa a los usuarios de Internet que el contenido que están buscando ha sido filtrado. En lugar de ello, los usuarios de Internet reciben un mensaje estándar de error que indica que el sitio web no está disponible⁵⁸.

Los países que implementan sistemas de filtrado de alcance nacional para restringir el acceso de sus ciudadanos a contenidos que consideran nocivos deberían, como mínimo, operar estos sistemas de manera abierta y transparente, en consonancia con los requisitos fundamentales del debido proceso adjetivo. Estos sistemas deberían operar de manera tal que (1) se comunique a los usuarios de Internet sobre la aplicación de estos sistemas de filtrado en general y (2) se informe específicamente a los usuarios afectados en casos en que se apliquen filtros para bloquear el acceso a un sitio web en particular. Solamente entonces se habrá informado a los proveedores de contenidos y usuarios afectados con la suficiente antelación para que puedan cuestionar la decisión del censor y someterla a control judicial.

III. B. Deben definirse y delinear claramente todas las categorías de expresiones prohibidas

Otro requisito procesal mínimo para cualquier sistema de filtrado de contenidos de Internet es que las facultades discrecionales del censor estén verdaderamente acotadas por pautas claramente definidas y precisas. Este

57. Véase *supra* nota 47, *Access Controlled*.

58. El sitio web de Cybertip indica en su página sobre Preguntas frecuentes:

¿Pueden las personas saber qué direcciones se filtran mediante este sistema?...

No. Reciben un mensaje estándar que indica que no pueden acceder a la dirección de Internet.

Véase [en línea]: <<http://www.cybertip.ca/app/en/cleanfeed>>. [Nota del editor: consultada el 28/10/11.]

requisito permite confinar y restringir la discrecionalidad del primer censor y exigir que respete la determinación legal acerca de qué contenidos pueden ser proscriptos. Si bien los países pueden tener divergencias en su determinación de las categorías de expresión que son ilícitas –pornografía, expresiones de odio, negación del Holocausto, etcétera–, es importante que, dentro de cada país, las definiciones de expresiones ilícitas y, en especial, las definiciones de aquellas sujetas a restricción previa, estén definidas de manera precisa y cuidadosa, y se limite de esta manera la discrecionalidad del censor inicial. La Corte Suprema de los Estados Unidos, por ejemplo, ha examinado minuciosamente la discrecionalidad de los censores en los sistemas de restricción previa y ha rechazado como inconstitucional cualquier sistema que asigne discrecionalidad absoluta para determinar si una expresión está protegida. Por ejemplo, en *Shuttlesworth c/ Birmingham*⁵⁹, la Corte evaluó la constitucionalidad de un sistema de autorización de desfiles que concedía a la Comisión de la Ciudad amplia discrecionalidad para negar permisos en casos donde «a criterio de la Comisión, el bienestar social, la paz, la seguridad, la salud, la decencia, el orden, la moral o la conveniencia requieran que se deniegue autorización para el desfile»⁶⁰. Al responder a una acción que impugnaba esta ley, la Corte determinó que, en tanto el sistema de permisos constituía una restricción previa a la expresión que otorgaba «facultades prácticamente irrestrictas y absolutas» a la Comisión, no se correspondía con el requisito esencial del debido proceso que dispone que cualquier ley que supedita el ejercicio de las libertades de la primera enmienda a la restricción previa de una licencia debe incorporar estándares «estrictos, objetivos y definidos que orienten la potestad de licencia»⁶¹.

Exigir que los criterios aplicados por la autoridad censora al decidir se establezcan con precisión contribuye a circunscribir la discrecionalidad administrativa y también ayuda a limitar el posible desvío de la misión del órgano censor. Sin una especificación precisa y detallada de los criterios de censura, el censor puede ejercer una discrecionalidad indiscriminada en la limitación de las expresiones.

No es sorprendente que los países que filtran el contenido de Internet en mayor medida también tengan las definiciones más amplias y vagas

59. 394 U.S. 147 (1969).

60. *Íd.* en 149-50.

61. *Íd.* en 150-51.

sobre cuáles son los contenidos sujetos a censura. China, por ejemplo, aplica filtros obligatorios a contenidos que «perturben la solidaridad de los pueblos», «atenten contra la integridad de la unidad nacional» o «dañen el honor o los intereses nacionales»⁶². De forma similar, como ha sido discutido más arriba, Venezuela tiene la intención de establecer un punto único de acceso a la red con el objetivo de impedir que sus ciudadanos accedan a expresiones dirigidas a «fomentar zozobra en la ciudadanía o alterar el orden público». Los ejemplos de China y Venezuela representan justamente el tipo de discrecionalidad sin estándares que no aplica limitaciones genuinas a los censores ni informa a los usuarios de Internet afectados cuáles son las expresiones que han sido censuradas.

III. C. Los sistemas de filtrado deberían contemplar la posibilidad de apelar las determinaciones

Existen consideraciones de debido proceso aplicables a la libertad de expresión que exigen que cualquier decisión inicial de censurar contenidos debe estar *sujeta a un control judicial inmediato* a través de un *procedimiento contradictorio*. Los tribunales estadounidenses han señalado la importancia

62. China restringe los contenidos de Internet que se encuadran en alguna de las siguientes categorías, en tanto:

- vulneren los principios básicos confirmados en la Constitución;
- pongan en riesgo la seguridad del Estado, divulguen secretos de Estado, subviertan el régimen nacional o menoscaben la integridad de la unidad nacional;
- dañen el honor o los intereses nacionales;
- inciten al odio entre pueblos, el racismo contra pueblos o perturben la solidaridad de los pueblos;
- perturben las políticas nacionales sobre religión y propaguen cultos malignos y supersticiones feudales;
- difundan rumores, alteren el orden social o perturben la estabilidad social;
- difundan materiales obscenos, pornografía, el juego, la violencia, el terror o instiguen la comisión de delitos;
- insulten o difamen a terceros y cercenen derechos e intereses legítimos de terceros;
- contengan otros contenidos prohibidos por la ley y las reglamentaciones administrativas;
- inciten a la conformación de asambleas, asociaciones, marchas, manifestaciones o reuniones ilícitas que perturben el orden social; y
- realicen actividades en nombre de una organización civil ilícita. Véase *supra* notas 47 y 57, *Access Controlled*, en 478.

de la disponibilidad de un *control judicial expeditivo* de las decisiones de censura en el contexto de las restricciones previas⁶³. Como lo explicó la Corte Suprema de los Estados Unidos, «únicamente una determinación judicial adoptada en el marco de un proceso contradictorio podría asegurar que se considere debidamente la libertad de expresión y, por ende, solamente un procedimiento que exija una determinación judicial servirá para imponer una restricción [previa] definitiva que sea válida»⁶⁴. Para que un sistema de filtrado pueda aplicar una restricción previa válida, el sistema en cuestión deberá notificar a las partes afectadas y permitir un control judicial expeditivo de la decisión inicial sobre censura⁶⁵.

La Justicia ha determinado la inconstitucionalidad de los intentos realizados dentro de los Estados Unidos para aplicar filtros a contenidos nocivos en Internet a nivel de los PSI, en tanto no contemplan ningún tipo de control judicial (inmediato o de otra índole) de la decisión del censor en el marco de un procedimiento contradictorio. En *Center for Democracy and Technology c/ Pappert*, por ejemplo, el estado

63. Véanse *Thirty-Seven Photographs*, 402 u.s. en 372-74; *Kingsley Books, Inc. v. Brown*, 354 u.s. 436 (1957); *Interstate Circuit, Inc. v. City of Dallas*, 390 u.s. 676 (1968) y *Bantam Books, Inc. v. Sullivan*, 372 u.s. 58 (1963).

64. Véase *United States v. Pryba*, 502 F.2d 391, 405 (D.C. Cir. 1974).

65. Para conocer la interpretación de la Corte sobre el requisito de celeridad, véanse *supra* nota 65, *Thirty-Seven Photographs*, 402 u.s. en 372-74 (en donde se muestra que son admisibles las demoras en las resoluciones judiciales de hasta tres meses; por consiguiente, debe interpretarse que una ley federal que aplique restricciones previas requiere de una determinación judicial en el término de sesenta días que confirme la constitucional de la norma); *Kingsley Books, Inc. v. Brown*, 354 u.s. 436 (1957) (donde se exigió el juicio un día después de trabada la litis y la resolución dos días después del juicio); *Interstate Circuit, Inc. v. City of Dallas*, 390 u.s. 676, 690 n. 22 (1968) (donde se resuelve que el control judicial inmediato estaba garantizado por la disposición que exigía una determinación judicial en un plazo de nueve días a partir de la resolución del órgano administrativo); *Bantam Books, Inc. v. Sullivan*, 372 u.s. 58, 70 (1963) (donde se señala que la restricción previa de las expresiones podía ser «tolerada... únicamente... si se aseguraba una determinación judicial prácticamente inmediata sobre la validez de la restricción») y *Redner v. Dean*, 29 F.3d 1495, 1501-02 (11th Cir.1994) (que determina que no existe control judicial inmediato cuando se exige agotar previamente todas las instancias administrativas y el sistema no impone restricciones temporales adecuadas a la decisión administrativa), *se rechaza pedido de revisión*, 514 u.s. 1066 (1995); cf. con *East Brooks Books, Inc. v. City of Memphis*, 48 F.3d 220, 225 (6th Cir.1995) (donde se indica que una demora potencial de cinco meses desde la solicitud de vista judicial resulta inadmisibles).

de Pensilvania (Commonwealth of Pennsylvania) intentó combatir la pornografía infantil en Internet sancionando la Ley sobre Pornografía Infantil en Internet (Internet Child Pornography Act), que exigía a los PSI que prestaban servicios a residentes de Pensilvania bloquear el acceso a sitios web presuntamente vinculados con este tipo de contenidos. La ley permitió que el Fiscal General de Pensilvania o los fiscales de distrito solicitaran al tribunal que, sin audiencia de parte, exigiera al PSI que quitara o deshabilitara el acceso a contenidos disponibles a través del servicio del PSI, cuando se demostrara que existía causa probable de que el contenido constituyera pornografía infantil. La ley no exigía una determinación concreta ni definitiva de que el material eliminado constituyera efectivamente pornografía infantil antes de su inclusión en la lista de sitios prohibidos. En consulta con los PSI afectados, la Fiscalía General decidió implementar la ley incluso sin solicitar que se dictaran órdenes judiciales *ex parte* y proporcionara, en vez, las denominadas Notificaciones Informales de Pornografía Infantil a los PSI que alojaban sitios web que hubieran sido denunciados por un agente o ciudadano y que la Fiscalía General hubiera identificado como posible pornografía infantil. La Notificación Informal ordena al PSI que quite el material presuntamente pornográfico o deshabilite el acceso a este para los residentes de Pensilvania en un plazo de cinco días desde la recepción de la notificación.

La ley fue objetada, entre otras razones, por imponer restricciones previas inconstitucionales sin las debidas garantías procesales. En defensa de la ley, el fiscal general explicó que solamente se había pedido que se eliminaran contenidos cuando, a criterio de la fiscalía, existían causas razonables para creer que se trataba de pornografía infantil. El tribunal determinó que la demostración de causa probable no validaba la ley (ni tampoco el hecho de que el fiscal general emitiera simplemente Notificaciones Informales en vez de órdenes judiciales y que, por consiguiente, el proceso fuera «voluntario» y no coercitivo⁶⁶). En primer lugar, el tribunal explicó que para que se cumplieran los estrictos requisitos de la Corte Suprema

66. Sobre este aspecto, el tribunal señaló que la naturaleza informal y técnicamente no coercitiva de los pedidos de cancelación de contenidos del fiscal general no lo eximían del control constitucional. El tribunal explicó que los pedidos de cancelación presentados por funcionarios de aplicación de la ley no eran interpretados por los PSI destinatarios como voluntarios, aun cuando técnicamente no tenían fuerza de ley.

sobre constitucionalidad, una restricción previa válida y definitiva debía ser resuelta mediante determinación judicial dictada en el marco de un procedimiento contencioso. La determinación del fiscal general acerca de que existía causa probable de que el material fuera ilícito resultaba insuficiente. Asimismo, tampoco bastaba para que la restricción previa definitiva fuera constitucional una determinación judicial sin audiencia de parte que resolviera que el material era ilícito, ya que esta no sería adoptada en el marco de un procedimiento contencioso. La Corte Suprema de los Estados Unidos señaló en *Freedman* que «únicamente una determinación judicial adoptada en el marco de un proceso contradictorio podría asegurar que se considere debidamente la libertad de expresión»⁶⁷. Las resoluciones judiciales que se adoptan *ex parte*, sin notificar al autor que será censurado y sin concederle posibilidad de audiencia, son constitucionalmente deficientes, y aún más lo son las determinaciones *ex parte no judiciales*.

Muchos de los sistemas de filtrado implementados en otros países prevén algún tipo de apelación de las decisiones de censura. Sin embargo, tales disposiciones sobre apelación en general no contemplan la determinación *judicial* y simplemente prevén un segundo control a cargo del mismo órgano administrativo que tomó la decisión de censura. En el Reino Unido, por ejemplo, el sitio web de la IWF indica que «cualquier parte que tenga un vínculo legítimo con el contenido [prohibido]... y que considere que está siendo privada del acceso a contenidos lícitos podrá apelar [enlace obsoleto] la determinación para que se revea su procedencia»⁶⁸. No obstante, el procedimiento de apelación establecido por la IWF no contempla el control judicial. (A su vez, como se señaló precedentemente, no resulta claro de qué manera una parte podría enterarse de que el contenido que está buscando o que pretende publicar fue incluido en la lista de sitios prohibidos de la IWF, puesto que el sistema Cleanfeed simplemente muestra a los usuarios de Internet un mensaje genérico de error de tipo «404/archivo no encontrado» cuando se intenta acceder a un sitio web de la lista.) La apelación consiste en una segunda evaluación por parte de la misma IWF y, posteriormente, una revisión a cargo de un organismo de policía, que adopta una determinación

67. *Freedman v. Maryland*, 380 u.s. 51 (1965).

68. Véase [en línea]: <<http://www.iwf.org.uk/services/blocking/blocking-faqs#WhisthethercriterionforaURLtobeaddedtothelist>>. [Nota del editor: consultada el 28/10/11.]

definitiva⁶⁹. De manera similar, el sistema de filtrado canadiense Cybertip permite al proveedor de contenidos afectado apelar la decisión inicial sobre censura, pero el proceso de apelación no contempla una instancia de control judicial. En lugar de ello, el proceso de apelación canadiense prevé un segundo examen a cargo de personal de Cybertip Canada y, posteriormente, una revisión ante el Centro de Coordinación Nacional sobre Explotación Infantil (*National Child Exploitation Coordination Centre*), una rama del Centro Policial Canadiense para Niños Desaparecidos y Explotados (*Canadian Police Centre for Missing and Exploited Children*)⁷⁰, cuya decisión tiene carácter definitivo⁷¹. Estas disposiciones sobre apelación, en tanto no contemplan una determinación judicial sobre los derechos de las partes afectadas, no ofrecen las estrictas garantías de la libertad de expresión. En resumen, los sistemas de filtrado de alcance nacional –que están siendo aplicados en más de cuarenta países en todo el mundo, a los cuales, aparentemente, en breve se sumaría Venezuela– contemplan restricciones previas a las expresiones que resultan incompatibles con los compromisos articulados en la Convención Americana sobre Derechos Humanos y que vulneran los requisitos de debido proceso inherentes a la garantía de libertad de expresión, en tanto no prevén garantías procesales fundamentales. Estos requisitos procesales sobre el debido proceso exigen que tales restricciones previas impuestas por sistemas de filtrado estén sujetas a *definiciones claras y precisas de las expresiones reguladas*, que se implementen *de manera abierta y transparente*, de modo que los usuarios de Internet y proveedores de contenidos afectados sean informados sobre el bloqueo y las razones correspondientes y que el sistema de filtrado conceda a usuarios de Internet y proveedores de contenidos la *posibilidad de apelar tales decisiones sobre bloqueo*, ante un *órgano judicial, de manera expeditiva*. Solamente mediante la aplicación de estas «herramientas sensibles» para distinguir las expresiones protegidas de aquellas no protegidas se podrá garantizar adecuadamente el derecho de libertad de expresión de las personas.

69. Véase Proceso de Apelación de la Evaluación de Contenidos de iwf [en línea]: <<http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process>>. [Nota del editor: consultada el 28/10/11.]

70. Véase [en línea]: <<http://www.rcmp-grc.gc.ca/ncecc-cncee/index-accueil-eng.htm>>. [Nota del editor: consultada el 28/10/11.]

71. Véase [en línea]: <http://www.cybertip.ca/app/en/Cleanfeed_p1#anchor_menu>. [Nota del editor: consultada el 28/10/11.]

IV. Conclusión

A fin de preservar y proteger Internet como foro para el intercambio libre, abierto e intenso⁷² de ideas e información en América, los Gobiernos deben adoptar medidas concretas tendientes a facilitar estos valores propios de la libertad de expresión. En este sentido, la relación entre Gobierno y proveedores de servicios de Internet reviste crucial importancia, en tanto los PSI, por la posición que ocupan, están en condiciones de facilitar la libre circulación de información e ideas. Por un lado, no se debería limitar a los PSI atribuyéndoles responsabilidad de intermediarios por alojar contenidos nocivos. Y, por otro lado, tampoco se debería reconocer a los PSI discrecionalidad para restringir aquellas comunicaciones que circulan a través de sus canales y que estos desapruaban por algún motivo. Deberían, en cambio, estar sujetos a reglamentaciones efectivas sobre neutralidad en la red, que les exijan facilitar todo tipo de comunicaciones sin discriminación ni censura. Con el fin de favorecer el libre flujo de información en Internet, los Gobiernos deberían, además, brindar garantías a los usuarios de Internet para que puedan expresarse en forma anónima o con seudónimos. Estas garantías son un aspecto integral del derecho a expresarse en forma crítica en el ámbito civil y político, y deben ser preservadas en la era de Internet. Por último, los mismos Gobiernos deberían abstenerse de censurar expresiones en Internet y actuar, así, en consonancia con el compromiso común de los países de América de renunciar a cualquier restricción previa de las expresiones. No obstante, cuando los Gobiernos *sí* decidan aplicar filtros a los contenidos ilícitos en Internet –como sucede actualmente en numerosos países de todo el mundo–, deberían asegurarse de que estos sistemas de filtrado exigidos por el Estado se adecuen a procedimientos que favorezcan, en la mayor medida posible, la libertad de expresión y apliquen «herramientas sensibles» para distinguir las expresiones protegidas de aquellas que no tienen este carácter.

72. *New York Times v. Sullivan*, 376 U.S. 254, 268 (1964) (donde se menciona un «profundo compromiso nacional con el principio que indica que el debate sobre cuestiones de interés público debe ser libre, intenso y abierto»).

Responsabilidad de los proveedores de servicios de Internet (ISPs) en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica

Claudio Ruiz Gallardo y Juan Carlos Lara Gálvez

Introducción

La masificación de las nuevas formas de comunicación mediadas a través de la tecnología ha supuesto diversos problemas y desafíos para la regulación. Tal vez uno de los temas donde mayor conflicto y sensibilidad surge desde el punto de vista de la importancia de los modelos económicos asociados y de la colisión con otros derechos de orden constitucional, particularmente con la libertad de expresión, tiene que ver con los mecanismos de determinación de responsabilidad legal. Como se sabe, la utilización de las redes digitales ha supuesto el traslado de múltiples aspectos todavía discutidos respecto de la responsabilidad civil de un nuevo entorno, con la dificultad que ello implica.

Cuando se trata del contexto en línea, al menos *a priori*, la infraestructura tecnológica no parece ser un obstáculo de orden normativo para el ejercicio de la libertad de expresión. En un principio, con la proliferación de *bulletin boards systems* (sistemas de tablón de anuncios), la posterior emergencia de listas de correos y la masificación del correo electrónico supuso una comunicación que se graficaba como esencialmente descentralizada y que se producía a través de protocolos de comunicación que permitían dichos intercambios. Pero será particularmente a partir de las posibilidades técnicas que permiten intercambios de intangibles, que surgen de estas redes digitales y en los últimos años la proliferación, el *boom* de las llamadas redes sociales, que se hará evidente la importancia normativa de esta infraestructura para el

ejercicio de derechos. Es que, de alguna manera, estos actos comunicativos tienen en común la necesidad de una infraestructura tecnológica. Esta, a su vez, es operada por los denominados prestadores de servicios de Internet, quienes no solo operan, sino que además tienen la posibilidad de controlar aquello que circula a través de sus redes.

De allí la importancia, siempre desde el punto de vista regulatorio, del establecimiento de criterios estrictos que garanticen la neutralidad de la red y, en el caso de Marras, la importancia y la necesidad de establecer un sistema que se haga cargo de la responsabilidad de quienes tienen la posibilidad técnica de poder controlar usos alejados de lo que indica el texto de la ley. Por esta y otras razones, pareciera ser que las medidas que la autoridad tome respecto de estos prestadores es no solamente deseable, sino necesaria, a efectos de prevenir la comisión de delitos e infracciones mediante las comunicaciones realizadas mediante esta crucial infraestructura. Es interesante como a nivel internacional no existen criterios claros al respecto. En tal sentido, propuestas diversas para poner el control (al menos, parcial) de las comunicaciones en manos de dichas instituciones han sido presentadas en el continente, y hasta hoy se discuten con distinto grado de conocimiento y participación social.

El presente artículo tratará de analizar tales propuestas a la luz de los derechos fundamentales reconocidos a nivel regional y a la eventual consecuencia de esa intervención legal en el desarrollo de las libertades y derechos comúnmente ejercidos a través de los medios de comunicación que se soportan en redes digitales, así como también con miras a la protección de los intereses de quienes se pudieran ver afectados por tales actos. En especial, se tratará de obtener conclusiones sobre la mejor forma de hacer efectiva la responsabilidad de los agentes intermediarios de la comunicación, allí donde parezca razonable hacer valer tal responsabilidad, y bajo qué mecanismo posible permitir la verificación de un equilibrio entre los distintos intereses en juego, teniendo en cuenta la experiencia comparada.

¿Debe o no ser el facilitador técnico responsable de los actos comunicativos constitutivos de delito o infracción? ¿Qué justificaría una intervención sobre las comunicaciones de los usuarios? En aquellos casos donde tales preguntas han sido resueltas, por la vía legal o judicial, ¿se ha entregado una respuesta óptima, que no perjudique a los usuarios que se comunican a través de Internet, ni a los agentes económicos encargados de la prestación del servicio? Son solo parte de las preguntas que es necesario dar respuesta cuando se trata de la responsabilidad de intermediarios en Internet.

I. Estudio de países

La diversidad de las realidades normativas en Latinoamérica obliga en este espacio a acotar nuestro campo de estudio. Por este motivo, consideramos prudente reducir este análisis a países que han demostrado ciertas situaciones especiales de desarrollo de estas áreas, primordialmente en lo que se refiere a las iniciativas legales de reciente data. Por lo tanto, el énfasis de las siguientes páginas se pondrá en los rasgos comunes y particulares existentes en la Argentina, Brasil, Chile y Colombia.

I.A. La regulación de los proveedores de Internet

Los actos de comunicación a través de Internet, sea cual sea su contenido, requieren atravesar una infraestructura tecnológica compleja, compuesta por muy diversos elementos físicos y lógicos, cada uno de los cuales está a cargo de un operador. Por supuesto, la participación de dichos operadores está sujeta a las regulaciones establecidas en cada territorio, sea dentro de la normativa relativa a servicios de comunicación en general o bien, de forma específica, para la prestación de aquellos servicios que son propios de Internet. De la misma manera, es posible encontrar diferencias de regulación en virtud del cumplimiento de reglas nacionales sobre concentración económica de empresas en relación con su nivel de participación en el mercado respectivo.

La relevancia de tales distinciones radica en que cada una de esas formas de operación podría, en teoría, dar lugar a una forma distinta de responsabilidad, en función del modo en que el contenido o acto comunicativo tiene lugar en cada una de las etapas envueltas en la comunicación que se da a través de Internet. En la medida en que cada operador controla una etapa, y en consecuencia, tiene la capacidad técnica para permitir la circulación de un contenido supuestamente delictivo o infractor de derechos ajenos, estaremos en presencia de un intermediario que facilita esa comunicación. Como es lógico, tal intermediario tendrá, también, la capacidad técnica para impedir la circulación de esa comunicación.

En tal sentido, podemos caracterizar los servicios de Internet de formas distintas según su carácter funcional¹:

(a) un *proveedor de acceso*, que presta el servicio que conecta al ordenador de usuario final, mediante cables o señales inalámbricas e, incluso, mediante el facilitamiento del equipo mediante el cual se accede a Internet;

(b) un *proveedor de tránsito*, que permite la interacción entre el ordenador final y el proveedor de acceso con los *proveedores de alojamiento*, sin tener más función que la de mero transporte de datos (*mere conduit*);

(c) un *proveedor de alojamiento*, que cuenta con uno o varios ordenadores con espacio disponible o «servidores», con acceso a los proveedores de tránsito, a fin de utilizarlos con sus propios fines o de ponerlos a disposición de terceros que, en uso de ese alojamiento, tengan contenido accesible desde otros ordenadores conectados a los proveedores de acceso y tránsito. Proveen tecnologías que permitirán servicios diferenciados para la visualización en la web, para envío, recepción y administración de correo electrónico, para el alojamiento de archivos, etcétera. Subdistinguimos aquí entre los que prestan alojamiento con el propósito de facilitar el funcionamiento de la red a través del almacenamiento automático, provisional y temporal de datos o *caching* y los proveedores comerciales o no de alojamiento permanente o, al menos, no meramente provisional o *hosting*;

(d) un *proveedor de contenidos*, que es como denominamos a quienes utilizan la infraestructura antes mencionada para poner a disposición de personas con ordenadores conectados servicios de la más diversa naturaleza, incluyendo páginas informativas, servicios, correo electrónico, conexión entre distintos usuarios finales y un largo etcétera cuyo límite es solo dado por la imaginación y mediante la entrega de contenidos provistos por el propio proveedor o bien, mediados y provenientes de terceros. Asimismo, dentro de los servicios de provisión de contenidos, podemos separar del resto a los proveedores de servicios de búsqueda y enlace de contenidos en Internet, en atención a la especial

1. Esta distinción entre servicios, si bien es propia, toma como base de lenguaje a la Directiva 2000/31/CE del Parlamento Europeo y del Consejo y a la recogida por Maturana, Cristian, «Responsabilidad de los Proveedores de Acceso y Contenido en Internet», en *Revista Chilena de Derecho Informático*, 1 (2002).

forma que ellos tienen de interactuar con los demás contenidos de la red, que ha redundado en el tratamiento diferenciado de ellos por la jurisprudencia y por recientes reformas legales propuestas.

Las diferencias en los aspectos organizacionales y económicos entre tales operadores (esto es, si la capacidad operativa y económica de uno o varios de tales elementos de la infraestructura comunicacional de Internet está o no concentrada) no serán relevantes a los efectos del presente informe. Sin perjuicio de ello, de la práctica observada a nivel continental, la forma en que se relacionan los distintos proveedores con sus usuarios es como proveedores de acceso y tránsito, como proveedores de telecomunicaciones que, además, permiten acceder a Internet, mientras que el contenido de Internet propiamente es manejado y puesto a disposición por distintos proveedores de contenidos, que pueden o no ser, además, dueños de los servidores que alojan tales contenidos.

Esta última división entre proveedores de servicios vinculados a la conexión y proveedores de servicios vinculados a la entrega de contenido resulta especialmente relevante a efectos de estudiar la aplicación de responsabilidad: proveedores de alojamiento y contenido tienen un alcance potencialmente global; los proveedores del servicio a usuarios finales o de conexión dentro de un territorio estarán, usualmente, sujetos a las limitaciones geográficas y legales de tales territorios. Es decir, una misma página puede ser vista en todo el mundo, pero los proveedores de conexión variarán junto con los ordenadores finales que realicen el acceso. La consecuencia lógica es que, en aquel territorio donde los proveedores del servicio de conexión y acceso tengan su ámbito de actuación, deberán obedecer la regulación del territorio; en tanto que, los proveedores de alojamiento y contenido estarán, eventualmente, sujetos a reglas en cualquier parte del mundo en que su contenido sea accesible. A efectos de hacer más fácilmente comprensible el análisis de estas materias, hablaremos, por una parte, de *proveedores de conexión* para referirnos a quienes prestan los servicios de acceso, conexión e infraestructura de conexión que permiten el acceso a Internet y la transmisión de datos; por otra, de *proveedores de alojamiento* para referirnos a quienes ponen a disposición de otros la posibilidad de mantener contenidos en la red y, finalmente, de *proveedores de contenido* para referirnos a quienes ponen a disposición de la generalidad de los usuarios diversos contenidos o servicios, sean ellos provistos o no por sí mismos.

Por cierto, cada país tiene sus propias normas respecto de la entrega del servicio en la relación entre el usuario final y el proveedor de acceso

a Internet². No es ello el centro del presente estudio, sino el rol y la responsabilidad del proveedor de acceso a Internet, en tanto intermediario, respecto de los actos de comunicación de sus usuarios. La pregunta general ante ese escenario es en torno a cuáles son las reglas de responsabilidad que rigen sobre dichos proveedores de acceso y conexión y sobre los proveedores de contenidos. Si todos ellos son nexos intermediarios entre un emisor y los actuales o potenciales receptores de un acto comunicativo o expresivo, cuáles serán las reglas de responsabilidad que mediarán a esa comunicación. Del mismo modo, allí donde un proveedor de contenido preste un servicio que permita que personas distintas de él, tales como sus clientes o usuarios, pongan a disposición contenidos o realicen actos de comunicación mediante los servicios por ellos prestados, podrían convertir a esos prestadores también en responsables de las consecuencias de dichos actos.

Esas preguntas, a nivel regional, presentan una respuesta general en sentido negativo. En términos generales, no existen regulaciones nacionales que afecten de forma directa y específica a los proveedores de conexión a Internet; salvo excepciones, también, los proveedores de contenido tampoco están sujetos a reglas especiales.

Esto tiene, por cierto, algunos matices. Debemos consignar, en primer término, que el rasgo de ausencia de regulación especial para la responsabilidad de los proveedores de servicios de Internet (o proveedores de contenidos, en su caso), no implica que no se pueda hacer valer responsabilidad civil respecto de ellos, sino que esa tarea estará entregada a las normas generales sobre responsabilidad, con lo que hacer valer esta será un asunto más complejo. El segundo punto por resaltar es que, si bien regionalmente son escasas las regulaciones específicas para la responsabilidad civil de los prestadores de servicios de Internet y de los proveedores de contenido, esa ausencia de regulación especial comienza a ser abandonada. Primero, a través de tratados internacionales, fundamentalmente de libre comercio o de cooperación mercantil, que ponen

2. La relación entre la persona que contrata una conexión a Internet y la entidad que provee dicho servicio es, en rigor, un vínculo de consumo o de servicio. Es de ese modo que las obligaciones relacionadas con la prestación de dicho servicio se encuentran reguladas en los distintos países, como, por ejemplo, en Brasil, a través del Código de Defesa do Consumidor (Lei N 8078/90), o bien considerado el servicio como uno entre varios servicios de telecomunicaciones, como ocurre en Chile a través de la Ley General de Telecomunicaciones (18168, de 1981).

a los países en obligación de introducir cambios legales a este respecto; adicionalmente, con leyes de reciente aprobación en Chile³; y luego, con propuestas de reforma hoy en curso en la Argentina⁴, Brasil⁵ y Colombia⁶, sobre las cuales volveremos más adelante.

II. La responsabilidad legal aplicada a los proveedores de servicios de Internet

Para referirse a las consecuencias legalmente impuestas por la incursión en conductas indeseadas, suele distinguirse entre responsabilidad penal y responsabilidad civil. Es responsabilidad penal la referida al cumplimiento de sanciones establecidas por ley por la comisión de actos que la sociedad prohíbe y califica como crímenes o delitos. En tanto que, cuando nos referimos a responsabilidad civil, en términos muy generales, hablamos del sistema que establece que quien mediante su conducta (activa o, en ciertos casos, pasiva) produce un daño a otro (en su persona o su patrimonio) está obligado a reparar económicamente ese daño. Ambas formas de responsabilidad pueden coexistir: quien comete un delito deberá no solamente enfrentar las sanciones que la ley establece, en detrimento de sus derechos o libertades, sino, también, realizar el desembolso económico (en dinero) para que los afectados por su ilícito sean compensados por el perjuicio sufrido.

3. Ley 20435 que modifica a la Ley de Propiedad Intelectual, del 5 de mayo de 2010.

4. Proyecto de Expediente 8793-D-2010, Trámite Parlamentario número 208 (22 de febrero de 2011), sobre Régimen para Proveedores del Servicio de Internet.

5. El proceso brasileño de modificación legal destinado a afectar el régimen de responsabilidad de los prestadores de servicio de Internet se inició dentro del proceso de reforma de su legislación de derechos de autor y, en especial, de la Lei de Direitos Autorais 9610, de 1998. Con diversos altibajos, controversias y cambios en la dirección gubernamental que han obviado la activa participación civil en el proceso, su éxito está todavía en duda. No obstante, existen ya anteproyectos en discusión. Para una completa línea de tiempo, véase, Paranaguá, Pedro, «Brazil's Copyright Reform: Are We All Josef K.?», en *Intellectual Property Watch* [en línea], en: <<http://www.ip-watch.org/weblog/2011/05/12/brazil%E2%80%99s-copyright-reform-are-we-all-josef-k/>>. [Nota del editor: consultada el 5/11/11.]

6. Proyecto 241 de 2011, por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet.

Una consecuencia fundamental de esta distinción entre responsabilidad civil y responsabilidad penal radica en la posibilidad de hacer valer una u otra. La aplicación de la responsabilidad penal está necesariamente sujeta a la existencia de una sanción legal establecida por ley, de forma anterior al hecho, plenamente vigente, aplicada de manera estricta y, con certeza, tanto respecto de la conducta castigada como de la sanción asociada (*nullum crimen, nulla poena sine lege praevia, scripta, stricta et certa*). La responsabilidad civil, en tanto, y tal como hemos mencionado, resulta de la aplicación de principios generalmente aceptados de reparación de todo daño causado o, incluso, antes de un deber general de no dañar a otro (*alterum non laedere*). Adicionalmente, la responsabilidad penal admite solamente sanción directa al infractor, sea como autor, cómplice o encubridor; respecto de la responsabilidad civil, por su parte, ella puede hacerse valer allí donde se logren probar los presupuestos que permitan establecer que una persona distinta del infractor es responsable.

Sin adentrarnos en los pormenores de las legislaciones nacionales ni en las distinciones doctrinarias dentro de cada cultura jurídica nacional, podemos hacer una somera distinción⁷ en el ámbito civil entre *responsabilidad por culpa o negligencia*, o *responsabilidad subjetiva*, que hace responsable a quien causa daño a otro a condición de actuar con culpa o dolo, y *responsabilidad estricta u objetiva*, que establece la obligación de reparar todo daño que se produzca en el ejercicio de cierta actividad, cualquiera sea la diligencia empleada. Paralelamente, se distingue entre la responsabilidad por el hecho propio, la responsabilidad por el hecho ajeno y la responsabilidad por el hecho de las cosas, cada una con diversos supuestos, dependiendo de cada realidad nacional. En algunos de tales casos, existen reglas legales que permiten la atribución de la responsabilidad de un proveedor de conexión a Internet o bien, de un proveedor de contenidos, pero en muchos otros, ese no es el caso.

Las causales de responsabilidad de los proveedores de Internet estará sujeta a la aplicación de distintas reglas en tanto intermediarios de contenido. Ello porque el carácter ilícito puede provenir de distintos actos comunicativos, realizados por personas o por empresas como emisoras de contenido. En tal sentido, son especialmente reconocidos como delitos realizables a través de Internet:

7. Para una mirada completa de la responsabilidad civil, especialmente la extracontractual, en la cultura jurídica del derecho civil continental, véase Barros, Enrique, *Tratado de Responsabilidad Extracontractual*, Santiago, Editorial Jurídica de Chile, 2006.

- (a) la difusión de instrucciones sobre preparación de bombas, las actividades terroristas, la producción y tráfico de drogas y el activismo político, lo que atenta contra la seguridad nacional y mundial;
- (b) la oferta de servicios sexuales y pornografía relacionada con niños (pedofilia), lo que requiere velar por la protección de menores;
- (c) el envío de mensajes que incitan al odio y la discriminación racial o religiosa, lo que atenta contra la dignidad humana;
- (d) las conductas de hurto y destrucción de datos que realizan los «hackers», que atentan contra la seguridad y confidencialidad de la información;
- (e) los delitos de «pirateo» de *software*, que vulneran la propiedad intelectual;
- (f) la recolección, procesamiento y transmisión no autorizada de datos personales, lo que requiere proteger legalmente la privacidad o intimidad de las personas;
- (g) el envío de mensajes difamatorios o injuriantes, lo que atenta contra la honra y dignidad de las personas; etcétera⁸.

En los últimos años, también parece buscarse a nivel internacional una fórmula legal que permita atribuir responsabilidades por la difusión de información sensible, secreta, confidencial o capaz de comprometer la seguridad de un Estado o de sus tropas desplegadas en el extranjero. No obstante, ello ha sido producto de la contingencia sobre el caso WikiLeaks⁹, situación todavía sujeta a la eventual resolución de órganos jurisdiccionales y a la sanción especial de leyes en la materia.

II.A. Responsabilidad y pornografía infantil

Desde la perspectiva penal, el ámbito en que se ha presentado de forma más clara la aplicación de responsabilidad en Internet ha sido a propósito de la elaboración y difusión de material pornográfico que involucra a menores

8. Véase Jijena, Renato, *Contenidos de Internet: censura o libertad de expresión* [en línea], en: <<http://www.mass.co.cl/acui/leyes-jijena2.html>>. [Nota del editor: consultada el 5/11/11.]

9. Un resumen del caso y de sus implicancias sobre la red, puede ser: UNESCO, *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*, París, 2011, p. 13.

de edad. En tal sentido, reformas en toda la región han buscado reflejar que el uso de la tecnología es una forma más de comisión de los ilícitos relacionados, y así ha sido posible verificar la aplicabilidad de estas reglas en la Argentina¹⁰, Brasil¹¹, Chile¹², Colombia¹³, Costa Rica¹⁴, El Salvador¹⁵, Nicaragua¹⁶, Paraguay¹⁷, Uruguay¹⁸ y Venezuela¹⁹. Lo relevante sobre este punto no es la consagración de dichos delitos, sino, a efectos del presente artículo, las obligaciones nacidas para los prestadores de servicios de Internet (de conexión y de contenidos) al respecto. De este modo, no solamente habrá penas para los responsables directos de la difusión o distribución de material pornográfico que involucre a menores de edad, de forma actual o representada (según cada legislación), sino que en Brasil y en Colombia, existen deberes especiales de retiro de dicho material.

En Brasil, el Estatuto de la Niñez, en su artículo 241-A²⁰, castiga con reclusión de tres a seis años y multa a quien ofrezca, comercialice, transmita,

10. Código Penal, artículo 128.

11. Estatuto da Criança e do Adolescente, artículos 241-A (para transmisión y distribución, entre otros), 241-B (para la adquisición, incluyendo el almacenamiento), y siguientes, introducidos por Ley 11829 de 2008.

12. Código Penal, artículos 374 bis y 374 ter, introducidos por Ley 19927 de 2004.

13. Código Penal, artículos 218 (Pornografía con personas menores de 18 años) y 219-A (Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años) y Ley 679 de 2001 sobre abuso y pornografía de menores en Internet, artículo 7.

14. Código Penal, artículos 173 (producción) y 174 (distribución y difusión).

15. Código Penal, artículo 173.

16. Ley 641, Nuevo Código Penal de 2007, artículo 175.

17. Código Penal, artículo 140.

18. Ley 17815 de 2003, artículos 2º y 3º.

19. Ley Especial contra Delitos Informáticos de 2001, artículo 24.

20. Véase Art. 241-A:

Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§ 1º Nas mesmas penas incorre quem:

I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

§ 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

distribuya, publique o divulgue por cualquier medio, incluyendo medios informáticos o telemáticos, material pornográfico que involucre a menores de edad. La misma pena (parágrafo 1º) se aplica a quien asegure los medios o servicios para almacenar dicho material (inciso I) o a quien asegure por cualquier medio el acceso por red de computadoras a ese material (inciso II). Conforme al parágrafo segundo, estas conductas son punibles cuando el responsable legal de la prestación de servicio, habiendo sido oficialmente notificado, deja de deshabilitar el acceso al contenido ilícito de carácter pornográfico infantil. En otros términos, una vez que existe conocimiento efectivo de la existencia de este material, los responsables de su alojamiento o de su transmisión, aun si no han sido quienes elaboran o ponen a disposición dicho material, están también sujetos a sanciones penales.

Adicionalmente, en el estado de Río de Janeiro, existen obligaciones adicionales para los proveedores de servicios de Internet. Una ley de 2003²¹ obliga a los «proveedores de acceso a Internet» (refiriéndose a los proveedores de alojamiento o *hosting*) establecidos en dicho estado a informar cada tres meses al Consejo Municipal de los Derechos del Niño de las páginas alojadas por ellos y de los responsables de esas²². Tales proveedores tienen, además, obligaciones de promover la denuncia y de denunciar los casos encontrados, sujetos a sanciones de multas que aumentan considerablemente con cada reincidencia.

El caso colombiano es ligeramente distinto. Además de contemplar la difusión de material pornográfico con menores de dieciocho años en el Código Penal de Colombia (artículo 218), la Ley 679 de 2001, modificada por la Ley 1336 de 2009, establece deberes adicionales ante la existencia

21. Ley 3644, del 17 de septiembre de 2003 de Río de Janeiro.

22. Véase artículo 1º:

Os provedores de acesso à internet estabelecidos no Município do Rio de Janeiro, fornecerão a cada três meses, relação completa das páginas home pages que hospedam ao Conselho Municipal dos Direitos da Criança e do Adolescente-CMDCA, bem como a dos respectivos responsáveis por sua elaboração.

Parágrafo único. A elaboração, remessa e análise da relação a que se refere o art 1º desta Lei, têm por objetivos precípuos:

- I - identificar as home pages que estejam veiculando materiais sobre pedofilia;
- II - coibir a prática da pedofilia na internet;
- III - facilitar e viabilizar a punição dos responsáveis por sua elaboração.

de material pornográfico infantil²³. En virtud del artículo 7° de esta ley, tanto los proveedores de servicio, como los proveedores y responsables de contenidos y los mismos usuarios de redes de información tienen la prohibición de almacenar material gráfico, audiovisual o, incluso textual que impliquen actividad sexual con menores, además de la prohibición de alojar material pornográfico cuando «existan indicios» de que las personas representadas son menores. Pero establece una prohibición adicional que parece ir mucho más allá de los deberes de no producir, almacenar o difundir pornografía infantil: la ley prohíbe (artículo 7° N° 3) alojar «vínculos o links sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad». La consecuencia de esto es que un motor de búsqueda podría verse sujeto a sanciones por el solo hecho de presentar entre sus resultados de búsqueda un sitio donde se provea tal clase de material y obliga a poner un celo casi excesivo al momento de practicar un enlace. Como ejemplo, podemos imaginar el caso de enlazar hacia un sitio con videos, desconociendo la totalidad del material audiovisual allí alojado: el enlazador asume de inmediato el enorme riesgo de ser responsable por vincular un sitio que ofrece pornografía infantil.

El artículo 8° del mismo cuerpo legal²⁴, en tanto, establece deberes generales de denuncia de actos criminales contra menores, combate de la difusión de pornografía infantil, abstención de uso de redes para divulgar

23. Véase artículo 7°:

Prohibiciones. Los proveedores o servidores, administradores y usuarios de redes globales de información no podrán:

1. Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.
2. Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.
3. Alojar en su propio sitio vínculos o links, sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.

24. Véase artículo 8°:

Deberes. Sin perjuicio de la obligación de denuncia consagrada en la ley para todos los residentes en Colombia, los proveedores, administradores y usuarios de redes globales de información deberán:

1. Denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de material pornográfico asociado a menores.
2. Combatir con todos los medios técnicos a su alcance la difusión de material pornográfico con menores de edad.

material ilegal con menores y, de forma especial, pone como deber el establecimiento de «mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de material ilegal, ofensivo o indeseable en relación con menores de edad».

La forma de hacer valer estos deberes es a través de sanciones administrativas, según lo establecido por el artículo 10 de la misma ley²⁵. Conforme a ese, es el Ministerio de Comunicaciones el que sancionará a los responsables mediante multas de hasta cien salarios mínimos legales y cancelación o suspensión de la página electrónica. Asimismo, el Ministerio puede requerir información a los proveedores de servicios de Internet sobre los mecanismos o filtros de control para bloquear páginas con pornografía infantil y puede ordenarles la incorporación de cláusulas obligatorias en

3. Abstenerse de usar las redes globales de información para divulgación de material ilegal con menores de edad.

4. Establecer mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de material ilegal, ofensivo o indeseable en relación con menores de edad.

25. Véanse artículo 10:

Sanciones administrativas. El Ministerio de Comunicaciones tomará medidas a partir de las denuncias formuladas, y sancionará a los proveedores o servidores, administradores y usuarios responsables que operen desde territorio colombiano, sucesivamente de la siguiente manera:

1. Multas hasta de 100 salarios mínimos legales vigentes.

2. Cancelación o suspensión de la correspondiente página electrónica.

Para la imposición de estas sanciones se aplicará el procedimiento establecido en el Código Contencioso Administrativo con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.

Y Parágrafo:

El Ministerio de Comunicaciones tendrá competencia para exigir, en el plazo que este determine, toda la información que considere necesaria a los proveedores de servicios de internet, relacionada con la aplicación de la Ley 679 y demás que la adicione o modifiquen. En particular podrá:

1. Requerir a los proveedores de servicios de internet a fin de que informen en el plazo y forma que se les indique, qué mecanismos o filtros de control están utilizando para el bloqueo de páginas con contenido de pornografía con menores de edad en Internet.

2. Ordenar a los proveedores de servicios de internet incorporar cláusulas obligatorias en los contratos de portales de internet relativas a la prohibición y bloqueo consiguiente de páginas con contenido de pornografía con menores de edad.

Los proveedores de servicios de internet otorgarán acceso a sus redes a las autoridades judiciales y de policía cuando se adelante el seguimiento a un número ip desde el cual se produzcan violaciones a la presente ley.

La violación de estas disposiciones acarreará la aplicación de las sanciones administrativas de que trata el artículo 10 de la Ley 679 de 2001, con los criterios y formalidades allí previstas.

contratos de portales de Internet sobre prohibición y bloqueo de páginas con pornografía infantil. La ley los obliga, además, a otorgar acceso para el seguimiento a un número de IP por parte de autoridades judiciales y de policía cuando se viole esta ley. La pertinencia de tales medidas, sin mediar sentencias ni procesos judiciales propiamente tales, implicará necesariamente obviar consideraciones sobre proporcionalidad, privacidad y debido proceso en virtud de la persecución de la pornografía infantil.

I.B. Responsabilidad y atentados contra el honor, la honra y la vida privada

Resulta particularmente digno de estudio el hecho de que las legislaciones agraven las sanciones sobre la comisión de delitos como injurias, calumnias, libelos u otras formas de difamación, ofensa o de atribución de delitos, cuando dicha comunicación es realizada por escrito, con publicidad o a través de medios de prensa o comunicación masiva. La práctica jurisprudencial en los distintos países ha seguido la persecución de estos delitos, allí donde han sido objeto de denuncia o querrela, conforme a las reglas generales de atribución directa y personal de la responsabilidad penal, sin distinguir de manera especial en el caso de realizarse por medio de Internet, sino en la medida que las herramientas tecnológicas permiten, incluso, la persecución de quien realice dicha difamación de forma anónima.

Desde el punto de vista del examen legal, resulta interesante estudiar el problema de atribución de responsabilidad penal que se produce a propósito de estos mismos delitos cuando la ley establece sanciones ya no sobre quien profiere las ofensas o calumnias, sino sobre quien las difunde. Hablamos, por supuesto, de aquellas circunstancias en las que es el intermediario el objeto de sanciones penales por facilitar o difundir tales contenidos. Así ocurre, precisamente, en Colombia²⁶ y de forma más limitada, en la Argentina²⁷,

26. Código Penal de Colombia, véase el artículo 222: «Injurias y calumnias indirectas. A las penas previstas en los artículos anteriores quedará sometido quien publicare, reprodujere, repitiere injuria o calumnia imputada por otro, o quien haga la imputación de modo impersonal o con las expresiones se dice, se asegura u otra semejante».

27. Código Penal de Argentina, véase el artículo 113: «El que publicare o reprodujere, por cualquier medio, injurias o calumnias inferidas por otro, será reprimido como autor de las injurias o calumnias de que se trate, siempre que su contenido no fuera atribuido en forma sustancialmente fiel a la fuente pertinente. En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas».

donde la difusión o publicación de injurias o calumnias proferidas por otros acarrearán, también, responsabilidad para quien realiza ese acto de divulgación. No obstante, en estos casos la aplicación de principios de responsabilidad penal, en particular la necesidad de existencia de *dolo* o intención para la comisión de los ilícitos, tiende a dejar sin efecto la aplicabilidad de las sanciones aparejadas cuando se trata de proveedores de servicios que no tienen influencia sobre el contenido de lo que difunden y son, por tanto, incapaces de mostrar una intención de ofensa o descrédito.

Ello no ha obstado, sin embargo, a que se haya perseguido la responsabilidad civil y penal, tanto sobre los proveedores de servicio de Internet como respecto de los proveedores de contenidos, ante situaciones percibidas como lesivas del honor.

Uno de los supuestos más conocidos entre lo que esto ha ocurrido es en la seguidilla de acciones llevadas adelante en la Argentina por distintos personajes de relevancia pública a fin de recibir indemnización por daños y perjuicios de parte de los buscadores y que, especialmente, han buscado la dictación de medidas cautelares que ordenen suspender, bloquear o dejar sin efecto cualquier vinculación efectuada por un buscador (usualmente Google y Yahoo!) entre el nombre o la imagen del personaje y las páginas de contenido sexual o difamatorio²⁸. Si bien ha sido poco lo que han avanzado dichas causas judiciales hasta una sentencia de término²⁹, sí han sido concedidas dichas medidas de manera cautelar. Como ejemplo de ello, la búsqueda de «Yesica Toscanini» en la versión para la Argentina en el buscador Yahoo!³⁰ entrega, junto con el número de resultados, una simple mención de por qué ninguno de esos resultados es enlazado: debido a una orden judicial.

No obstante la proliferación de dichos litigios en la Argentina y el éxito de muchos de ellos en las medidas cautelares mencionadas, uno de los casos más recientes (y todavía en curso) demuestra las notables

28. Para un relato más acabado del estado de la discusión en la Argentina sobre la responsabilidad de buscadores, véase Tomeo, Fernando y Roberto Abieri, «Responsabilidad de los buscadores de Internet», en *Revista de Responsabilidad Civil y Seguros*, año 11, 12 (2009), pp. 66-70.

29. Hasta mediados de 2010, se contaban apenas dos sentencias entre más de ciento treinta casos, véase Sreeharsha, Vinod, «Google and Yahoo Win Appeal in Argentine Case», en *The New York Times*, 20 de agosto de 2010, p. B4.

30. Acceso disponible en: <<http://ar.yahoo.com>>.

diferencias de opinión entre distintas instancias de la judicatura y ayudan a sentar criterios futuros para la eventual determinación de responsabilidad de proveedores de servicios y, muy particularmente, de los servicios de búsqueda y enlace de contenidos. La cantante Virginia da Cunha demandó en el año 2006 por este mismo expediente a Google Inc. y a Yahoo! Argentina y exigió indemnización por los daños y perjuicios de su imagen, producto del enlazamiento de su nombre e imagen a ciertos sitios, al realizar una búsqueda de su nombre en dichos servicios, con lo que se entendía que se producía «un avasallamiento a sus derechos personalísimos al honor, al nombre, a la imagen y a la intimidad al haber sido vinculada a páginas de Internet de contenido sexual, erótico y pornográfico y, asimismo, por la utilización comercial y no autorizada de su imagen»³¹. La sentencia de primera instancia falló a favor de la artista, ordenando a las demandadas el pago de 100 000 pesos argentinos más intereses como compensación por el daño moral. En cuanto a la responsabilidad, hace aplicación de las reglas generales sobre responsabilidad civil del Código Civil de la Argentina a falta de regla especial en la materia. Señala en sus considerandos sobre responsabilidad que, efectivamente, los buscadores tienen control sobre el sistema de búsquedas, además de tratarse de páginas web cuyo contenido desplegado es de su responsabilidad. Es más, hallando la importancia de los buscadores, entiende la sentencia de que su responsabilidad sobre los resultados desplegados se maximiza en vez de reducirse, pues el crecimiento de Internet no puede hacerse a expensas de derechos personalísimos de los individuos³². Condenó, finalmente, a la suma ya indicada, en atención a la lesión de derechos personalísimos y como indemnización por el daño moral sufrido. En agosto de 2010, sin embargo, la Sala D de la Cámara Nacional de Apelaciones en lo Civil, tribunal de segunda instancia del sistema argentino de justicia civil, revocó la sentencia anterior, con dos votos a favor y uno en contra³³. El primer voto favorable a la revocación, de la doctora Patricia Barbieri, citó, entre diversos textos doctrinarios y legales, aquellas normas de legislación interna que consagran a Internet como una vía de ejercicio

31. *Da Cunha Virginia c/ Yahoo de Argentina S.R.L. y otro*, Juzgado Nacional de Primera Instancia en lo Civil N° 75, Buenos Aires, 29 de julio de 2009.

32. *Íd.*

33. Cámara Nacional de Apelaciones en lo Civil, sala D, Expte. N° 99.620/2006, *D. C. V. c/ Yahoo de Argentina SRL y otros/ Daños y Perjuicios*, Recurso N° 541482, Juzgado N° 75.

del derecho fundamental y constitucionalmente reconocido a la libertad de expresión³⁴. Además, hace presente una consideración que se extiende considerablemente en la discusión sobre regímenes de responsabilidad: si no está establecido un sistema de responsabilidad de carácter estricto u objetivo, determinado por el resultado, entonces deben probarse los supuestos generales de la responsabilidad civil extracontractual, entre ellos, la culpa o negligencia³⁵. En tal sentido, solamente con posterioridad a un reclamo, sería procedente acusar de negligencia en el actuar a los buscadores (en caso de no responder satisfactoriamente a dicho reclamo), y no esperando una forma de censura previa de contenidos no controlados por ellos³⁶. El segundo voto de mayoría, de la doctora Ana María R. Brilla de Serrat, además de hacer

34. Opinión de la doctora Barbieri:

Sí, se encuentra vigente el decreto 1279/97 que declara que el servicio de Internet se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión, correspondiéndole las mismas consideraciones que a los demás medios de comunicación social. Esto significa que resultan aplicables a los servicios de Internet las disposiciones de los arts. 14, 32 y 42 de la Constitución Nacional, que establecen la libertad de expresión y prohíben la censura previa. A su vez, la ley 26 032/05 establece que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión.

35. Opinión de la doctora Barbieri:

Y desde este punto de vista, entonces, no basta que la información o el contenido existente en la web y encontrado a través de los buscadores sea erróneo y aun lesivo para el honor, la imagen o la intimidad de una persona para que esta tenga derecho a que le sea reparado el perjuicio causado. Comprobado el exceso o la ilegalidad, quien pretenda el resarcimiento deberá demostrar la culpa o negligencia en que incurrió el buscador conforme al régimen general de responsabilidad por el hecho propio que contiene la fórmula del artículo 1109 citado, y que sigue el principio *alterum non laedere*. Es decir, no basta la sola comprobación del daño para imponer el deber de resarcir, sino que es necesario probar el factor de imputabilidad subjetivo, sea la culpa o el dolo.

36. Opinión de la doctora Barbieri:

Pero entiendo que aun admitiendo la responsabilidad civil, la misma solamente puede hacerse efectiva contra las demandadas en la medida en que, frente a una situación ilícita, y advertidas a través de los mecanismos pertinentes, no realicen la conducta atinente y necesaria para obtener la cesación de las actividades nocivas, pues, recién en ese momento, se configuraría una falta propia susceptible de ser apreciada en los términos de los artículos 512, 902, 1109 y cc. del Código de fondo. Resumiendo, entonces, con anterioridad a cualquier reclamo del afectado solicitando el bloqueo del contenido que considera agravante y disponible en Internet a través de los buscadores demandados, no puede a los mismos serle atribuida o adjudicada culpa alguna por los contenidos cuestionados.

suyos los argumentos del primer voto, plantea el funcionamiento mismo de los motores de búsqueda como meros agregadores de información que no atribuyen ningún carácter especial ni lesivo a la demandada³⁷. El voto disidente, si bien se niega a aceptar la censura previa como método para evitar el daño causado, sí señala que bien podrían las demandadas poner filtros y que es inexcusable que años después de dictadas las medidas cautelares los enlaces lesivos sigan presentándose como resultados de búsqueda³⁸. Actualmente, el caso espera ser resuelto por la Corte Suprema de la República Argentina.

Varios años antes, en un fallo célebre por tratar de abordar estos temas a pesar de la falta de reglas legales específicas sobre la materia, los tribunales

37. Opinión de la doctora Brilla de Serrat:

No se trata de transmisiones lesivas de los derechos de la personalidad, incluidas imágenes, a través de operadores de medios de comunicación escritos, orales o televisivos, sino, como bien se afirma, de actividad auxiliar para facilitar el acceso de los usuarios del servicio a los sitios presentes en la web. Tampoco se trata del suministro de datos personales que allí obren de modo que se pudiera afectar el derecho a la vida reservada que tiene todo ser humano si así fuera su deseo, dado que no nos hallamos ante esos extremos, sin perjuicio de reconocerse la natural desazón de la actora –cantante de un grupo musical en su momento y luego devenida modelo y actriz, según se afirma-, al encontrarse vinculada del modo señalado con páginas relacionadas con actividad sexual, prostitución y pornografía, pero, en modo alguno sindicada o descripta, como incluida personalmente en ese tipo de prácticas.

38. Opinión del doctor Diego C. Sánchez:

Porque resulta de la experticia admitida y hago lo propio (arts. 477 y concs. del Cód. Proc.), también admitido por mis colegas, que Google Inc. y Yahoo!, tuvieron conocimiento de que a través de sus motores de búsqueda se podía acceder a determinados contenidos de sitios de terceros indexados en sus búsquedas que utilizan la imagen y/o vinculan el nombre de la actora con textos eróticos, pornográficos, sexuales u otros que se consideran ilícitos, que las demandadas pueden voluntariamente establecer filtros para impedir la indexación de sitios o imágenes que vinculen determinadas palabras con tales contenidos. Admitido todo ello, insisto, resulta inadmisibles que, según constancias del incidente de medidas cautelares (exp. N 63314/06, que tengo a la vista), se las haya decretado con fecha 23 de agosto de 2006 (fundado entre otras constancias, en la de fojas 64, que es el acta notarial del esc. Arias del 27-06-06) y notificado de inmediato a la demandada; se presentó Google el 7 de septiembre siguiente (fojas 147/9) y a principios de este año 2010 (fojas 2139/40, ahora de este expediente principal) ¡más de tres años después de decretada judicialmente la medida cautelar! mantiene vínculos y enlaces que permiten identificar el nombre de la demandante con sitios de contenido sexual y pornográfico. [...] La conducta en que incurrieron las demandadas al no cumplir oportunamente las medidas cautelares ordenadas y firmes, procediendo a bloquear o impedir la existencia de contenidos ilegales y perjudiciales de los derechos personalísimos de la actora es relevante e inexcusable.

superiores de Chile intentaron sentar doctrina sobre la difusión de avisos difamatorios en Internet. El fallo ha sido discutido por la literatura en diversas ocasiones³⁹, precisamente por sus aspectos innovadores y por ser una de las pocas oportunidades en que las Cortes de ese país han tenido la oportunidad de ver materias relacionadas con estos asuntos. En *Fuentes c/ Entel*⁴⁰, el recurrente actuaba contra la empresa de Internet Entel, a propósito de un aviso de oferta de servicios sexuales que apareció a mediados de 1999 en el sitio de avisos económicos dispuesto por la misma empresa de servicios de Internet. En tal aviso, la oferente no era nada menos que su propia hija, entonces de diecisiete años de edad, quien recibiría con posterioridad innumerables llamadas telefónicas «obscenas, insultantes, groseras y pervertidas» que forzaron la suspensión del servicio por parte de la familia. Claramente, a juicio del recurrente, existía afectación del derecho constitucional de la menor a su honra. La defensa de la empresa era su falta de responsabilidad, pues el aviso provenía de un usuario en la ciudad de Concepción, en uso de la plataforma gratuita facilitada por Entel, pero cuyo contenido era total responsabilidad de quien exponía el aviso.

La sentencia del caso *Fuentes c/ Entel* fue de rechazo a la pretensión del actor, por haberse presentado de forma extemporánea la acción constitucional de protección, declarándose dicha decisión en la sentencia no sin antes hacer alusión a diversas materias involucradas. Entre ellas, la sentencia reconoce la falta de legislación especial en la materia e identifica tres clases de prestadores de servicio de Internet: el proveedor de acceso, el proveedor de almacenamiento y el proveedor de contenido. Señala que, para que se cometa el ilícito, todos ellos deben participar; califica a Entel como proveedor de acceso y de almacenamiento y a la empresa externa, GrupoWeb, como proveedora de contenido. Citando la opinión

39. Entre otros, véanse Lipszyc, Delia, «Responsabilidad de los proveedores de servicios en línea por las infracciones del derecho de autor y derechos conexos en el entorno digital: análisis de la jurisprudencia internacional», en el XI Curso Académico Regional OMPI/SGAE sobre derecho de autor y derechos conexos para países de América Latina, OMPI, 2005; Piñeiro, Lorena, «Responsabilidad de los ISPs por violación a la propiedad intelectual: Estados Unidos, Europa y Chile», en *Revista Chilena de Derecho Informático*, 5 (2004) y Carrasco, Humberto, «Algunos aspectos de la responsabilidad de los proveedores de servicios y contenidos de Internet», en *AR: Revista de Derecho Informático*, 26, septiembre de 2000.

40. Corte de Apelaciones de Concepción, fallo sobre Recurso de protección, *Orlando Fuentes Siade c/ Empresa Nacional de Telecomunicaciones Entel S.A.*, rol 243-19-99, sentencia de 6 de diciembre de 1999.

del profesor Santiago Schuster⁴¹, indica la sentencia que la responsabilidad recae directamente en el usuario proveedor de contenido en la red, cuando tal contenido es ilícito o nocivo, y que tal responsabilidad podría, incluso, extenderse a aquellos contenidos que son incorporados directamente por los destinatarios finales del servicio Internet, cuando el proveedor de sitio ha creado un fondo de información con los aportes de los clientes de sus diferentes foros puestos a disposición de cualquier abonado en la red y no ha tomado las providencias mínimas necesarias para la adecuada identificación de los usuarios que publican tales mensajes, a fin de asegurar las eventuales responsabilidades por el posible menoscabo a terceros. Siguiendo al autor citado, la Corte establece un deber de control sobre Entel, debiendo tomar las medidas susceptibles de hacer cesar el perjuicio que hubiera causado a un tercero, puesto que sería «evidente» la responsabilidad del proveedor de servicios de alojamiento, cuando este permite que mediante los servicios que presta se cometan hechos ilícitos, al conocerlo efectivamente o pudiendo hacerlo puesto que por medio de este comportamiento (culposo o negligente) se convierte en cooperador y responsable de la ilicitud. Por cierto, ello no responde a la inquietud por los costos de dicho nivel de control o si la empresa debiera llevarlo a cabo en su papel de proveedora de acceso o como proveedora de almacenamiento, atendiendo que una empresa distinta era proveedora de contenido.

El caso tuvo todavía una secuela, sin que con ello fuera superada la ambigüedad de la primera sentencia. Con posterioridad al rechazo del recurso de protección, la afectada por la situación de deshonra trató de hacer valer sus intereses, ya no buscando la protección de sus derechos fundamentales mediante una acción constitucional directa, sino haciendo valer la responsabilidad civil extracontractual mediante una demanda civil ordinaria, otra vez contra Entel, la proveedora de acceso a Internet, pero de forma conjunta contra la persona desde cuyo computadora fue subido el aviso económico que la promovía como trabajadora sexual. La demanda se dirigió contra la señora Yáñez Vargas por haber entregado su clave de acceso a Internet a otra persona, sin considerar el uso malicioso o negligente que esta realizó al publicar el aviso, causando daño a los demandantes; y contra Entel, por no haber cumplido con su deber de cuidar de que a través de su

41. Schuster, Santiago, «Responsabilidad legal en las redes rigitales», en la Conferencia en la Facultad de Derecho de la Universidad de Chile, Santiago, 1999.

red no se atentara contra el honor y la integridad psíquica de la afectada, encontrándose en condiciones de borrar los avisos, pero sin hacerlo. En primera instancia, la demanda fue desechada, una vez más, negando la razón a la afectada.

La Corte de Apelaciones de Concepción, fallando el recurso de apelación⁴², otra vez en contra de la demandante y afectada, tuvo una nueva oportunidad de revisar temas examinados varios años antes. En la sentencia de apelación de *Fuentes c/ Entel II*, la Corte de Concepción determinó una vez más que las normas por aplicar serían las de responsabilidad extracontractual y sus factores de imputación subjetiva de daños, el dolo y la culpa. Asimismo, estableció esta vez que la persona natural demandada no tenía culpa propia, por no haber falta de cuidado en permitir a otras personas usar la clave de acceso a Internet de su computadora («No se contratan tantas claves como miembros de la familia existen», en opinión de la Corte), mientras que quien subió el contenido ilícito era una hija de ella, mayor de edad y responsable de sus propios actos.

En cuanto al proveedor de acceso a Internet, esta vez la Corte señala de forma expresa que tal proveedor «no se encuentra obligado a controlar el ingreso de contenido a la red; es más, debe respetar el principio de la libertad de la información que circula en la red». Agrega que no ha faltado a deberes de cuidado, pues «no estaba en conocimiento» de la realización del ilícito, además de haber eliminado el aviso, prudentemente, a las pocas horas de haber recibido el respectivo reclamo. De este punto, si bien la Corte sigue criterios tradicionales sobre responsabilidad para resolver la cuestión, resulta relevante, precisamente, aquel punto señalado esta vez por la Corte, en parte incluso contradictorio con la resolución anterior: el proveedor de acceso a Internet no se encuentra obligado a controlar el ingreso de contenidos a la red, pero sí se encuentra obligado a respetar el principio de libertad de la información que circula en Internet. La Corte no define tal principio, pero es capaz de defenderlo aun de la acción por parte de los proveedores de Internet.

De las soluciones jurisprudenciales antes descritas, no resulta claro que exista una única fórmula de atribución de responsabilidad. Por cierto, pareciera ser aceptable que un proveedor de acceso y conexión, que no lo

42. Corte de Apelaciones de Concepción, sentencia sobre recurso de apelación, causa *Paulina Fuentes Almendra y otro c/ ENTEL S.A.*; *Carmen Gloria Yáñez Vargas*, rol 1223-2003, sentencia de 21 de diciembre de 2007.

es de almacenamiento ni contenido, esté liberado de responsabilidad por los contenidos o actos comunicativos realizados por los usuarios finales (a pesar de la opinión de la Corte de Concepción en el primer caso *Fuentes c/ Entel*). Pero ello no resulta igualmente claro respecto de los contenidos o actos comunicativos cuando ellos son alojados y puestos a disposición del resto de los usuarios de la red aprovechando la infraestructura física y técnica dispuesta por proveedores de alojamiento y contenido. El seguimiento de estándares de conducta y diligencia, en tal ámbito, requiere de mayor depuración doctrinaria y dogmática, si es que no del establecimiento de nuevas condiciones legales. No necesariamente con el objetivo de fijar responsabilidad civil sobre los prestadores de servicios de Internet, en el entendido que son, en teoría, económicamente más fuertes que otros usuarios y posibles demandados⁴³; sino con el fin de dilucidar su real nivel de participación (y, por tanto, de responsabilidad) respecto de actos que pudieran ser ilícitos, afectando derechos ajenos.

II.C. Responsabilidad de proveedores de Internet por infracciones de derechos de propiedad intelectual

Si bien hemos visto y examinado casos de judicialización de conflictos entre proveedores de contenidos (y buscadores de contenido) en la relación entre la prestación de servicios de Internet y los atentados contra la honra, no es ese el ámbito que más discusión ha traído a propósito de la responsabilidad de los prestadores de servicios de Internet. O sea, no es a propósito de la tensión entre libertad de expresión e imagen y honra⁴⁴, sino de los derechos

43. Xalabarder, Raquel, «La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios», en *Revista de Internet, Derecho y Política*, 2 (2006) [en línea], en: <<http://www.uoc.edu/idp/2/dt/esp/xalabarder.pdf>>. [Nota del editor: consultada el 5/11/11.]

La tentación de designar a los prestadores de servicios en Internet (en adelante, ISP) como responsables por las infracciones que cometan los usuarios de sus servicios en Internet es fácil de explicar. Por una parte, toda infracción (de cualquier tipo, ya sea civil, penal o administrativa) que tiene lugar en Internet, se materializa a través de sus servicios (piénsese en los servicios de acceso, de almacenaje, motores de búsqueda, y routers o direccionadores); Internet no existiría sin los isp. Por otra parte, los isp son de fácil localización y tienen –normalmente– mayor solvencia para reparar el daño cometido, que el infractor.

44. Bertoni, Eduardo, *Libertad de Expresión en el Estado de Derecho*. Buenos Aires, del Puerto, 2008.

patrimoniales de autor vulnerados mediante el intercambio en línea⁴⁵, ya que en los últimos años ha surgido con más fuerza la idea de regular la responsabilidad de los prestadores de servicios de Internet. Dejando de lado, de este modo, otras temáticas vinculadas con los posibles delitos realizables en la red, como los mencionados al principio de este informe.

II.C.I. La influencia extranjera: tratados internacionales en discusión y legislaciones extranjeras

Como se ha indicado, el asunto relativo a la responsabilidad de los agentes intermediarios de la comunicación por los hechos que realizan terceros ha sido blanco de amplias discusiones a nivel doctrinario, en algunos casos, legal, y en nuestra región, especialmente jurisprudencial. No obstante la existencia de algunos casos con cierta relevancia pública (sea desde el punto de vista de sus actores, sea desde el punto de vista de los efectos que eventualmente podrían tener para la regulación futura), es a partir de instrumentos internacionales que muchas veces el sistema general de derechos de autor ha intentado levantar la agenda que pretende reformar las normativas locales de derechos de autor.

Pero esta no es una estrategia aislada. Si se analiza en perspectiva, resulta más o menos obvio el viraje, el cambio de énfasis, si se quiere, que ha sufrido la legislación de derechos de autor en el concierto internacional. De un tratamiento en tratados particulares referentes a derechos de autor y conexos y luego de la creciente importancia económica de las industrias de la informática, durante las últimas décadas del siglo recién pasado, se fue desarrollando una importante tendencia a nivel internacional respecto del desarrollo de los asuntos vinculados a derechos de autor y, en general, de la emergencia de las nuevas tecnologías. Esta tendencia surge y se explica a partir de un importante cambio de paradigma en la regulación internacional, donde a partir de los años setenta y ochenta comienza a cambiar la orientación de la regulación internacional en materia de derechos autorales hacia la agenda de comercio liderada por la OMC. Ejemplos de lo anterior son la celebración de los Aspectos de los Derechos de Propiedad Intelectual relacionados con el comercio (ADPIC), en 1994, y los denominados Tratados Internet de OMPI, en 1996.

45. Véase *supra* nota 43.

En parte producto de las críticas recibidas tanto de manera interna en OMPI por países en vías de desarrollo, en parte como resultado de la importancia comercial de las presuntas pérdidas como consecuencia de la denominada piratería es que durante la primera mitad de los años noventa se produce otro cambio de dirección –y que, como se verá, va a ser, en cierto modo, relevante para el análisis del tema central de este artículo–, las medidas para hacer frente a la piratería y la emergencia de nuevas formas de protección de derechos de autor, particularmente en el contexto del entorno en línea, dieron paso a que las temáticas comenzaran a ser parte de instrumentos de carácter bilateral, siempre dentro del marco de la agenda de comercio. De esta manera, y con particular énfasis en Latinoamérica, los denominados Tratados de Libre Comercio comenzaron a ser una nueva forma mediante la cual la regulación internacional, liderada en este caso particular por los Estados Unidos, pretende influir, esta vez favorecida por las eventuales sanciones comerciales ante su incumplimiento, en la normativa local. De esta manera, es posible verificar la existencia de este tipo de tratados con Chile (2003), el Perú (2007) y los países de Centroamérica (2003-2006). Hoy existen etapas avanzadas de negociación con Panamá y Colombia.

Dichos tratados de libre comercio cuentan con capítulos completos referidos al *enforcement* (observancia, incluso, forzada) de los derechos de autor y conexos, estableciendo no solo procedimientos de policía y judiciales, sino, además, aspectos referidos a medidas tecnológicas de protección (MTP) y limitación de responsabilidad de prestadores de servicios de Internet, como se verá más adelante, utilizando como criterio normativo lo establecido a nivel federal en la Digital Millennium Copyright Act (DMCA) de 1998.

La polémica DMCA de 1998 es la ley federal que implementa y hace operativos los tratados Internet de la OMPI. Dentro del contenido al que las normas de dicho texto normativo hacen referencia, se encuentran la penalización de diversos actos relativos a la elusión de medidas de protección tecnológica; el aumento de las penas frente a las infracciones a derechos de autor en el entorno en línea y el establecimiento de un modelo denominado de *Safe Harbor* o de puerto seguro. Por medio de este modelo, se establece una exención o limitación de responsabilidad en caso de que el prestador de servicios cumpla de buena fe con ciertos estándares establecidos por la ley⁴⁶. Así, por medio de él, se establecen actividades que se entenderán

46. Véase [en línea]: <http://www.law.cornell.edu/uscode/17/usc_sec_17_00000512--000-.html>. [Nota del editor: consultada el 5/11/11.]

como parte de este puerto seguro: cuando los ISP actúan como conductores de las comunicaciones, los actos de captura de información, el alojamiento –*hosting*– de contenido creado por el usuario y la provisión de herramientas de localización de información en la red vinculada a los buscadores de contenido. Así, y desde el punto de vista de la puesta en conocimiento del prestador de servicios, en el modelo de la DMCA solo hace falta una notificación privada que envíe el titular eventualmente afectado al prestador para que se active el mecanismo legal que supone el cumplimiento de las condiciones de puerto seguro.

La existencia de estos tratados de libre comercio no significa que los esfuerzos a nivel regional o suprarregional por parte de países con economías consolidadas se hayan estancado. Muy por el contrario. Existen al menos dos experiencias que hemos creído importante destacar por el especial énfasis que hacen respecto de las responsabilidades de los intermediarios en cuanto a eventuales infracciones hechas por terceros. Por cierto que estos instrumentos en caso alguno están solo referidos a esos asuntos. Como se verá, en el caso del tratado TPP, los aspectos vinculados a *enforcement* y responsabilidad civil son solo partes de proyectos regulatorios de más largo alcance para establecer una zona de libre comercio entre países del Pacífico.

El Acuerdo de Asociación TransPacífico de Libre Comercio (conocido como TPP, por las siglas en inglés, *Trans-Pacific Partnership Agreement*) tiene su origen en uno suscrito por Brunei, Chile, Nueva Zelanda y Singapur en el año 2005, en el que estableció un área de libre comercio entre estos países y el que implica una alta exención arancelaria con el fin de facilitar procesos comerciales en la región Asia-Pacífico. Desde 2010, y particularmente por la intención de los Estados Unidos, Australia, el Perú, Vietnam y Malasia de incorporarse formalmente a este acuerdo, se han llevado adelante negociaciones tendientes a ampliar los alcances del acuerdo inicial, ampliaciones que, en parte importante, se refieren a asuntos ligados con la circulación internacional de bienes y productos intelectuales y con las medidas judiciales y administrativas para afrontar los intercambios informales. Por otro lado, y de acuerdo con lo que hemos expuesto, TPP es parte de una nueva estrategia a nivel internacional, que supone sacar la discusión respecto de las medidas judiciales por tomar en sede nacional desde el aparato internacional vinculado con las Naciones Unidas, como lo es OMPI, hasta la discusión plurilateral. Esto también ha sido objeto de críticas en cuanto se verifican serios problemas a los efectos de poder establecer condiciones mejoradas y que no incluyan solo criterios que apunten a la sobreprotección de los derechos de autor, sino que también incluyan medidas

internacionales que apunten al acceso o que favorezcan de alguna manera los derechos de los ciudadanos, particularmente en el entorno en línea.

De alguna manera, y desde el punto de vista de sus contenidos, el TPP se emparenta con el largamente negociado y polémico Acuerdo Comercial Antifalsificación (ACTA)⁴⁷ en cuanto a que responde a una misma práctica del Gobierno estadounidense de utilizar convenios internacionales de carácter multilateral a los efectos de imponer reglas cada vez más protectoras de los derechos de los titulares de derechos de autor en un sentido amplio, incluyendo medidas relativas a patentes, indicaciones geográficas, entre otras. Además se relaciona con el producto del hermetismo en las negociaciones multilaterales a las que el texto ha estado sometido, no obstante la realización de más de cinco jornadas de negociación.

Pero respecto de la responsabilidad de intermediarios, en particular de prestadores de servicios de Internet, el TPP va un poco más allá que las últimas versiones del ACTA^{48 y 49}. En efecto, el artículo 16 y final del último borrador que se ha filtrado dan cuenta de un especial tratamiento a las medidas relativas al *enforcement* en el entorno digital. Como veremos, las normas del TPP van más allá que ADPIC y establece criterios de aplicación internacional muchísimo más restrictivos que las propias normas de DMCA. Tanto es así que grupos de expertos, profesores y activistas han llevado adelante importantes campañas para transparentar el proceso de negociación y, eventualmente, poder intervenir en él con el fin de intentar equilibrar los

47. El tratado fue firmado en una ceremonia en Tokio, Japón, el día 1º de octubre de 2011. Firmaron el tratado Australia, Canadá, Corea del Sur, los Estados Unidos, Japón, Marruecos, Nueva Zelanda y Singapur. Asistieron sin firmar la Unión Europea, México y Suiza.

48. La versión final de ACTA, de hecho, desestima la propuesta estadounidense relativa a responsabilidad de prestadores de servicio y solo indica amplias referencias relativas al punto:

Artículo 23.5. Cada Parte adoptará las medidas que sean necesarias, conforme a sus principios jurídicos, para establecer la responsabilidad, que podrá ser penal, de las personas jurídicas por los delitos referidos en este Artículo, para los cuales una Parte provee procedimientos y sanciones penales. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas físicas que hayan cometido los delitos.

49. Como se ha indicado, el texto de las negociaciones se mantiene en reserva, pero el trabajo de una serie de organizaciones de la sociedad civil ha permitido poder acceder a versiones no oficiales. Véase [en línea]: <<http://keionline.org/node/1091>>. [Nota del editor: consultada el 5/11/11.]

criterios regulatorios, no solo pensando en la criminalización y *enforcement*, sino, también, tomando en cuenta los derechos e intereses de los ciudadanos.

El artículo 16 se titula «Special measures relating to enforcement in the digital environment» y tiene amplia aplicación para asuntos vinculados a las formas de hacer efectivas las normas de aplicación directa tanto del tratado, como también de las normas legales nacionales relativas no solo a derechos de autor, sino, también, a los conexos. El artículo 16.3 comienza:

3. Con el propósito de proveer procedimientos de observancia que permitan acción eficaz en contra de cualquier acción infractora de derechos de autor cubierta por este Capítulo, con inclusión de recursos ágiles para prevenir infracciones y recursos criminales y civiles que constituyan un medio de disuasión de nuevas infracciones, cada Parte deberá proveer, de manera consistente con la estructura fijada en este Artículo:

(a) incentivos legales para que los proveedores de servicio cooperen con los titulares de derechos de autor en disuadir el almacenamiento y la transmisión no autorizados de materiales protegidos por derechos de autor [...] ⁵⁰.

Lo que resulta interesante de la letra (a) del 16.3 es que, de manera expresa, se obliga a los países a que suscriban el tratado a establecer medidas que provean incentivos legales para que los prestadores de servicio cooperen con titulares de derechos de autor, ya sea por actos de almacenamiento, como también de transmisión de material protegido. Dada la naturaleza del instrumento, no se especifica en qué podrían consistir dichas medidas o incentivos, pero resulta problemático al menos en dos sentidos. En primer lugar, porque una prescripción en este sentido no clarifica la estrategia procesal para llevar adelante la medida, lo que permitiría la cooperación entre privados, incluso sin pasar por el filtro

50. [Nota del editor: la traducción es del autor] En idioma original expresa:

3. For the purpose of providing enforcement procedures that permit effective action against any act of copyright infringement covered by this Chapter, including expeditious remedies to prevent infringements and criminal and civil remedies that constitute a deterrent to further infringements, each Party shall provide, consistent with the framework set out in this Article:

(a) legal incentives for service providers to cooperate with copyright owners in deterring the unauthorized storage and transmission of copyrighted materials[...]

jurisdiccional, lo que es de la mayor importancia, cuando se trata de medidas que eventualmente pueden afectar el ejercicio de derechos fundamentales en línea. En segundo lugar, es problemático porque este tipo de medidas se emparenta, de alguna manera, con ciertas prácticas hoy legales que se han implementado en algunos países europeos, donde sea a través de un sistema privado (el caso de Francia y la ley HADOPI), o uno pseudoadministrativo (en España), se verifican medidas de corte de conexiones a usuarios acusados de intercambios no autorizados de archivos.

En el artículo 16.3 letra (b) se hace referencia expresa a la responsabilidad de los prestadores de servicios de Internet, donde se establecen reglas relativas a actividades de transmisión; enrutamiento o provisión material; actividades de *caching* a través de procedimientos automatizados, almacenamiento o enlace, en similar redacción a lo dispuesto en la ley chilena, como se verá más adelante. Adicionalmente, el artículo 16.3.b.xi indica que

- (xi) Cada Parte establecerá un procedimiento administrativo o judicial que permita que los titulares de derechos de autor que han efectuado notificación efectiva de una infracción reclamada obtengan de forma expedita por parte de un proveedor de servicios información en su poder que identifique al supuesto infractor.⁵¹

Más allá de que los términos de este artículo exceden tanto el texto regular de los Tratados de Libre Comercio como también, en cierta medida, las resoluciones establecidas en la propia DMCA, esta norma deja entregada a las autoridades nacionales la decisión de establecer procedimientos o bien administrativas o bien judiciales con el fin de entregar información respecto de un eventual infractor desde un prestador de servicios de Internet a un titular de derechos de autor. Como es posible verificar, esta previsión contempla la posibilidad de que se trate de procedimientos de notificación y bajada administrativos o judiciales que impliquen la posibilidad de que quien ha llevado adelante notificación efectiva de acuerdo con la norma consiga información relevante de los usuarios, la que en cualquier caso debiera contemplar medidas de protección de los derechos vinculados con la privacidad y la protección de los datos personales. Esto resulta especialmente

51. Nota del editor: la traducción es del autor] En idioma original expresa:

(xi) Each Party shall establish an administrative or judicial procedure enabling copyright owners who have given effective notification of claimed infringement to obtain expeditiously from a service provider information in its possession identifying the alleged infringer.

importante, teniendo presente no solo la heterogeneidad de normativa respecto de responsabilidad de intermediarios, sino, también, las peculiaridades de la normativa regional en torno a la protección de los datos personales y la privacidad, que en buena parte de los países de la región no cumple con los estándares internacionalmente aceptados por gran parte de los países europeos.

II.C.II. La regulación de la responsabilidad de prestadores de servicios de Internet en Chile

En este país, el proceso de modificación a la Ley de Propiedad Intelectual se produjo a propósito del cumplimiento de tratados internacionales y, fundamentalmente, del Capítulo sobre Propiedad Intelectual del Tratado de Libre Comercio entre ese país y los Estados Unidos de América⁵². Conforme a dicho tratado, las partes se obligaron a proveer incentivos legales para la cooperación entre proveedores de servicios y titulares de derechos de autor además de limitaciones a la responsabilidad de aquellos⁵³. Tales limitaciones debían referirse a la exención de responsabilidad civil y a las medidas judiciales respecto de ciertas funciones técnicas de forma excluyente, a saber:

- (i) transmisión, enrutamiento o suministro de conexiones para el material sin modificar su contenido;
- (ii) almacenamiento temporal (*cached*) llevado a cabo mediante un proceso automático;
- (iii) almacenamiento a petición de un usuario de material que se aloja en un sistema o red controlada u operada por o para el proveedor, incluidos correos electrónicos y sus archivos adjuntos almacenados en el servidor del proveedor y páginas web alojadas en el servidor del proveedor; y
- (iv) referir o vincular a los usuarios a un sitio en línea mediante la utilización de herramientas de búsqueda de información, incluidos hipervínculos y directorios⁵⁴ [.]

siempre y cuando el proveedor no fuera quien inicia la transmisión o selecciona el material o sus destinatarios, con algunas condiciones formales

52. Tratado de Libre Comercio Chile-Estados Unidos (vigente desde 1º de enero de 2004), capítulo Diecisiete: Derechos de propiedad intelectual.

53. TLC Chile-Estados Unidos, cap. 17 (a).

54. TLC Chile-Estados Unidos, cap. 17 (b).

adicionales para la procedencia del respectivo sistema. Es decir, se trata de un régimen destinado a quienes no proveen directamente el contenido, sino que actúan más bien como intermediarios.

Desde el Tratado en cuestión, se fija un procedimiento de notificación y bajada de contenidos, relativo al retiro y bloqueo de los servicios de almacenamiento y de búsqueda y enlace, creando la obligatoriedad para ambas partes de establecer legalmente tal procedimiento, que involucre la «notificación efectiva» del material infractor al respectivo responsable del prestador de servicios⁵⁵. Por cierto, la obligatoriedad de dicho sistema, así fijada, ya era cumplida por los Estados Unidos a través del procedimiento de notificación y bajada de la DMCA, quedando en negociación solamente los caracteres de dicha normativa que se haría exigible implementar en Chile y siendo el punto de la notificación efectiva precisamente uno donde la ley chilena representará mayor innovación frente a la normativa internacional existente e, incluso, en discusión.

A mediados del año 2010, se dictó en Chile la que sería la reforma a la ley de propiedad intelectual más importante en sus cuarenta años de vigencia⁵⁶, aprovechando una instancia de modificación legal imperativa bajo el TLC antes mencionado para introducir otros cambios sensibles en materias sustantivas de la ley, como el régimen de excepciones y limitaciones al derecho de autor y la solución de conflictos por tarifas impuestas por sociedades de gestión colectiva⁵⁷. Si bien no todas las materias contempladas en el TLC fueron implementadas a través de esta ley (como ejemplo, las medidas de protección tecnológica fueron dejadas de lado en esta ocasión), se introdujo un capítulo completo a la ley de derechos de autor chilena para implementar las obligaciones de delimitación de responsabilidad de los prestadores de servicios de Internet.

El capítulo sobre «Limitación de responsabilidad de los prestadores de servicios de Internet» de la Ley sobre Propiedad Intelectual chilena establece estas exenciones de responsabilidad, siguiendo de cerca la delimitación de proveedores hecha por el TLC. Como condiciones generales para los distintos

55. TLC Chile-Estados Unidos, cap. 17 (f).

56. Ley 20435 del 5 de mayo de 2010, que modifica a la Ley 17336 sobre Propiedad Intelectual.

57. En Chile, la afiliación a una sociedad de gestión colectiva de derechos de autor es voluntaria. No obstante, su comportamiento, propio de instituciones monopólicas, ha llevado a cuestionamientos por parte de la autoridad en materia económica, por el posible abuso de esta posición dominante.

prestadores de servicios, para gozar de estas limitaciones de responsabilidad, se establecen tres condiciones generales, de las que solamente se exceptúa a los servicios de búsqueda, enlace o referencia. Tales condiciones son:

- a) haber establecido condiciones generales y públicas, bajo las cuales este podrá hacer uso de la facultad de poner término a los contratos de los proveedores de contenido calificados judicialmente como infractores reincidentes de los derechos protegidos por esta ley⁵⁸;
- b) no interferir en las medidas tecnológicas de protección y de gestión de derechos de obras protegidas ampliamente reconocidas y utilizadas lícitamente;
- c) no haber generado, ni haber seleccionado el material o a sus destinatarios⁵⁹.

Además de esas condiciones generales, existen condiciones específicas que difieren según el servicio que preste cada buscador. En primer término, la ley se dedica a los meros proveedores de acceso, conexión y enrutamiento, desligándolos de responsabilidad en la medida en que no interfieran con el contenido de que se trate⁶⁰.

58. Llama la atención que un proveedor *deba* establecer su propia facultad en términos unilaterales de contratos ante infracciones legales, en lugar de hacerlo un juez o llegarle a ello tras un procedimiento legalmente establecido para un resultado así de lesivo del derecho de utilizar la tecnología de comunicación provista por Internet. En tal sentido, se pone a cargo del prestador de servicios de Internet algo ya buscado e, incluso, logrado en jurisdicciones como la francesa (con la Ley HADOPI): que las reincidencias en materia de infracción de derechos de propiedad intelectual tengan por consecuencia la desconexión de los usuarios.

59. Véase Ley 17336, artículo 85 o.

60. Véase Ley 17336, artículo 85 m:

Los prestadores de servicios de transmisión de datos, enrutamiento o suministro de conexiones no serán considerados responsables de los datos transmitidos a condición de que el prestador:

- a) no modifique ni seleccione el contenido de la transmisión. Para estos efectos no se considerará modificación del contenido, la manipulación tecnológica del material necesaria para facilitar la transmisión a través de la red, como la división de paquetes;
- b) no inicie él la transmisión, y
- c) No seleccione a los destinatarios de la información.

Esta limitación de responsabilidad comprende el almacenamiento automático o copia automática y temporal de los datos transmitidos, técnicamente necesarios para ejecutar la transmisión, siempre que este almacenamiento o copia automática no esté accesible al público en general y no se mantenga almacenado por más tiempo del razonablemente necesario para realizar la comunicación.

En segundo término, la ley establece condiciones para los prestadores de almacenamiento temporal y automático⁶¹. Las condiciones, en esta oportunidad, son las de no intervenir respecto de los procesos tecnológicos establecidos por proveedores de origen del contenido, ni sobre la tecnología que admite la interacción con ese proveedor. Además, se reitera el deber de no modificar el contenido. Finalmente, se establece la irresponsabilidad de esta clase de proveedores allí donde el proveedor impida el acceso a material que, a su vez, haya sido retirado de ese proveedor de origen, una vez notificado de tal deber conforme a la ley. Es esta la primera mención operativa de la noción de notificación o conocimiento efectivo.

Esta mención es más relevante a propósito del tercer grupo de proveedores de Internet identificado por la ley chilena: los prestadores de almacenamiento para usuarios y los servicios de búsqueda, enlace y referencia. Es decir, los prestadores de servicios que permiten el acceso a contenidos provistos por terceros, precisamente el grupo de proveedores de servicios de Internet sobre los que se cierne con más fuerza la amenaza de hacer valer la responsabilidad civil, suponiendo que, en alguna capacidad mayor que los meros proveedores de conexión o de almacenaje automático y temporal, ellos tienen una posibilidad más inmediata de conocer del contenido puesto a disposición por ellos mismos. Por tal razón, es esa la clase de servicios que recibe usualmente, especialmente en los Estados Unidos de América, la mayor cantidad de notificaciones y avisos para la operación del sistema de *notice and take-down*.

61. Véase Ley 17336, artículo 85 n:

Los prestadores de servicios que temporalmente almacenen datos mediante un proceso de almacenamiento automático no serán considerados responsables de los datos almacenados a condición que el prestador:

- a) respete las condiciones de acceso de usuarios y las reglas relativas a la actualización del material almacenado establecidas por el proveedor del sitio de origen, salvo que dichas reglas sean usadas por este para prevenir o dificultar injustificadamente el almacenamiento temporal a que se refiere este artículo;
- b) no interfiera con la tecnología compatible y estandarizada utilizada en el sitio de origen para obtener información sobre el uso en línea del material almacenado, cuando la utilización de dichas tecnologías se realice de conformidad con la ley y sean compatibles con estándares de la industria ampliamente aceptados;
- c) no modifique su contenido en la transmisión a otros usuarios, y
- d) retire o inhabilite en forma expedita el acceso a material almacenado que haya sido retirado o al que se haya inhabilitado el acceso en su sitio de origen, cuando reciba una notificación de conformidad con el procedimiento establecido en el artículo 85 o.

Las condiciones para que estos últimos proveedores no estén sujetos a la responsabilidad establecida en la ley de derechos de autor en Chile, son: que el prestador no tenga «conocimiento efectivo» del carácter ilegal del contenido; que el prestador no obtenga un beneficio económico que sea directamente atribuible a la actividad infractora, debiendo y pudiendo controlarlo; que el prestador tenga designado un representante a quien hacer llegar notificaciones y, finalmente, que retire o impida, de forma expedita, el acceso al contenido infractor⁶². Condiciones todas que han sido ya recogidas por las leyes extranjeras ya mencionadas con anterioridad.

Pero el carácter que distingue favorablemente la ley chilena dentro del contexto internacional, es respecto de la definición de «conocimiento efectivo» entregada a propósito de estos prestadores de contenido aportado por terceros. Para entender que existe «conocimiento efectivo» y que, por lo tanto, el prestador de servicios es responsable, a diferencia de los sistemas de notificación extrajudicial de existencia de contenido infractor, se requiere cumplir dos requisitos: primero, que exista una orden judicial, emanada de tribunal competente, que ordene el retiro del contenido o el bloqueo de su acceso; segundo, que habiendo sido notificado de dicha orden judicial, el prestador de servicios no la cumpla «de manera expedita»⁶³.

En consecuencia, no hay conocimiento efectivo sin una orden judicial de retiro o bloqueo, que a su vez no haya sido obedecida. Ese dictamen

62. Véase Ley 17336, artículo 85 ñ, inciso primero:

Los prestadores de servicios que a petición de un usuario almacenan, por sí o por intermedio de terceros, datos en su red o sistema o que efectúan servicios de búsqueda, vinculación y o referencia a un sitio en línea mediante herramientas de búsqueda de información, incluidos los hipervínculos y directorios, no serán considerados responsables de los datos almacenados o referidos a condición de que el prestador:

- a) no tenga conocimiento efectivo del carácter ilícito de los datos;
- b) no reciba un beneficio económico directamente atribuible a la actividad infractora, en los casos en que tenga el derecho y la capacidad para controlar dicha actividad;
- c) designe públicamente un representante para recibir las notificaciones judiciales a que se refiere el inciso final, de la forma que determine el reglamento, y
- d) retire o inhabilite en forma expedita el acceso al material almacenado de conformidad a lo dispuesto en el inciso siguiente.

63. Véase Ley 17336, artículo 85 ñ, inciso segundo: «Se entenderá que el prestador de servicios tiene un conocimiento efectivo cuando un tribunal de justicia competente, conforme al procedimiento establecido en el artículo 85 o, haya ordenado el retiro de los datos o el bloqueo del acceso a ellos y el prestador de servicios, estando notificado legalmente de dicha resolución, no cumpla de manera expedita con ella».

jurisdiccional, que puede o no estar enmarcado en un proceso judicial ya iniciado (esto es, se puede solicitar prejudicialmente antes de requerir la responsabilidad del infractor, a fin de cautelar los derechos de quien se ha visto afectado por el ilícito), debe ponderar otros bienes puestos en riesgo a través de la misma orden (eficacia, factibilidad técnica, eventual daño al ya afectado, posibilidad de medidas menos gravosas) y puede accionar solamente:

- respecto de los proveedores de conexión, transmisión o enrutamiento, «medidas razonables» que impidan acceso a un contenido infractor sin implicar bloqueo de contenidos lícitos;
- respecto de los proveedores de almacenamiento (temporal o no), el retiro o el bloqueo al contenido ilícito o la terminación de los servicios de infractores reincidentes⁶⁴.

Entendiendo esto como quien haga operar el sistema de notificación y bajada de contenido de forma maliciosa o como quien provea datos

64. Véase Ley 17336, artículo 85 R:

En los casos en que se hayan cumplido los requisitos generales del artículo 85 o y los requisitos establecidos en el artículo 85 m, respecto de las funciones de transmisión, enrutamiento o suministro, el tribunal solo podrá disponer como medida prejudicial o judicial la adopción de medidas razonables para bloquear el acceso a un determinado contenido infractor que sea claramente identificado por el solicitante y que no implique el bloqueo de otros contenidos legítimos, de acuerdo con lo dispuesto en el inciso segundo del artículo precedente.

En los casos en que se hayan cumplido los requisitos generales del artículo 85 o y los requisitos especiales establecidos en los artículos 85 N y 85 Ñ, respecto de las funciones mencionadas en dichos artículos, el tribunal solo podrá disponer como medidas prejudiciales o judiciales las siguientes:

- a) el retiro o inhabilitación del acceso al material infractor que sea claramente identificado por el solicitante de acuerdo con lo dispuesto en el inciso segundo del artículo 85 q;
- b) la terminación de cuentas determinadas de infractores reincidentes de dicho prestador de servicio, que sean claramente identificadas por el solicitante de acuerdo con lo dispuesto en el inciso segundo del artículo 85 q, y cuyo titular esté usando el sistema o red para realizar una actividad infractora a los derechos de autor y conexos.

Todas estas medidas se dictarán con la debida consideración de la carga relativa para el prestador de servicios, para los usuarios y para los suscriptores, del eventual daño al titular del derecho de autor o conexos, de la factibilidad técnica y eficacia de la medida, y de la existencia de otras formas de observancia menos gravosas para asegurar el respeto del derecho que se reclama.

Estas medidas se decretarán previa notificación al prestador de servicios, de conformidad con los incisos tercero, cuarto y quinto del artículo 85 q, con la excepción de los mandamientos judiciales que busquen asegurar la preservación de la evidencia o cuando se trate de otros mandamientos judiciales que se estime no tendrán un efecto real en la operación del sistema o red del prestador de servicios.

falsos dentro de este procedimiento, será también responsable por los perjuicios causados⁶⁵, tales medidas pueden ser, incluso, decretadas *ex parte*, habida caución por parte del solicitante y motivos graves fundantes. El procedimiento, en tanto, tiene el carácter de «breve y sumario», y se sigue ante un juez civil, debiendo individualizarse con precisión los derechos infringidos, su titularidad, el contenido infractor, la forma de infracción y su ubicación en la red. Sin embargo, este mismo procedimiento contempla la posibilidad de oposición, a partir de la solicitud del proveedor de que se deje sin efecto la medida decretada⁶⁶. Por cierto, en el mismo procedimiento

65. Véase Ley 17336, artículo 85 τ: «El que, a sabiendas, proporcione información falsa relativa a supuestas infracciones a los derechos reconocidos en esta ley, deberá indemnizar los daños causados a cualquier parte interesada, si estos daños son resultado de acciones que el proveedor de servicios de red tome con base en dicha información y le será aplicable lo dispuesto en el artículo 197 del Código Penal».

66. Véase Ley 17336, artículo 85 ο:

Para las infracciones a los derechos reconocidos por esta ley cometidas en o por medio de redes o sistemas controlados u operados por o para prestadores de servicios, el titular de los respectivos derechos o su representante podrán solicitar como medida prejudicial o judicial las que se señalan en el artículo 85 r. Cuando las medidas se soliciten en carácter de prejudicial, y siempre que existan razones graves para ello, se podrán decretar sin audiencia del proveedor del contenido, pero debiendo el solicitante rendir caución previa, a satisfacción del tribunal. Esta solicitud será conocida por el juez de letras en lo civil del domicilio del prestador de servicios, sin perjuicio de las acciones penales que pudieran interponerse.

Para estos efectos, la solicitud, además de cumplir con los requisitos de los números 1°, 2° y 3° del artículo 254 del Código de Procedimiento Civil, deberá indicar claramente:

- a) los derechos supuestamente infringidos, con indicación precisa de la titularidad de estos y la modalidad de la infracción;
- b) el material infractor, y
- c) la localización del material infractor en las redes o sistemas del prestador de servicios respectivos.

Cumplido lo dispuesto en el inciso anterior, el tribunal decretará sin demora el retiro o bloqueo de los contenidos infractores. Dicha resolución se notificará por cédula al prestador de servicios respectivo y por el estado diario al solicitante.

El proveedor de contenido afectado podrá, sin perjuicio de otros derechos, requerir al tribunal que decretó la orden que se deje sin efecto la medida de restricción de acceso o retiro de material. Para ello, deberá presentar una solicitud que cumpla con los mismos requisitos señalados en el inciso segundo y deberá acompañar todo antecedente adicional que fundamente esta petición e implicará su aceptación expresa de la competencia del tribunal que está conociendo del asunto.

Este procedimiento se tramitará breve y sumariamente, y las apelaciones se concederán en el solo efecto devolutivo, gozando de preferencia para su conocimiento y vista por el tribunal de alzada.

el tribunal puede tomar las medidas para identificar al verdadero infractor, en orden a perseguir su responsabilidad directa⁶⁷. Es este carácter de judicialización del procedimiento que antecede al retiro o bloqueo de un contenido lo que genera que se aparte esta ley del resto de las legislaciones sobre la materia.

La ley chilena no establece una prohibición de controlar o monitorear contenido, sino que, siguiendo normas tales como la Directiva sobre Comercio Electrónico del Parlamento Europeo, solamente se los dispensa del deber de hacerlo⁶⁸, igualmente aplicable para todos los prestadores aludidos por la ley. Esto coincide, no obstante, con una obligación más general de no intervención sobre los contenidos, establecida ya no a propósito de los derechos de propiedad intelectual eventualmente afectados por el tráfico en Internet, sino por las obligaciones derivadas de la ley chilena sobre neutralidad de la red⁶⁹.

Una peculiaridad, en la que vemos escasa utilidad más allá del amedrentamiento, es el deber de los prestadores acerca de informar a sus usuarios, supuestamente infractores, de los avisos de aparentes infracciones cometidas, con información completa sobre el representante del afectado, contenido infractor, derechos vulnerados, forma de infracción, ubicación en la red y otros datos, dentro de cinco días desde recibido el reclamo⁷⁰.

67. Véase Ley 17336, artículo 85 s: «El tribunal competente, a requerimiento de los titulares de derechos que hayan iniciado el procedimiento establecido en el artículo precedente podrá ordenar la entrega de la información que permita identificar al supuesto infractor por el prestador de servicios respectivo. El tratamiento de los datos así obtenidos se sujetará a lo dispuesto en la Ley 19628, sobre protección de la vida privada».

68. Véase Ley 17336, artículo 85 p:

Los prestadores de servicios referidos en los artículos precedentes no tendrán, para efectos de esta ley, la obligación de supervisar los datos que transmitan, almacenen o referencien ni la obligación de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas.

Lo establecido en el inciso anterior se comprenderá sin perjuicio de cualquier actividad que los tribunales ordinarios de Justicia decreten para investigar, detectar y perseguir delitos o prácticas constitutivas de ejercicios abusivos de los derechos de autor o conexos reconocidos por esta ley.

69. Véase la Ley 20453, que consagra el principio de Neutralidad en la red para los Consumidores y usuarios de Internet, del 26 de agosto de 2010.

70. Véase Ley 17336, artículo 85 u:

Sin perjuicio de las disposiciones previas contenidas en este capítulo, los prestadores de servicios de Internet deberán comunicar por escrito a sus usuarios los avisos de supuestas infracciones que reciban, a condición de que en la comunicación que reciban cumplan los siguientes requisitos:

Una gran duda aún no resuelta por la ley chilena tiene que ver con su carácter de norma especial, pero que no rige en perjuicio de las normas generales sobre responsabilidad civil. En otras palabras, si bien la ley chilena intenta resolver el problema de responsabilidad de la que hemos venido hablando en el presente informe, deja expresamente libre el camino para demandar de parte de los prestadores de servicios de Internet a través de la justicia civil y mediante las reglas ordinarias de esa forma de responsabilidad. En efecto, con esa mención es que comienza el respectivo capítulo de la Ley de Propiedad Intelectual⁷¹. Asimismo, y como parece lógico, estas normas, por lesivas que resulten respecto del prestador de servicios, no operan en perjuicio de la eventual responsabilidad penal que pueda hacerse valer.

-
- a) reciba en forma electrónica o de otra forma escrita del titular de los derechos o de su representante aviso de la supuesta infracción;
 - b) el titular de los derechos o su representante deberá tener domicilio o residencia en Chile y, en su caso, contar con poder suficiente para ser emplazado en juicio, en representación del titular;
 - c) se identifiquen los derechos supuestamente infringidos, con indicación precisa de la titularidad de estos y la modalidad de la infracción;
 - d) se identifique el material infractor y su localización en las redes o sistemas del prestador de servicios a quien se envía la comunicación, a través del url o sus equivalentes, y
 - e) contenga datos que permitan al prestador de servicios identificar al usuario proveedor del supuesto material infractor.

Los prestadores de servicios de Internet, una vez recibida una comunicación de conformidad al inciso anterior, informarán al usuario supuestamente infractor esta situación acompañando los antecedentes proporcionados por el titular del derecho o su representante, dentro del plazo de cinco días hábiles contados desde la recepción de la referida comunicación.

71. Véase Ley 17336, artículo 85 L:

Sin perjuicio de las normas generales sobre responsabilidad civil aplicables, en el caso de aquellas infracciones a los derechos protegidos por esta ley cometidas por terceros, que ocurran a través de sistemas o redes controladas u operadas por personas naturales o jurídicas que presten algunos de los servicios señalados en los artículos siguientes, los prestadores de tales servicios no serán obligados a indemnizar el daño, en la medida que cumplan con las condiciones previstas en los artículos siguientes para limitar tal responsabilidad, conforme a la naturaleza del servicio prestado. En estos casos, los prestadores de servicio solo podrán ser objeto de las medidas prejudiciales y judiciales a que se refiere el artículo 85 r.

[Nota de los autores: el destacado es nuestro.]

II.C.III. La responsabilidad por propiedad intelectual: el caso Taringa!

A mediados de 2011, en la ciudad de Buenos Aires, capital de la República Argentina, fue confirmado el procesamiento penal de los hermanos Hernán y Matías Botbol por el delito de violación a la propiedad intelectual realizado a través de la página web de la que ellos son administradores y representantes, el sitio conocido como Taringa!. Dicho sitio, de alta popularidad, tiene como objeto la subida de contenidos por parte de sus usuarios registrados –fundamentalmente textos e imágenes–, quienes de tal forma discuten y «comparten» contenidos protegidos por las normas sobre propiedad intelectual. En tal sentido, por intermedio de la página es posible acceder a un sinnúmero de enlaces, varios de ellos dirigidos a la descarga de obras protegidas, tal como fue denunciado por un grupo de editoriales argentinas, en tanto titulares de derechos de autor sobre diversas obras literarias.

Si bien el caso judicial trata de la búsqueda de la responsabilidad de carácter penal de los hermanos Botbol, escapando parcialmente del foco de nuestro análisis, dentro de este incipiente proceso judicial surgen varias claves que se han convertido en parte de una álgida discusión en la Argentina. El fallo que confirma el procesamiento, emitido por la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Argentina⁷², los hermanos Botbol tendrían tanto la calidad de «partícipes necesarios» como la de efectivos «conocedores» de la actividad ilícita, lo que justificaría la persecución penal⁷³. A pesar de que la página registraba al momento del fallo decenas de millones de visitas mensualmente y más de veinte mil nuevos mensajes de la comunidad con enlaces hacia otros sitios, la Cámara no deja lugar a dudas sobre la participación de los administradores del sitio en cuanto el mismo facilita la posibilidad de que se «publiciten obras que, finalmente, eran reproducidas sin consentimiento de sus titulares». El grado de tal participación en los delitos, en tanto, es una cuestión que queda por resolver. De manera aún más tajante, la Cámara reafirma su certeza sobre

72. Sentencia sobre recurso de apelación, Causa N° 41.181 *www.taringa.net y otros / procesamiento*, Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional.

73. De la sentencia que confirma el procesamiento: «Adviértase que si bien los autores del hecho finalmente serían aquellos que subieron la obra al website y los que “la bajan”, lo cierto es que el encuentro de ambos obedece a la utilización de la página *www.taringa.net*, siendo sus responsables al menos partícipes necesarios de la maniobra y, además, claros conocedores de su ilicitud, por lo que el convenio que exhiben para pretender exonerarse de responsabilidad [las condiciones de uso del sitio] no podrá ser tenido en cuenta».

la calidad de «claros conocedores» de esos administradores en cuanto a los mensajes con enlaces a material protegido. No es difícil ser incrédulo ante esa hipótesis: revisar todos los mensajes diarios; examinar si todos ellos dirigen hacia obras para su descarga; estudiar si las obras están protegidas y analizar si el acto de subida (posiblemente hecho por alguien distinto a quien enlaza) fue hecho sin autorización o infringiendo derechos exclusivos, parece al menos una tarea de difícil ejecución sobre veinte mil mensajes diarios. La idea de que un administrador *sepa o debiera saber* sobre los contenidos que se suben a su sitio o se enlazan desde este, a la luz de situaciones como las de Taringa!, obliga a ser cuidadoso con las atribuciones de responsabilidad que hagan caso omiso de las particularidades de cada búsqueda de esa responsabilidad.

Del eventual fallo de Taringa!,⁷⁴ a pesar de tratarse de un proceso criminal, nacerán, sin duda alguna, consecuencias para la búsqueda de responsabilidad en el ámbito civil en sitios similares o, incluso, en aquellos motores de búsqueda que enlazan a otros sitios o contenidos de manera automatizada. Especialmente ello ocurrirá si a pesar de buscarse responsabilidad penal bajo los estrictos márgenes de sus normas y principios, se extiende esta a situaciones como las ya descritas y confirmadas en el procesamiento de los titulares de Taringa!

III.C.IV. Las propuestas legislativas en curso

II.C.IV.a. COLOMBIA. Tal como en el caso de Chile, Colombia ha dedicado los últimos años a la negociación y firma de un TLC con los Estados Unidos de América, en términos muy similares respecto de la protección de la propiedad intelectual y también de la responsabilidad de los prestadores de servicio de Internet⁷⁵. Aun antes de la plena entrada en vigor de dicho tratado, se produjo en los últimos meses una polémica en torno a una propuesta de ley que modifica la legislación sobre derechos de autor en ese país e incluye entre sus reformas nuevas reglas sobre responsabilidad de prestadores de servicios de Internet.

74. El procesamiento fue posteriormente ratificado por la misma sala, con fecha 25 de octubre de 2011.

75. Acuerdo de Promoción Comercial entre Estados Unidos y Colombia (no ratificado), capítulo 16.

Esta propuesta de ley⁷⁶, conocida popularmente (especialmente entre sus detractores) como «Ley Lleras»⁷⁷, recoge de forma muy similar a la ley chilena sobre estos temas tanto las definiciones sobre los prestadores de servicios de Internet acogidos a sus normas⁷⁸, como sobre los regímenes de responsabilidad civil y penal⁷⁹ que continúan siendo aplicables⁸⁰, así como también, sobre la ausencia de deber de supervisión⁸¹.

76. Proyecto 241 de 2011, por medio del cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet.

77. El nombre de «Ley Lleras» fue adoptado coloquialmente, como derivación del nombre del ministro de Interior y Justicia de Colombia, don Germán Vargas Lleras, quien presentó dicho proyecto al Congreso Nacional de Colombia el 4 de abril de 2011.

78. Proyecto N° 241, véase artículo 1:

Prestadores de servicios de Internet. A los efectos de esta ley se entenderán por tales las personas que presten uno o varios de los siguientes servicios:

- a) transmitir, enrutar o suministrar conexiones para materiales sin hacer modificaciones en su contenido;
- b) almacenar datos temporalmente mediante un proceso automático (caching);
- c) almacenar a petición de un usuario del material que se aloja en un sistema o red controlado u operado por o para el prestador de servicios; y
- d) aeeferir o vincular a los usuarios a un sitio en línea mediante la utilización de herramientas de búsqueda de información, incluyendo hipervínculos y directorios.

79. Véase artículo 2:

Régimen de responsabilidad. Los prestadores de servicio de Internet, los proveedores de contenido, y los usuarios serán responsables por el uso de los contenidos, de conformidad con las normas generales sobre responsabilidad civil, penal y administrativa. La información utilizada en sistemas o redes informáticas será protegida por la legislación sobre derecho de autor y derechos conexos si reúne las condiciones de tal protección.

El artículo aquí citado, no obstante, estaría sujeto a modificación conforme a lo discutido en el debate sobre la ley en la Comisión Primera del Senado de Colombia, el 14 de junio de 2011, que aprobó el proyecto en general para ser discutido por el Plenario del Senado.

80. Véase artículo 4:

Exoneración de la responsabilidad de los prestadores de servicios en internet. Sin perjuicio de las normas generales sobre responsabilidad civil aplicables, en el caso de aquellas infracciones al derecho de autor y derechos conexos cometidas por terceros, que ocurran a través de sistemas o redes controladas u operadas por personas naturales o jurídicas que presten algunos de los servicios señalados en los artículos siguientes, los prestadores de tales servicios no serán obligados a indemnizar el daño, en la medida que cumplan con las condiciones previstas en los artículos siguientes para limitar tal responsabilidad, conforme a la naturaleza del servicio prestado.

En estos casos, los prestadores de servicios de Internet solo podrán ser objeto de las medidas cautelares y judiciales a que se refieren los artículos 13, 14 y 16 de esta Ley.

81. Véase artículo 3:

Inexistencia de obligación general de supervisión. Los prestadores de servicios de Internet no tendrán, para efectos de esta ley, la obligación de supervisar los datos que

A propósito de la exención de responsabilidad, clasifica de forma similar a la ley chilena respecto de los distintos proveedores, distinguiendo las causales de liberación de responsabilidad según si se trata de prestadores de acceso, conexión y enrutamiento^{82 y 83}, de almacenamiento temporal⁸⁴ y

transmitan, almacenen o referan, ni la obligación de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas.

Lo establecido en el inciso anterior se entenderá sin perjuicio que la autoridad competente ordene a los prestadores de servicios de Internet realizar alguna actividad a efecto de investigar, detectar y perseguir delitos o cualquier infracción al derecho de autor o los derechos conexos.

82. Véanse artículo 5:

Prestadores de servicios de transmisión de datos, enrutamiento o suministro de conexiones. Los prestadores de servicios de transmisión de datos, enrutamiento o suministro de conexiones no serán considerados responsables de los datos transmitidos a condición que el prestador:

- a) no modifique ni seleccione el contenido de la transmisión. Para estos efectos no se considerará modificación del contenido, la manipulación tecnológica del material necesaria para facilitar la transmisión a través de la red, como la división de paquetes;
- b) no inicie la transmisión;
- c) no seleccione a los destinatarios de la información;
- d) establezca condiciones generales y públicas, bajo las cuales el prestador de servicios podrá hacer uso de la facultad de finalizar los contratos de los proveedores de contenido que sean infractores reincidentes de los derechos protegidos por las leyes de derecho de autor o derechos conexos;
- e) no interfiera en las medidas tecnológicas de protección y de gestión de derechos de obras protegidas;
- f) no genere ni seleccione el material o a sus destinatarios.

Y Parágrafo:

En los casos en que se hayan cumplido los requisitos de este artículo, el juez competente solo podrá disponer como medida cautelar o mediante sentencia, la adopción de medidas razonables para bloquear el acceso a un determinado contenido infractor o supuestamente infractor que sea claramente identificado por el solicitante y que no implique el bloqueo de otros contenidos legítimos.

83. Tal como en la ley chilena, llama aquí la atención que el proveedor deba establecer su propia facultad de término unilateral por infracciones reincidentes.

84. Véanse artículo 6:

Prestadores de servicios de almacenamiento temporal llevado a cabo mediante un proceso automático. Los prestadores de servicios que temporalmente almacenen datos mediante un proceso automático realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, no serán considerados responsables de los datos almacenados a condición que el prestador:

- a) respete las condiciones de acceso de usuarios y las reglas relativas a la actualización del material almacenado establecidas por el proveedor del sitio de origen, salvo que dichas reglas sean usadas por este para prevenir o dificultar injustificadamente el almacenamiento temporal a que se refiere este artículo;

de almacenamiento a solicitud de terceros⁸⁵, separando de forma especial (al menos desde el punto de vista formal) a los proveedores de servicios de

- b) no interfiera con la tecnología compatible y estandarizada utilizada en el sitio de origen para obtener información sobre el uso en línea del material almacenado, cuando la utilización de dichas tecnologías se realice de conformidad con la ley y sean compatibles con estándares de la industria ampliamente aceptados;
- c) no modifique su contenido en la transmisión a otros usuarios;
- d) retire o inhabilite en forma expedita el acceso a material almacenado que haya sido retirado o al que se haya inhabilitado el acceso en su sitio de origen, cuando reciba una solicitud de retiro de conformidad con el procedimiento establecido en los artículos 9, 10, 11 y 12 de esta ley.
- e) establezca condiciones generales y públicas, bajo las cuales el prestador de servicios podrá hacer uso de la facultad de finalizar los contratos de los proveedores de contenido que sean infractores reincidentes de los derechos protegidos por el derecho de autor o derechos conexos;
- f) no interfiera en las medidas tecnológicas de protección y de gestión de derechos de obras protegidas; y
- g) no genere ni seleccione el material o a sus destinatarios.

Y Parágrafo:

En los casos en que se hayan cumplido los requisitos de este artículo, el juez competente soloso podrá disponer como medida cautelar o mediante sentencia el retiro o inhabilitación del acceso al material infractor que sea claramente identificado por él; y/o la terminación de cuentas determinadas de infractores reincidentes de dicho prestador de servicio, que sean claramente identificadas por el solicitante, y cuyo titular esté usando el sistema o red para realizar una actividad infractora al derecho de autor o derechos conexos.

85. Véanse artículo 7:

Prestadores de servicios de almacenamiento a petición del usuario del material que se aloja en un sistema o red controlado u operado por o para el prestador de servicios. Los prestadores de servicios que a petición de un usuario almacenan, por sí o por intermedio de terceros, datos en su red o sistema, no serán responsables del contenido almacenado a condición que el prestador:

- a) no tenga conocimiento efectivo del supuesto carácter ilícito de los datos;
- b) no reciba un beneficio económico directamente atribuible a la actividad infractora, en los casos en que tenga el derecho y la capacidad para controlar dicha actividad;
- c) retire o inhabilite en forma expedita el acceso al material almacenado de conformidad a lo dispuesto en los artículos 9, 10, 11 y 12;
- d) designe públicamente un representante para recibir las notificaciones judiciales y un medio adecuado para recibir solicitudes de retiro o inhabilitación de material aparentemente infractor;
- e) establezca condiciones generales y públicas, bajo las cuales el prestador de servicios podrá hacer uso de la facultad de finalizar los contratos de los proveedores de contenido que sean infractores reincidentes de los derechos protegidos por el derecho de autor o derechos conexos;
- f) no interfiera en las medidas tecnológicas de protección y de gestión de derechos de obras protegidas; y
- g) no genere ni seleccione el material o a sus destinatarios.

búsqueda, de enlace y de referencia⁸⁶. En cuanto al contenido, no existen materias con diferencias (salvo formales) entre lo que establecen los tratados de libre comercio con los Estados Unidos ni lo fijado por la ley chilena.

Las diferencias más relevantes, y que han producido gran resistencia civil a la reforma propuesta⁸⁷, provienen del procedimiento establecido para hacer valer estas exenciones de responsabilidad. Tal como en la generalidad de los sistemas de notificación y bajada, es necesaria una comunicación completa al proveedor de servicios de quien se exige el retiro o bloqueo de contenidos. En la propuesta colombiana, sin embargo, esa

Y Parágrafo:

En los casos en que se hayan cumplido los requisitos de este artículo, el juez competente solo podrá disponer como medida cautelar o mediante sentencia el retiro o inhabilitación del acceso al material infractor que sea claramente identificado por él; y/o la terminación de cuentas determinadas de infractores reincidentes de dicho prestador de servicio, que sean claramente identificadas por el solicitante, y cuyo titular esté usando el sistema o red para realizar una actividad infractora al derecho de autor o derechos conexos.

86. Véanse artículo 8:

Prestadores de servicios consistentes en referir o vincular a los usuarios a un sitio en línea mediante la utilización de herramientas de búsqueda de información, incluyendo hipervínculos y directorios. Los prestadores de servicios que efectúan servicios de búsqueda, vinculación y/o referencia a un sitio en línea mediante herramientas de búsqueda de información, incluidos los hipervínculos y directorios, no serán considerados responsables de los datos almacenados o referidos a condición que el prestador:

- a) no tenga conocimiento efectivo del supuesto carácter ilícito de los datos;
- b) no reciba un beneficio económico directamente atribuible a la actividad infractora, en los casos en que tenga el derecho y la capacidad para controlar dicha actividad;
- c) retire o inhabilite en forma expedita el acceso al material almacenado de conformidad a lo dispuesto en los artículos 9, 10, 11 y 12;
- d) designe públicamente un representante para recibir las notificaciones judiciales y un medio adecuado para recibir solicitudes de retiro o inhabilitación de material aparentemente infractor.

Y Parágrafo:

En los casos en que se hayan cumplido los requisitos de este artículo, el juez competente solo podrá disponer como medida cautelar o mediante sentencia el retiro o inhabilitación del acceso al material infractor que sea claramente identificado por él; y/o la terminación de cuentas determinadas de infractores reincidentes de dicho prestador de servicio, que sean claramente identificadas por el solicitante, y cuyo titular esté usando el sistema o red para realizar una actividad infractora al derecho de autor o derechos conexos.

87. Especialmente clarificadora sobre el proceso completo resulta la contextualización y relación hecha por Botero, Carolina: «#Leylleras, crónica de una polémica social anunciada», en *Open Business Latin America*, 18 de junio de 2011, disponible [en línea], en: <<http://www.openbusinesslatinamerica.org/wp/2011/06/18/leylleras-chronica-de-una-polemica-social-anunciada>>. [Nota del editor: consultada el 5/11/11.]

comunicación, si bien completa, no requiere de la intervención judicial⁸⁸. Se exigen como requisitos: remisión formal por escrito; identificación del titular de derechos o su representante y domicilio en Colombia; identificación de la obra usada sin autorización; identificación de los derechos infringidos, su titularidad y forma de infracción; identificación de ubicación en la red; declaración de buena fe respecto de la denuncia y de que la información sea precisa y, en lo posible, identificación del usuario infractor; y, finalmente, la respectiva firma.

88. Véanse artículo 10:

Requisitos de las solicitudes de retiro o inhabilitación. Las solicitudes de retiro o inhabilitación de contenidos, que en virtud del artículo anterior realicen los titulares de derecho de autor o derechos conexos, o sus respectivos representantes, deberán como mínimo tener en cuenta los siguientes requisitos:

- a) Se remitan en forma electrónica o de otra forma escrita;
- b) Se incluya la identidad, domicilio, número telefónico, dirección de correo electrónico del titular de derecho de autor o conexos, o sus representantes respectivamente;
- c) El titular de los derechos o su representante deberá tener domicilio o residencia en Colombia y, en su caso, contar con poder suficiente para ser emplazado en juicio, en representación del titular;
- d) Se adjunte información razonablemente suficiente que permita al prestador del servicio identificar la obra o prestación protegida por el derecho de autor o los derechos conexos, que se alega está siendo usada sin la respectiva autorización;
- e) Se identifiquen los derechos supuestamente infringidos, con indicación precisa de la titularidad de estos y la modalidad de la infracción;
- f) Se adjunte la url o cualquier otra información razonablemente suficiente, que permita al prestador de servicio localizar el material supuestamente infractor que reside en un sistema o red controlada u operado por este o para este, el cual es reclamado de estar infringiendo o ser el objeto de una actividad infractora y el cual debe ser removido o su acceso debe ser inhabilitado;
- g) Realice el titular de derecho o su representante una declaración en la que exprese que cree de buena fe que el uso que se le está dando al material no cuenta con la autorización de dicho titular del derecho de autor o conexo, su representante, quien esté legitimado para otorgar dicha autorización o de la legislación;
- h) De ser posible, adjuntar información que contenga datos que permitan al prestador de servicios identificar al usuario proveedor del supuesto material infractor;
- i) Se efectúe una declaración en el sentido de que la información contenida en la solicitud de retiro o inhabilitación es precisa;
- j) Se firme por la persona que hace la solicitud de retiro o inhabilitación. A este efecto la firma transmitida como parte de una comunicación electrónica cumple con el requisito descrito.

Y Parágrafo:

El que a sabiendas, proporcione información falsa relativa a supuestas infracciones a los derechos reconocidos en esta ley, deberá indemnizar los daños causados a cualquier parte interesada, si estos daños son resultado de acciones que el prestador de servicios de red tome con base a dicha información.

Enviada esa comunicación, y tomadas las medidas por el respectivo proveedor de servicios en orden de retirar, inhabilitar o bloquear los contenidos así denunciados, sin una orden ni una participación judicial en tal sentido, el proveedor queda exento de responsabilidad⁸⁹, siempre que informe oportunamente de tal medida al supuesto infractor⁹⁰.

Por cierto, esto es solamente una forma de distribuir responsabilidad, que en ningún caso obsta a que medidas similares sean solicitadas, ya con carácter de medida cautelar⁹¹ o de forma definitiva⁹², ante un juez,

89. Véanse artículo 9:

Procedimiento de detección y retiro de contenidos. Si los prestadores de servicio, cumpliendo los demás requisitos establecidos en los artículos 6, 7 y 8, actuando de buena fe, retiran o inhabilitan el acceso al material basado en una infracción reclamada o aparente, estarán exentos de responsabilidad por cualquier reclamo resultante, a condición que, en relación con el material que resida en su sistema o red, tome prontamente los pasos razonables para informar del retiro o inhabilitación al supuesto infractor que pone el material a disposición en su sistema o red.

Y Parágrafo:

Si el supuesto infractor realiza una solicitud de restablecimiento del material retirado o inhabilitado y está sujeto a la jurisdicción en una demanda por infracción, el prestador de servicios debe restablecer el material, a menos que la persona que realizó la solicitud de retiro o inhabilitación original procure una orden judicial dentro de un plazo razonable.

90. Véase artículo 11:

Obligación de informar el retiro o inhabilitación al supuesto infractor. Una vez recibida la solicitud de retiro y verificado el cumplimiento de los requisitos establecidos en el artículo anterior, los prestadores de servicios de Internet, dentro de un plazo de 72 horas contadas desde la recepción de la reclamación, deberán informar por escrito a sus usuarios de las solicitudes de retiro basadas en supuestas infracciones, acompañando los antecedentes proporcionados por el titular del derecho o su representante.

91. Véase propuesto artículo 245 de la Ley 23 de 1982 (Medidas Cautelares), párrafo segundo:

Así mismo, para las infracciones al derecho de autor o los derechos conexos cometidas en o por medio de redes o sistemas controlados u operados por o para prestadores de servicios, los titulares podrán pedir al juez del domicilio del prestador de servicios, aun sin ser el competente para conocer del juicio, como medida cautelar el retiro o inhabilitación del acceso al material infractor que sea claramente identificado por el solicitante (y/o la terminación de cuentas determinadas de infractores reincidentes de dicho prestador de servicio), que sean claramente identificadas por el solicitante, y cuyo titular esté usando el sistema o red para realizar una actividad infractora al derecho de autor y conexos." Así como cualquier otra medida de carácter provisional encaminada a proteger el derecho, conservar las pruebas y evitar que se produzcan otros daños como consecuencia de la presunta infracción.

No obstante, tratándose de prestadores de servicios de transmisión de datos, enrutamiento o suministro de conexiones, el juez competente solo podrá disponer como medida cautelar la adopción de medidas razonables para bloquear el acceso a un determinado

procediendo solamente en esta oportunidad judicial de defensa de derechos la posibilidad de solicitar medidas que permitan identificar al supuesto infractor⁹³.

Sin perjuicio de estas últimas vías de acción para retirar definitivamente un contenido infractor desde la red, la exención de responsabilidad ante un sistema de notificación privada trae consigo, necesariamente, la consecuencia de poner a cargo del proveedor de servicios de Internet la decisión sobre la permanencia en línea de un contenido. Por supuesto, el respectivo proveedor tendrá que actuar, en teoría, como un juez que dilucide la pertinencia y procedencia de la denuncia de contenido infractor, pero, también, como una parte interesada, toda vez que el retiro de contenido lo libera de eventual responsabilidad, pero el no retiro no tiene la misma consecuencia favorable. En consecuencia, el proveedor de servicios se verá en situación de afectación

contenido infractor que sea claramente identificado por el solicitante y que no implique el bloqueo de otros contenidos legítimos. Para estos efectos, la solicitud de medidas cautelares deberá indicar claramente:

1. Los derechos supuestamente infringidos, con indicación precisa de la titularidad de estos y la modalidad de la infracción;
2. El material infractor,
3. La localización del material infractor en las redes o sistemas del prestador de servicios respectivos.

92. Véase artículo 16:

Orden definitiva de retiro o inhabilitación del acceso al material infractor y/o la terminación de cuentas. Las medidas de que trata el artículo 13 tendrán carácter definitivo cuando así lo ordene el juez competente mediante sentencia. Estas medidas se dictarán con la debida consideración de:

- 1) la carga relativa para el prestador de servicios, para los usuarios y para los suscriptores;
- 2) la proporcionalidad con el daño inferido al titular del derecho;
- 3) a factibilidad técnica y eficacia de la medida; y,
- 4) la existencia de otras medidas menos gravosas para asegurar el cese de la infracción y el restablecimiento del derecho que se reclama.

Estas medidas se aplicarán de manera estricta y limitada al acceso de servicios de comunicación al público en línea. Cuando estos servicios sean comprados de acuerdos a ofertas comerciales compuestas, incluyendo otro tipo de servicios tales como servicios de telefonía o de televisión, estas medidas no se aplicarán a estos últimos.

93. Véase artículo 15:

Entrega de información sobre supuestos infractores. A requerimiento de los titulares de derechos que hayan solicitado una medida cautelar o hayan interpuesto demanda para obtener orden definitiva de retiro o inhabilitación del acceso al material infractor y/o la terminación de cuentas, el juez competente podrá ordenar la entrega de la información que permita identificar al supuesto infractor por el prestador de servicios respectivo, incluida la información confidencial. El tratamiento de los datos así obtenidos se sujetará a la protección y reserva de datos personales conforme con la ley.

de derechos fundamentales de los usuarios que han provisto el contenido, de forma extrajudicial, ante una simple denuncia y sin determinación del ilícito por los cuerpos institucionales llamados a tal efecto.

La participación judicial, en caso de que la notificación no sea pertinente, solamente se produce ante el reclamo por la medida ya adoptada, a través de una solicitud de restablecimiento⁹⁴, sujeta a formalidades en principio no menos gravosas que aquellas utilizadas para la solicitud de bajada, pero que para un usuario podrían resultar innecesariamente engorrosas. En una circunstancia de esas características, el proveedor de servicios, velando por sus propios intereses, preferirá un acto de censura, que, incluso considerando las posibilidades de reclamo, parece ser menos dispendioso que mantener el contenido en línea.

Tras la polémica suscitada por el proyecto y el amplio debate posterior, fue finalmente archivado (es decir, suspendida de forma indefinida su tramitación), a principios de noviembre de 2011⁹⁵.

94. Véase artículo 12:

Elementos de la solicitud de restablecimiento. Para entender como efectiva la solicitud de restablecimiento del material retirado o inhabilitado, mencionada en el párrafo del artículo 9, esta debe constar por escrito o mediante comunicación electrónica que incluya los siguientes aspectos:

- a) la identidad, domicilio, número telefónico, dirección de correo electrónico por parte del supuesto infractor;
- b) identificación del material que ha sido removido y cuyo acceso ha sido inhabilitado;
- c) la ubicación del sitio en el cual se encontraba el material antes de ser removido o antes que su acceso haya sido inhabilitado;
- d) una declaración bajo la gravedad del juramento en la que el supuesto infractor manifiesta que provee el material y expresa que cree de buena fe que fue removido o inhabilitado como consecuencia de un error o de una indebida identificación del material;
- e) una declaración en la cual el supuesto infractor acceda a estar sujeto a ordenes impuestas por cualquier autoridad judicial de su domicilio, o si el domicilio se encuentra fuera del territorio de la parte, cualquier otra autoridad judicial con jurisdicción en cualquier lugar del territorio de la parte en donde el prestador del servicio pueda ser encontrado, y en la cual una demanda por la alegada infracción al derecho de autor o derechos conexos pueda ser interpuesta;
- f) una declaración en la cual se acepte ser notificado de cualquiera de estas demandas; y
- g) la firma de la persona que realiza la solicitud de restablecimiento del material retirado o inhabilitado. A este efecto la firma transmitida como parte de una comunicación electrónica cumple con el requisito descrito.

95. «Congreso y Gobierno acuerdan archivo de “Ley Lleras”», en *Semana.com*, del 20 de octubre de 2011, disponible [en línea] en: <<http://www.semana.com/nacion/congreso-gobierno-acuerdan-archivo-ley-lleras/166045-3.aspx>>. [Nota del editor: consultada el 5/11/11.]

II.C.IV.b. LA ARGENTINA. Su propia polémica ha vivido la República Argentina a propósito del establecimiento, a nivel federal, de reglas no del todo distintas de las propuestas por Colombia, a través de un proyecto presentado solo días antes de la presentación de la «Ley Lleras».

A fines de marzo de 2011, se presentó ante el Congreso Nacional de la Argentina el proyecto sobre Régimen para proveedores del servicio de Internet, también conocido como «Ley Pinedo»⁹⁶. La aspiración del ámbito de cobertura de esta norma, sin embargo, es vastamente superior, pues no se restringe necesariamente a la propiedad intelectual, como veremos. Tal como en otros proyectos, y como los estudios doctrinarios, el proyecto dedica parte de su articulado a la definición de tales prestadores de servicio en su primer artículo⁹⁷, englobando en

96. Proyecto: Trámite parlamentario 208 (del 22 de febrero de 2011), firmado por Federico Pinedo, Diputado Nacional por Buenos Aires.

97. Véase artículo 1°:

A los efectos de la presente ley, los términos que a continuación se indican tendrán el significado previsto en el presente artículo:

- 1) Proveedores de servicios de Internet: incluye a los proveedores de acceso a Internet, proveedores de facilidades de interconexión, proveedores de alojamiento, proveedores de contenido o de información y proveedores de servicios.
- 2) Proveedores de acceso a Internet: son quienes por medio de diferentes medios técnicos, prestan el servicio de conexión a la red Internet.
- 3) Proveedores de facilidades de interconexión: son quienes aportan los medios estructurales para la circulación de la información en Internet, independientemente de las características de la conexión o de la circulación de la información en la red.
- 4) Proveedores de servicios: los motores de búsqueda y todos aquellos que ofrecen servicios y/o programas que utilizan Internet como medio necesario para prestar dichos servicios o utilizar dichas aplicaciones o programas.
- 5) Proveedores de contenido o de información: son todos los que suministran contenidos a Internet, independientemente del formato utilizado para suministrar dichos contenidos e independientemente de si los suministraran en sitios webs propios o provistos por terceros.
- 6) Motores de búsqueda: quienes ofrecen en un sitio web el servicio de buscar en internet enlaces a otros sitios webs en los que se encuentre o se encontraba el o los términos ingresados por el usuario.
- 7) Proveedores de alojamiento: quienes ofrecen los medios técnicos para que los desarrolladores y/o titulares de sitios web hagan disponible el contenido de los mismos a todos los usuarios de Internet, almacenando o no los contenidos de los sitios en servidores de su propiedad.
- 8) Contenido específico: todo archivo de cualquier naturaleza o formato al que se pueda acceder a través de Internet.

la aplicación de la ley a aquellos que prestan acceso, interconexión, alojamiento, servicios y contenido o información.

Comienza la Ley Pinedo haciendo responsables a los proveedores de almacenamiento automático de contenido de terceros, exclusivamente ante la existencia de conocimiento efectivo⁹⁸. Respecto de aquellos proveedores de contenido, de alojamiento y de servicios que incluyan el enlace a contenidos infractores, el proyecto establece la responsabilidad de tales prestadores, otra vez, ante el conocimiento efectivo⁹⁹. En cuanto a los proveedores de transmisión, solamente los hace responsables cuando ellos la originen, o bien, cuando modifiquen o seleccionen el contenido o sus destinatarios¹⁰⁰.

Las medidas en orden al bloqueo o retiro de contenidos son ordenadas judicialmente, en proceso sumarísimo, que puede derivar, incluso, en la adopción *ex parte* de tales medidas de forma provisional y pueden no solamente ser promovidas por titulares de derechos, sino por cualquier persona, ante contenido que lesione derechos o garantías reconocidos en la Constitución o las leyes. Las medidas tendientes a la identificación de esa persona como afectada o titular de un derecho alegado y potencialmente vulnerado, es una facultad privativa del

98. Artículo 2º: «Los proveedores de servicios de Internet serán responsables por el almacenamiento automático de contenidos generados por terceros exclusivamente cuando tuvieren conocimiento efectivo, en los términos de esta ley, de que los contenidos almacenados violan normas legales o derechos de terceros».

99. Véase artículo 6º:

Los proveedores de alojamiento, los proveedores de contenidos y los proveedores de servicios que ofrezcan enlaces a otros sitios webs u ofrezcan información provista por terceros, serán responsables respecto de la información provista por los terceros exclusivamente en los casos en que tengan conocimiento efectivo de que la información almacenada viola normas legales o derechos de terceros.

100. Véase artículo 5º:

Los proveedores de servicios de Internet serán responsables por la transmisión o retransmisión de contenidos generados por terceros exclusivamente cuando los propios proveedores de servicios de Internet sean quienes originen dicha transmisión o retransmisión, o cuando modifiquen o seleccionen los contenidos y/o seleccionen a los destinatarios de la información transmitida o retransmitida.

Se entenderá por modificación a la variación concreta, parcial o total, del contenido, pero no a la variación estrictamente técnica del formato de los contenidos transmitidos o retransmitidos.

juez¹⁰¹. A su vez, queda bajo responsabilidad del Ministerio Público la solicitud de tales medidas en los casos de afectación de derechos de carácter sexual de menores de edad¹⁰².

El conocimiento efectivo del que se trata en esta ley está condicionado a la notificación de una de las medidas antes mencionadas¹⁰³. Claro está, esto involucra participación judicial en la materia. Pero no es ese el mayor problema identificable en el proyecto argentino, sino la ambigüedad de los términos usados y los eventuales vacíos de aplicación. Si cualquier persona puede solicitar el retiro o bloqueo de un contenido, bajo condiciones que ni siquiera la propia ley del proyecto establece, pero pudiendo dictarse la medida sin audiencia del proveedor respectivo bajo una ponderación de

101. Véase artículo 3°:

Toda persona, de existencia visible o ideal, podrá promover una medida ante el juez con competencia en su domicilio con el objeto de solicitar judicialmente que se elimine y/o se restrinja y/o se bloquee el acceso a uno o más contenidos específicos -sea en forma de texto, sonido, imagen o cualquier otra información o representación- que lesionen derechos o garantías reconocidos por la Constitución Nacional, un tratado o una ley de la República Argentina.

En el caso, el juez podrá ordenar las medidas requeridas en forma provisional sin haber oído a la otra parte, en particular cuando haya probabilidad de que cualquier retraso cause daño irreparable al titular de los derechos, o cuando haya un riesgo demostrable de destrucción de pruebas. El juez podrá exigir al demandante que presente las pruebas de que razonablemente disponga, con el fin de establecer con un grado suficiente de certidumbre que el demandante es el titular del derecho alegado y que ese derecho es objeto o va a ser objeto inminentemente de violación, y ordenar que preste caución juratoria o aporte una fianza, o garantía equivalente, que sea suficiente para proteger al demandado y evitar abusos.

En todo aquello no previsto especialmente por esta ley, la medida establecida en el presente artículo tramitará de conformidad con las normas del proceso previsto en los artículos 232 y 321 inciso segundo del Código Procesal Civil y Comercial de la Nación y normas análogas de las legislaciones procesales provinciales.

102. Véase artículo 4°: «Será responsabilidad primaria del Ministerio Público solicitar las medidas indicadas en el artículo tercero de la presente ley ante contenidos específicos en los que se pueda observar la representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales».

103. Véase artículo 7°: «A los fines de la aplicación de la presente ley, se entenderá que los Proveedores de Servicios de Internet tienen conocimiento efectivo de que determinados contenidos violan normas legales o derechos de terceros desde el momento en que sean notificados del dictado de alguna de las medidas previstas en el artículo 3° de esta ley o de otra resolución judicial que así lo establezca».

gravidad de la que el proyecto no se encarga, se vuelve extremadamente fácil buscar esa inhabilitación de contenidos. Es allí donde las deficiencias se discuten de manera más enérgica. Derechos fundamentales no pueden ser dejados a una acción tan ambigua en sus términos ni tan vaga en sus requisitos, pues si la propia libertad de expresión carece de un margen de garantías formales que permitan su desarrollo en línea, la búsqueda de eximirse de responsabilidad estará, otra vez, más condicionada por el interés del proveedor de servicios que, en atención a los derechos y las libertades de los usuarios, generan y proveen contenidos.

II.C.IV.c. BRASIL. A nivel de contingencia, el caso brasileño es el que resulta más tumultuoso y, por la misma razón, el más difícil de asir actualmente. Durante la presidencia de Luiz Inácio Lula da Silva, a fines de 2009, el Ministerio de Justicia convocó a la ciudadanía a participar de la formación de un Marco Civil de Internet¹⁰⁴, coordinado entre el Ministerio y el Centro de Tecnología y Sociedad de la Fundación Getulio Vargas, que proveyera al país de una nueva regulación sobre los distintos puntos de vinculación entre los derechos fundamentales, el interés público, los intereses de las industrias de contenidos y de telecomunicaciones y el entorno digital. El llamado recogía años de discusión académica y social en torno a la necesidad de regulación en este sentido.

Tras varios meses de debate a lo largo de las diversas etapas de discusión abiertas, a mediados de 2010, se llegó a un texto que parecía incluir de manera suficiente todas las demandas ciudadanas de forma más o menos equilibrada. En dicho texto, en la forma final adquirida, se estableció de manera expresa que un proveedor de conexión a Internet no sería responsable por los contenidos provistos por terceros¹⁰⁵. Solamente cabría responsabilizar al proveedor de servicio de Internet (considerándose como tales también a quienes tienen «poder de moderación» sobre contenido ajeno¹⁰⁶) allí donde

104. Sobre el particular, véase el sitio de la discusión [en línea], en: <<http://culturadigital.br/marcocivil/>>. [Nota del editor: consultada el 5/11/11.]

105. Véase artículo 19: «O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros».

106. Véase artículo 23: «Os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de serviços de Internet para efeitos do disposto nesta Seção».

este fuera notificado judicialmente de una orden de retiro o bloqueo, que cumpliera con los requisitos legales en cuanto a la identificación del titular de derechos, las obras, los derechos vulnerados, la forma de infracción y la ubicación del material infractor¹⁰⁷, y no le diera cumplimiento a dicha orden¹⁰⁸. Al ejecutarla, no obstante, el proveedor debía informar al usuario (si era identificable)¹⁰⁹.

El proceso de discusión en el Marco Civil corría junto al Foro de Consulta Pública de la Ley de Reforma de Derechos de Autor, ya centrado no en Internet en general, sino en los derechos de propiedad intelectual y su actual regulación en Brasil, también con alta participación ciudadana. Pero todos estos esfuerzos parecieron ser en vano cuando, el 1º de enero de 2011, el nuevo gobierno de Dilma Rouseff, a través de la ministra de Cultura, doña Ana de Hollanda, comprometió la revisión del hasta entonces ya discutido proceso de reforma a las leyes relativas a contenidos en línea. Después de amargas polémicas, el Marco Civil continúa esperando ser ingresado para su discusión en el Congreso, mientras que un proceso nuevo sobre reforma a la Ley de Derechos de Autor de 1998 esperaba ser convertido en proyecto en el mes de julio de 2011.

Este último punto es especialmente relevante. Sin hacerse cargo del proyecto logrado a través del Marco Civil y cambiando las condiciones de consulta para reformar la Ley de Derechos de Autor, la nueva autoridad ministerial estableció el nuevo proceso de consulta, a partir de un nuevo anteproyecto de reforma, posterior a las consultas públicas

107. Véase artículo 21:

A intimação de que trata o art. 20 deverá conter, sob pena de invalidade:

- I- identificação da parte que solicitou a remoção do conteúdo, incluindo seu nome completo, seus números de registro civil e fiscal e dados atuais para contato;
- II- identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material;
- III- descrição da relação existente entre a parte solicitante e o conteúdo apontado como infringente;
- IV- justificativa jurídica para a remoção.

108. Véase artículo 20: «O provedor de serviço de internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após intimado para cumprir ordem judicial a respeito, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente».

109. Véase artículo 22: «Ao tornar indisponível o acesso ao conteúdo, caberá ao provedor do serviço informar o fato ao usuário responsável pela publicação, comunicando-lhe o teor da intimação, nos casos em que o usuário responsável seja identificável».

llevadas adelante durante 2010¹¹⁰. Junto a otras reformas, mayormente tendientes a una mayor protección de derechos de autor, se introducía en la Ley de Derechos de Autor un nuevo y extenso artículo, el 105-A¹¹¹,

110. Véase *Anteproyecto de Lei*: «Altera e acresce dispositivos à Lei no 9610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais, e dá outras providências».

111. Véase artículo 105-A:

Os responsáveis pela hospedagem de conteúdos na Internet poderão ser responsabilizados solidariamente, nos termos do Artigo 105, por danos decorrentes da colocação à disposição do público de obras e fonogramas por terceiros, sem autorização de seus titulares, se notificados pelo titular ofendido e não tomarem as providências para, no âmbito do seu serviço e dentro de prazo razoável, tornar indisponível o conteúdo apontado como infringente.

§ 1º. Os responsáveis pela hospedagem de conteúdos na Internet devem oferecer de forma ostensiva ao menos um canal eletrônico dedicado ao recebimento de notificações e contranotificações, sendo facultada a criação de mecanismo automatizado para atender aos procedimentos dispostos nesta Seção.

§ 2º. A notificação de que trata o caput deste artigo deverá conter, sob pena de invalidade: I- identificação do notificante, incluindo seu nome completo, seus números de registro civil e fiscal e dados atuais para contato;

II- data e hora de envio;

III- identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material pelo notificado;

IV- descrição da relação entre o notificante e o conteúdo apontado como infringente; e VI- justificativa jurídica para a remoção.

§ 3º. Ao tornar indisponível o acesso ao conteúdo, caberá aos responsáveis pela hospedagem de conteúdos na Internet informar o fato ao responsável pela colocação à disposição do público, comunicando-lhe o teor da notificação de remoção e fixando prazo razoável para a eliminação definitiva do conteúdo infringente.

§ 4º. Caso o responsável pelo conteúdo infringente não seja identificável ou não possa ser localizado, e desde que presentes os requisitos de validade da notificação, cabe aos responsáveis pela hospedagem de conteúdos na Internet manter o bloqueio.

§ 5º. É facultado ao responsável pela colocação à disposição do público, observados os requisitos do § 2º, contranotificar os responsáveis pela hospedagem de conteúdos na Internet, requerendo a manutenção do conteúdo e assumindo a responsabilidade exclusiva pelos eventuais danos causados a terceiros, caso em que caberá aos responsáveis pela hospedagem de conteúdos na Internet o dever de restabelecer o acesso ao conteúdo indisponibilizado e informar ao notificante o restabelecimento.

§ 6º. Qualquer outra pessoa interessada, física ou jurídica, observados os requisitos do § 2º, poderá contranotificar os responsáveis pela hospedagem de conteúdos na Internet, assumindo a responsabilidade pela manutenção do conteúdo.

§ 7º. Tanto o notificante quanto o contranotificante respondem, nos termos da lei, por informações falsas, errôneas e pelo abuso ou má-fé.

§ 8º. Os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos responsáveis pela hospedagem de conteúdos na Internet para efeitos do disposto neste artigo.

destinado a regular la responsabilidad de los prestadores de servicios de Internet, particularmente, de los prestadores de alojamiento de contenidos. El anteproyecto los hace solidariamente responsables por los daños producidos por la puesta a disposición por parte de terceros y el no retiro de estos una vez notificados a tal fin. Pero sobre estas materias, la polémica no es gratuita. El articulado propuesto exige una dirección donde hacer llegar las notificaciones (§ 1º); exige requisitos formales para esa notificación (§ 2); exige la información al tercero proveedor del contenido infractor, fijando un «plazo razonable» para su remoción definitiva (§ 3); obliga al proveedor de *hosting* a mantener el bloqueo si ese proveedor de contenido no es ubicable (§ 4). Este anteproyecto, además, permite al proveedor de contenidos realizar una contranotificación, manteniendo así en línea el contenido, pero asumiendo la total responsabilidad por los eventuales daños (§ 5), como también permite que cualquier otro interesado haga esa contranotificación asumiendo igual responsabilidad (§ 6). Al igual que en otras propuestas, se fija responsabilidad por la entrega de informaciones falsas (§ 7), y tal como en el proyecto del Marco Civil, los usuarios con poderes de moderación se hacen equiparables a los responsables del servicio de alojamiento (§ 8).

Por cierto, este somero examen aborda solamente el anteproyecto en su formulación actual. Si bien en los detalles no dista significativamente de otros proyectos, destacando por no exigir retiro inmediato y permitiendo expresamente la contranotificación, también es cierto que fija todo un mecanismo que opera sin especial intervención judicial; es más, se entiende que cumplidos los requisitos formales fijados por el proyecto y eventual ley, una comunicación privada es más que suficiente notificación para que haga operar la responsabilidad del proveedor de alojamiento, o bien su exención si existe retiro de material. Una vez más, queda a cargo del proveedor del respectivo servicio de Internet (y de sus moderadores) la determinación de la responsabilidad, no en atención a la lesión de leyes o de derechos ajenos, sino de la posibilidad de verse personalmente sujetos a responsabilidad por actos ajenos, presuntamente infractores de derechos de propiedad intelectual. La solución impulsada por las nuevas autoridades aparece, necesariamente, como una forma de «cooperación» privada que poco parece resguardar los derechos de los usuarios que aportan contenido a la red. Cuál será el proyecto privilegiado a nivel de parlamento y cuál será el resultado de esa discusión quedan todavía a la expectativa.

II.D. Hacia una delimitación de la responsabilidad de los proveedores de Internet

Como se ha visto, muchas formas existen para establecer regímenes de responsabilidad que afecten a proveedores de servicios de conexión y de alojamiento de Internet, pero la exploración de cualesquiera de ellas a nivel legal estará sujeta a incontables debates y discusiones sobre su procedencia, en resguardo de los distintos intereses en juego. Si bien la intervención judicial previa pareciera ser, en cualquier caso, deseable, no es menos cierto que dentro de la propia cultura jurídica latinoamericana, como también en la comparada, existen movimientos que propenden a una «cooperación» entre los interesados¹¹², que conlleve una salida extrajudicial rápida, pero sancionada por el derecho¹¹³ y que muchas veces obvia la intervención jurisdiccional.

No obstante, ideas algo más razonables en la aplicación de estas medidas parecen permear a la doctrina¹¹⁴ y a las decisiones judiciales más recientes. En tal sentido, parte de la doctrina se inclina por no regular especialmente a los proveedores de los distintos servicios de Internet, sino dejar que la aplicación de normas civiles sobre responsabilidad civil sean las que

112. Además de los ejemplos ya vistos, puede revisarse, sin ir más lejos, en el Informe 301 de la oficina del United States Trade Representative, la continua mención a la búsqueda del establecimiento de mecanismos legales de “cooperación” para evitar los ilícitos vinculados a los derechos de propiedad intelectual de forma rápida y efectiva.

113. Véase *supra* nota 39:

Y que al considerar si esos proveedores de servicios deben ser tratados como editores electrónicos y, por tanto, responsables de la transmisión de contenidos no autorizados (ilícitos) o bien como los “carteros de Internet”, es decir, exentos de toda responsabilidad, se debe tener en cuenta que aunque dichos proveedores no provean los contenidos ni tomen parte en la decisión de difundir las obras y prestaciones, sin embargo participan directamente en la difusión de esos contenidos y –salvo situaciones muy particulares– están obligados a responder por el carácter fraudulento de estos, aún cuando se trate de actos de intermediación en los cuales el prestatario del servicio es un mero transmisor o conductor de los mensajes, pero el autor o el titular de derechos conexos perjudicado hubiese advertido al proveedor de servicios en línea sobre el carácter ilícito del contenido transmitido sin autorización y lo intimase a rechazar el alojamiento en su servidor y la circulación de esa información, y el operador -advertido e intimidado- no la eliminara de su servidor y su circulación en la red, no podría excusarse en la ignorancia y la buena fe.

114. Santos, Fabio Lima dos, «Responsabilidade civil dos provedores de conteúdo de Internet», en *Dos blogs aos jornais online*, Jus Navigandi, Teresina, año 16, 2783, 13 de febrero de 2011, disponible [en línea] en: <<http://jus.uol.com.br/revista/texto/18489/responsabilidade-civil-dos-provedores-de-conteudo-de-internet>>. [Nota del editor: consultada el 5/11/11.]

diluciden, existiendo dolo o culpa, la existencia de una obligación de reparar el daño causado, aplicando reglas generales¹¹⁵.

De alguna manera no deja de ser razonable pensar que la proliferación de sistemas particulares de responsabilidad civil puede provocar más problemas que los que pretende resolver. El establecimiento de un nuevo régimen de responsabilidad que establezca deberes a los que detentan la capacidad técnica de poner alto a la circulación de contenidos ilícitos en Internet, parece innecesario si el sistema es capaz de entregar soluciones sobre la base de principios generales, que solamente deben trasladarse a las nuevas realidades. Sin embargo, la alta complejización del escenario obliga a adecuar los criterios con que esa determinación de responsabilidad se efectúa. Atendidos los disensos a nivel de discusión académica y de organizaciones sociales, las soluciones normativas se vuelven de pronto necesarias: no parece haber buenas razones para decidir abstractamente los casos futuros a partir de discusiones complejas y que distan de estar cerca de un consenso.

Pero lo que en ningún caso podría ocurrir, estimamos, es que el control sobre los contenidos que viajan a través de las redes digitales quede en manos de los proveedores de servicio de Internet, sean ellos prestadores de acceso, conexión o prestadores de contenido que no controlen *a priori* el material que aparezca como provisto por ellos. Esto por varias razones, que van desde aquellas vinculadas al funcionamiento de la red y a las condiciones de no exclusión necesarias para la circulación de contenido desde la creación de Internet, que se suelen agrupar normativamente bajo la discutida regulación de neutralidad de la red, hasta por razones vinculadas con el ejercicio de derechos fundamentales en el entorno en línea, particularmente por las posibilidades de control que tendrían, en este caso, privados, respecto del ejercicio de la libertad de expresión en Internet.

Un sistema de responsabilidad para prestadores de los distintos servicios de Internet, sea este establecido de forma legal o bien como una elaboración doctrinaria, deberá, en primer lugar, desligarse de considerar a los proveedores de los servicios como sujetos a responsabilidad estricta, a fin de evitar que ellos se conviertan en una suerte de policías del contenido que circula a través de sus redes. Un modelo más adecuado sobre responsabilidad civil

115. A esta misma solución arriba uno de los más completos estudios sobre el tema en la realidad brasileña, véase Leonardi, Marcel, *Responsabilidade Civil dos Provedores de Serviços de Internet*, San Pablo, Juarez de Oliveira, 2005.

para los prestadores de servicios, adoptado en atención a las dificultades y consideraciones ya estudiadas, debiera descansar necesariamente en principios largamente aceptados sobre responsabilidad allí donde ha existido intención o negligencia inexcusable por parte del agente cuya responsabilidad se exige.

En segundo lugar, y dadas las complicaciones enfrentadas por los aparatos judiciales cuando se han enfrentado a la problemática de la atribución de responsabilidad bajo las reglas de responsabilidad subjetiva, se hace necesario delimitar claramente a qué estará obligado un proveedor de servicios de Internet. Es decir, si vamos a incluir como factor de atribución de responsabilidad a la culpa o negligencia, es menester dilucidar cuáles son los deberes que podremos considerar como infringidos¹¹⁶. Con este fin, ayuda considerablemente la existencia de reglas generales, especialmente a través de leyes, que garanticen algunos de tales deberes. Sin perjuicio de su ausencia, entenderemos que un prestador de servicios deberá cumplir, por lo menos, con:

- a) la utilización de tecnologías apropiadas para los fines por ellos perseguidos, haciéndose responsables de los daños producidos por una mala mantención de su infraestructura física y lógica: un servicio defectuoso y dañino por descuido o dejación de quien lo mantiene no será conceptualmente muy distinto que la existencia de situaciones de riesgo creado ya conocidas en los sistemas legales estudiados;
- b) conocer y manejar los datos de sus usuarios, a fin de hacer posible su localización en situaciones específicas que así lo justifiquen, como lo es el combate al crimen bajo control judicial estricto;
- c) conservar, por un tiempo determinado, cierta información particular y determinada por ley de los usuarios y sus actividades en la red, sin que ello implique en modo alguno dar a conocer esa información. Esto es importantísimo en el ámbito de la persecución criminal, como también en la atribución de responsabilidad civil. Sin embargo, es todavía materia de discusión qué tan extenso debiera ser ese plazo¹¹⁷;

116. Seguimos parcialmente en este punto a Leonardi, *í.d.*, sin perjuicio de nuestras propias opiniones en la materia.

117. Mientras las reglas de responsabilidad civil suelen estar sujetas a plazos de prescripción de varios años, lo que justificaría una extensión similar para esa conservación de datos, surgen de inmediato reparos a la luz del derecho a la intimidad o privacidad y a la inviolabilidad o sigilo de las comunicaciones privadas, así como también la objeción tecnológica derivada de las dificultades de almacenamiento por tan largo tiempo y de la pérdida de idoneidad de los mismos datos para la identificación precisa de un usuario y posible infractor de ley.

- d) mantener en secreto los datos de sus usuarios. No solamente de sus clientes, sino de cualquiera persona que utilice sus servicios. Otra vez, solamente la intervención judicial, por motivos fundados, justificaría romper esta regla general y en caso alguno la mera actividad policial o de las instituciones llamadas a la persecución criminal;
- e) no monitorear los contenidos que atraviesen sus redes, por tratarse de comunicaciones privadas cuyo carácter secreto está protegido como derecho fundamental. La excepción vendría dada por la persecución penal, dentro de márgenes estrictos y establecidos obligatoriamente por ley; y
- f) no intervenir en las comunicaciones realizadas en la red. De aquí derivan múltiples deberes menores, entre ellos los que suelen ser englobados en la idea de la «neutralidad de la red»: no discriminar ni restringir en virtud de la clase de contenido, de los sitios accesibles, de las plataformas usadas, de los dispositivos conectados o de los modos de comunicación. Asimismo, no interferir, filtrar, censurar ni bloquear en modo alguno las comunicaciones de los usuarios, sino ante una orden judicial fundada.

Un deber adicional parece entrar sobre este punto¹¹⁸: el deber de informar sobre la comisión de actos ilícitos verificada por el prestador de servicios. La discusión sobre este punto suele centrarse en la capacidad técnica del prestador de servicios de Internet para conocer los ilícitos cometidos a través de sus servicios y en la protección de los intereses afectados a través de los actos ilícitos que pondría de cargo del tenedor de esa capacidad técnica el deber de informar a las autoridades. Disentimos. No creemos que la privacidad y la intimidad de las comunicaciones merezcan reserva solo en cuanto se haga un uso adecuado o lícito de los servicios, sino que cualquier acción sobre el uso de tales servicios necesariamente debe pasar por la existencia de una orden judicial fundada, en el entendido que cualquier regulación a este respecto debe también ser analizada y las políticas regulatorias decididas a la luz de las garantías establecidas en la Constitución.

Esta última idea resulta clave para entender la magnitud del problema. Si bien pareciera ser que no existe una tendencia a regular ni a resolver estos

118. Defendido, así, por Lipszyc, *supra* nota 39 y Leonardi, *supra* nota 110.

problemas a través de reglas de responsabilidad objetiva, sino más bien a través de una responsabilidad subjetiva bajo condiciones especialmente fijadas (como ocurre en el caso de la normativa internacional ya descrita y de la ley chilena), hay también una fuerte tendencia hacia la fijación de condiciones especiales de persecución que obligan a la antes mencionada «cooperación» entre afectados y proveedores de servicios de Internet. Pero exigir la información sobre actividad ilegal, sin consideraciones especiales sobre el nivel de control que ejerce el respectivo proveedor de servicios, pone a cargo de este inmediatamente deberes de vigilancia sobre actos ajenos y lo que parece más grave, deberes de denuncia o de control sobre situaciones cuya ilicitud podría ser solo aparente, como ocurre en muchos casos de supuesta violación de derechos de propiedad intelectual.

Es en razón de esta situación que existen los sistemas de «notificación y bajada» de contenidos o *notice and take-down*. En virtud de estos sistemas, los proveedores se eximen de responsabilidad en la medida en que retiren el material ilícito una vez que tengan conocimiento de su existencia y existe de forma disímil en la DMCA estadounidense y en la Directiva 2001/31/CE europea, ya mencionadas con anterioridad. La cooperación antes citada puede existir con dichos sistemas, en la medida que institucionalmente se respalde una notificación por vía privada como forma de establecer el conocimiento del ilícito que decantaría en responsabilidad en caso de no retirarse.

No es extraño pensar que en tales casos, la amenaza de abuso del sistema es enorme. Se trataría, por una parte, de un incentivo perverso a la solución de situaciones en las que se involucran derechos de carácter privado sin un control judicial que resguarde o trate de resguardar las libertades y derechos de quien realiza el acto supuestamente infractor. Esto lesiona el propio carácter del aparato judicial como mediador imparcial entre las pretensiones de distintos interesados o como –en su caso– garante de los derechos fundamentales de las víctimas de ilícitos, así como también de los derechos de los imputados o acusados de la comisión de esos injurios. Ese equilibrio de intereses carecería de un foro para hacerse valer. Se trataría, en rigor, de una forma de privatización de la Justicia aun sin un expreso consentimiento de quien ha procurado el ejercicio de sus derechos y libertades allí donde ello se produce de corriente hoy en día, es decir, Internet, quedando esos derechos en manos de entidades sin la preparación ni la legitimidad de disponer de ellos que, naturalmente, poseen los tribunales de justicia, a efectos de defender derechos e intereses, en cualquier caso, privados.

Por supuesto, ello amenaza esos mismos derechos y esas mismas libertades. Si el ilícito como tal, es calificado y sancionado entre privados, con exclusión

de quien lo ha efectuado, pero, con el respaldo de la institucionalidad que sí busca garantizar imparcialidad en otros ámbitos, el desincentivo a la propia expresión se vuelve palpable. Esto ocurre especialmente allí donde, sin intervención judicial alguna, puede hacerse al proveedor de servicios de Internet directamente como responsable. El supuesto es el siguiente: si hablamos de una empresa proveedora de servicios de Internet, que ve su propio patrimonio y su propio funcionamiento amenazados por la eventualidad de una demanda judicial que no tiene posibilidades de sortear con éxito, gracias a reglas especiales de responsabilidad ya instituidas, tomará de inmediato cualquier acción o medida tendiente a evitar esa responsabilidad. Dicha acción o medida, a efectos de evitar las consecuencias civiles ya expuestas va a suponer, en buena parte de los casos, la bajada de contenidos eventualmente ilícitos o no autorizados por la ley, sin que esa calificación haya sido realizada por los órganos jurisdiccionales. Además, este efecto se hace más grave cuando se toma en consideración que los actores que se verán involucrados primariamente, al menos en este procedimiento privado, serán entidades de gestión colectiva en defensa de los intereses de sus asociados contra empresas que realizan alguna de las actividades que la ley contempla como de «prestación de servicios», según lo anteriormente apuntado. Así, el usuario final, eventualmente infractor, se encuentra en una posición de negociación gravemente desmejorada cuando no existe un órgano jurisdiccional que vele por las medidas que se tomen a efectos de combatir el uso y tráfico ilegal de contenidos.

En síntesis, allí donde el proveedor de servicios sea el encargado de determinar la ilicitud de un contenido y las medidas que se deben adoptar sobre sí, ese proveedor no velará necesariamente por la protección de los derechos e intereses vulnerados, sino que velará por la no materialización de la amenaza de sanciones y de responsabilidad que se ciernen sobre él. Se trata, en rigor, de la decisión *más segura* a efectos de evitar conflictos judiciales y sanciones. Y nada obsta a que se abuse de ese sistema para reprimir y hacer retirar discurso crítico, actos vinculados al ejercicio de otras libertades o, incluso, actos autorizados directamente por ley, como en el caso de las excepciones al derecho de autor. De hecho, en el caso estadounidense, existe amplia literatura que apunta a los efectos perniciosos que tiene un sistema de notificación y bajada privado¹¹⁹. Dado que los actos

119. Véase Gr. <<http://www.chillingeffects.org>>. [Nota del editor: consultada el 5/11/11.]

que realizamos a través de Internet están protegidos por el derecho a la libertad de expresión, un marco jurídico débil para el adecuado ejercicio de esa misma libertad termina convirtiendo esa libertad en algo teórico cuando se trata del ejercicio en línea. Tomarse en serio la libertad de expresión en Internet, en este contexto, implica establecer condiciones legales mediante las cuales el ejercicio de actos de comunicación a través de medios digitales sea protegido ante evidente tensión promovida por una sobrerregulación de derechos de autor y la arremetida de olas regulatorias que apuntan a la protección de modelos de negocio sin tomar en consideración criterios de análisis *desde* los derechos fundamentales.

Se inclina en el mismo sentido el Informe del Relator Especial de la Organización de Naciones Unidas para la Libertad de Opinión y Expresión, Frank La Rue, quien en atención a la responsabilidad de los intermediarios como posible restricción a la libertad de expresión declara en su Informe anual, en términos inequívocos, que tales medidas de censura no debieran ser entregadas a instituciones privadas, y que nadie debiera estar sujeto a responsabilidad por contenido en Internet del que no son autores, y enfatiza, también, la necesidad de órdenes de carácter judicial o, al menos, independiente¹²⁰. Debemos agregar que, si tales medidas han de existir, el sistema debe asegurar la posibilidad de reclamo o defensa contra ellas. Hacemos nuestra su apreciación: hacer que los intermediarios sean responsables, menoscaba el goce del derecho a la libertad de opinión y expresión, pues lleva a una censura amplia, de autoprotección, desprovista de transparencia y de garantías legales de debido proceso¹²¹.

La misma posición fue demostrada recientemente por distintas relatorías para la libertad de expresión de organizaciones internacionales. El 1 de junio de 2011, el Relator Especial de ONU para la Libertad de Opinión y de Expresión, Frank La Rue; la Relatora Especial para la Libertad de

120. La Rue, Frank, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, ONU, mayo de 2011, p.20.

The Special Rapporteur emphasizes that censorship measures should never be delegated to private entities, and that intermediaries should not be held liable for refusing to take action that infringes individuals' human rights. Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences.

121. *Id.*

Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) de la Organización de Estados Americanos (OEA), Catalina Botero Marino; la Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la Libertad de los Medios de Comunicación, Dunja Mijatović; 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), Faith Pansy Tlakula; emitieron una declaración conjunta¹²², en que recordaron el importante rol de Internet como medio de expresión, relevando su crucial función y la necesidad de contar con normas que impidan acciones arbitrarias sobre la información y el contenido que viajan a través de la red. Reconocen, en definitiva, que el acceso a Internet, en la sociedad actual, es un derecho básico y digno de reconocimiento y protección, atendido su carácter de medio de comunicación cada vez más masivo y poniendo a cargo de los Estados la facilitación del acceso a la red y el establecimiento de reglas que protejan la neutralidad y la libertad.

En dicha declaración, los relatores fueron especialmente enfáticos en cuanto a la responsabilidad de los intermediarios en Internet, esto es, de los prestadores de los distintos servicios que componen la comunicación en la red, declarando¹²³:

- a) 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»).
- b) 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**

122. *Declaración conjunta sobre libertad de expresión e Internet*, cuyo texto puede ser consultado junto al comunicado oficial de prensa [en línea] en: <<http://cidh.org/relatoria/showarticle.asp?artID=848&IID=2>>. [Nota del editor: consultada el 5/11/11.]

123. *Íd.* [Nota del autor: el destacado es nuestro].

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).

III. Conclusiones y recomendaciones

De todas las leyes y regulaciones estudiadas, resulta evidente que los regímenes latinoamericanos se encuentran todavía lejos de poder hallar una respuesta comúnmente aceptada a la disyuntiva sobre la forma de hacer responsables a los intermediarios por los contenidos emitidos por los usuarios finales o, aun más, si es posible reconocer, determinar y delimitar esa responsabilidad. Es más, a nivel comparado tampoco es posible verificar criterios que sean aceptados y acogidos normativamente de manera amplia. La decisión política que supone la regulación de la responsabilidad de los intermediarios en Internet es aún motivo de debates. Lo anterior, tomando especialmente en cuenta las estrategias que se llevan a cabo a nivel comparado que, como hemos indicado anteriormente, han pasado a estar dominadas por los intereses de la agenda internacional del comercio, favoreciendo una regulación desequilibrada y que favorece medidas de control privado en detrimento de los adecuados equilibrios pensando en el interés público.

Entendiendo la necesidad de avanzar hacia el establecimiento de un régimen de responsabilidad para los proveedores de servicios de Internet en tanto intermediarios, el Informe del Relator Especial de la ONU propone un conjunto de pasos por seguir cuando se imponga una restricción como medida excepcional sobre contenido en línea que pueden servir como criterios orientadores de una regulación razonada y equilibrada¹²⁴:

- a) que sea establecido por ley, cuyo sentido sea claro y accesible por todos (principios de previsibilidad y transparencia);
- b) que persiga uno de los propósitos fijados en el artículo 19, párrafo 3, del Pacto Internacional sobre Derechos Civiles y Políticos, a saber:
 - (i) proteger los derechos o la reputación de otros; (ii) proteger la

124. Véase *supra* nota 115.

- seguridad nacional o el orden pública o la salud y la moral públicas (principio de legitimidad); y
- c) que demuestre ser el medio necesario y el menos restrictivo que se requiera para lograr el objetivo pretendido (principios de necesidad y proporcionalidad).

Cualquier forma de regulación, en tal sentido, debe siempre permitir la contrariedad, el control judicial y la formalidad a efectos de asegurar un nivel de certeza antes de tomar medidas que, en definitiva, no hacen sino acallar o impedir la circulación de información o de incontables formas de expresión. En definitiva, si han de resolverse cuestiones de esta naturaleza, no son criterios económicos sobre atribución eficiente de los costos de los daños los que han de prevalecer, sino consideraciones sobre principios y derechos fundamentales constitucionalmente reconocidos, que están más que nunca en situación de ser aprovechados y ejercidos, pero también más susceptibles que nunca al capricho ajeno. Un marco de respeto debe prescindir de incentivos a actividades que afecten a tales principios, por el bien de la democracia y del desarrollo de los derechos de los ciudadanos de la región.

Intermediarios y libertad de expresión: apuntes para una conversación

Hiram A. Meléndez Juarbe¹

I. Intermediarios y el riesgo de sobreprotección

Atrás quedan los días en que concebíamos el entorno digital interconectado como uno absolutamente excepcional, completamente inmune al alcance de los Gobiernos y del derecho². Hoy resulta incuestionable que nuestra actividad en Internet es regulada cotidianamente, pues, como cuestión práctica, existe el poder de estructurar ese entorno tecnológico mediante, entre otras cosas, el derecho³.

Y es que la red no existe en abstracto —depende de entidades intermediarias que hacen posible la comunicación y que están bajo la jurisdicción legal y el

1. Elaboré reflexiones similares en un escrito previo, preparado para el Seminario en Latinoamérica de Teoría Constitucional y Política (SELA), dictado en junio de 2011, titulado «Tecnopolítica y derechos de autor». Una versión anterior de este escrito fue presentada en el Taller sobre libertad de expresión e Internet llevado a cabo en la Universidad de Palermo, en septiembre de 2011, como comentario a «*Responsabilidad de los proveedores de servicios de Internet (ISPs) en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica*» capítulo 1 del presente libro.

2. Penney, Jonathon W., «Understanding the New Virtualist Paradigm», en *Journal of Internet Law*, 12, 8 (2009).

3. Lessig, Lawrence, *Code and Other Laws of Cyberspace; sine nomine et sine loco*, 1999.

alcance de Gobiernos que tendrán a su disposición mecanismos coercitivos convencionales para lograr sus objetivos—. La conducta en Internet es regulada cada vez más mediante *intermediarios de conexión*, como los Proveedores de Servicio de Internet; *intermediarios de información*, como los motores de búsqueda; e *intermediarios financieros*, como tarjetas de crédito y PayPal⁴, entre otros⁵.

El rol de los intermediarios en la regulación es vital en nuestros días. En la medida en que los Gobiernos persigan objetivos políticos (legítimos o no) en Internet, los blancos de ataque poco a poco dejarán de ser los individuos cuya actividad preocupa al Estado, para ser aquellas entidades que provean los medios tecnológicos para esa actividad. Después de todo, será más económico y sencillo dirigirse contra unas pocas entidades sujetas a la jurisdicción del Estado que contra miles de individuos en ocasiones difíciles de identificar o imposibles de alcanzar.

En este contexto, una de las formas más efectivas de regular por medio de intermediarios es sujetándolos a responsabilidad (civil o criminal) por los actos de sus clientes o usuarios. La idea de esta estrategia es lograr que estas entidades sientan en su bolsillo presión por el acto potencialmente ilegal de sus clientes y, de esta forma, utilicen sus recursos tecnológicos (así como la oportunidad y superior información que se da en virtud de la relación con sus clientes) para supervisar, castigar o delatar a los usuarios.

Y este no es un componente exclusivo del ambiente digital actual. La reglamentación por medio de terceros es una estrategia común, especialmente cuando se refiere a la expresión⁶. Exponer a los intermediarios a responsabilidad (y convertirlos en guardianes o porteros) para reclutar ayuda y hacer cumplir compromisos normativos, ocurre en situaciones en que imponer responsabilidad en un infractor directamente no disuadiría la mala conducta o resultaría costoso.

4. Véase, por ejemplo, Wolverson, Troy N.Y. *subpoenas PayPal over gambling*, 12 de julio de 2002: [en línea] <http://news.cnet.com/N.Y.-subpoenas-PayPal-over-gambling/2100-1017_3-943533.html>. [Nota del editor: consultada el 17/10/2011.]

5. Goldsmith, Jack y Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World; sine nomine et sine loco*, 2006.

6. Kreimer, Seth, «Censorship by Proxy- the First Amendment Internet Intermediaries and the Problem of the Weakest Link», en *U. Pa. L. Rev.*, 155 (2007), p. 11. Véanse, *NAACP v. Alabama* ex rel. Patterson, 357 U.S. 449 (1958) (donde se invalida el requerimiento gubernamental de listas del NAACP de Alabama); *New York Times v. Sullivan*, 376 US 254 (1964) y *Bantham Books v. Sullivan*, 372 U.S. 58 (1963).

Pero el riesgo principal con esa estrategia es la probabilidad de sobreprotección y el impacto de esta sobre valores vinculados con la libertad de expresión. En la medida en que los intermediarios y los usuarios tienen intereses divergentes, un intermediario no va a tener necesariamente en cuenta el valor expresivo que goza para el usuario la actividad objeto de reglamentación, sino que, racionalmente, va a maximizar su bienestar, buscando reducir el costo esperado de responsabilidad. El problema, en fin, es que al sopesar los costos privados de la responsabilidad frente a sus beneficios –dentro de la concepción racional que constituye su bienestar–, el intermediario no considerará los intereses individuales del usuario (o los intereses sociales de que el usuario realice actividad presumiblemente protegida por la libertad de expresión).

En este ensayo, examino el fenómeno de la reglamentación de intermediarios en el contexto de los derechos de autor, la pornografía infantil y los ataques a la honra, la intimidad y la dignidad (tales como la difamación), y el potencial impacto de esta reglamentación sobre la libertad de expresión. A tales fines, y en lugar de desarrollar prescripciones en torno a cómo resolver estos riesgos de sobreprotección detalladamente, esbozo algunos apuntes para definir la agenda de investigación –teórica y práctica–, de manera tal que podamos forjar estrategias de política pública sensible y dirigir, así, de manera estratégica los esfuerzos de la sociedad civil donde sea más efectivo. En fin, planteo algunos puntos de partida para continuar la conversación.

II. Contextos de libertad de expresión

El primer punto de partida para esta discusión es que cualquier alternativa de regulación deberá contar con mecanismos legales particulares para cada contexto expresivo. Es decir, debemos cuidarnos de soluciones universales aplicables a todo tipo de contexto.

Proteger los derechos de autor en línea, detener la pornografía infantil y proteger contra ataques abusivos a la honra y vida privada constituyen objetivos gubernamentales legítimos en América Latina. Asimismo, su regulación mediante intermediarios, si bien puede resultar importante, presenta los riesgos de sobreprotección antes mencionados. Y es por ello que debemos seleccionar mecanismos legales de regulación que mientras atiendan estas preocupaciones estatales, reduzcan al máximo estos riesgos nocivos contra la libertad de expresión. Sin embargo, cada

uno de estos objetivos gubernamentales presenta retos particulares en atención a los diversos intereses de expresión que están potencialmente afectados. Puesto que los riesgos de sobreprotección afectan valores de expresión distintos, los mecanismos de regulación serán probablemente diferentes para cada uno.

Así, las reglas de responsabilidad de intermediarios deben variar de acuerdo con el tipo de acto comunicativo que atendamos y, por ello, es necesaria una conceptualización sustantiva más precisa de los valores sociales presentes en estos entornos expresivos (qué tipo de difamación es tolerable; en qué circunstancias los derechos de autor deben ceder ante reclamos de libertad de expresión; etcétera). Todo esto tendrá como objeto que podamos recomendar cuáles son las medidas más razonables para atender los riesgos de la reglamentación por intermediarios. Sin embargo, debemos primero adentrarnos en terrenos escabrosos y definir los contornos de los valores de expresión que deseamos proteger, y en ese proceso, realizar juicios valorativos sobre problemas de difícil solución.

En este sentido, es necesario comprender qué diferencias existen entre los intereses expresivos de un usuario no autorizado de obras protegidas por derechos de autor y los intereses de quien se expresa sobre otra persona de una manera que, posiblemente, afecte el buen nombre y la honra de ese otro. ¿Son similares estos intereses? O visto del otro lado de la moneda, ¿es equivalente el daño alegado por un autor cuya obra se usa sin permiso al daño invocado por una persona que arguye ser difamada? Como segundo paso, si no son similares estos intereses expresivos (los del usuario no autorizado de obras y el difamador –o el pornógrafo–), entonces ¿serán necesarios distintos tipos de reglamentación de los intermediarios que facilitan estas conductas? ¿En qué medida serán diferentes? Investigación subsiguiente debe tomar estas preguntas como punto de partida de manera sistemática. Solo ofrezco unas sugerencias.

Claramente, los intereses de expresión son diferentes en cada caso y se enfrentan a intereses colectivos e individuales distintos.

Por un lado, la expresión que potencialmente afecte tanto la honra como la vida privada de alguien podría encontrar su límite en un interés por preservar las reglas de civismo que configuran condiciones de cohesión social, así como el respeto a la dignidad humana que, por igual, todos ostentamos. Por ejemplo, el régimen constitucional interamericano permite limitar la expresión difamatoria contra personas privadas, pero este hecho es más difícil cuando se trata de funcionarios públicos

(por el valor que se le impone a la participación en el debate público)⁷. En cualquier caso, no hay una regla mágica que pueda definir con precisión qué constituye un ataque abusivo contra la honra y la reputación de otro, aunque habrá razones poderosas para proteger la expresión en muchos casos (como, por ejemplo, cuando se refiere a figuras públicas). La falta de certeza en cuanto a qué distingue la expresión legítima de la que no produce en el intermediario el ya mencionado riesgo de sobreprotección; en particular, cuando las sanciones son altas, lo cual incide sobre su análisis de riesgo.

Del otro lado, el uso no autorizado de obras realizadas por otros (y protegidas por derechos de autor) no debe demonizarse catalogándolas como «robo» o «piratería»; este uso puede responder a intereses individuales y colectivos relacionados con la expresión política, social y artística. El uso no autorizado de obras puede ser parte de lo que Fisher llama «democracia semiótica»⁸ –la descentralización del poder para atribuir significado a elementos de nuestra cultura–. Estos usos se destacan hoy en el contexto de las tecnologías digitales, pues las condiciones materiales para la producción y manipulación de productos culturales permiten identificarnos y experimentar con ellos como participantes activos de estos procesos culturales, ya no como receptores de información pasivos⁹. Sin embargo, los derechos de autor balancean estos intereses expresivos con otros dos (individuales y colectivos): (a) los derechos de autor son justificados como moralmente merecidos a partir de la mezcla del trabajo de un autor con recursos comunes o a partir de la conexión personal entre el autor y su obra; y (b) tiene como objetivo maximizar el bienestar social brindando incentivos

7. *Kimel c/ Argentina*, sentencia del 2 de mayo de 2008, dictada por la Corte Interamericana de Derechos Humanos, párrafo 86:

Respecto al derecho a la honra, las expresiones concernientes a la idoneidad de una persona para el desempeño de un cargo público o a los actos realizados por funcionarios públicos en el desempeño de sus labores gozan de mayor protección, de manera tal que se propicie el debate democrático. La Corte ha señalado que en una sociedad democrática los funcionarios públicos están más expuestos al escrutinio y a la crítica del público. Este diferente umbral de protección se explica porque se han expuesto voluntariamente a un escrutinio más exigente. Sus actividades salen del dominio de la esfera privada para insertarse en la esfera del debate público.

8. Fisher III, William W., *Promises to Keep: Technology, Law and the Future of Entertainment*; Stanford, *sine nomine*, 2004, pp. 30-31.

9. Benkler, Yochai, «From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access», en *Fed. Comm. L. J.* 52 (2000), p. 561.

suficientes a productores de información mediante la privatización de recursos intelectuales (a la vez que se quiere limitar ese derecho para evitar que la obra sea subutilizada)¹⁰. De ahí que conjugar estos intereses resulte complejo, contextual e indeterminado. No basta con alegar que alguien tiene derecho de propiedad absoluto sobre una obra, si no se consideran los intereses de expresión que puedan verse afectados, pero tampoco basta decir que un individuo tiene derecho a todo tipo de uso de la obra sin autorización (ignorando los intereses sociales e individuales que justifican el monopolio). Así, necesitamos criterios normativos para ayudarnos a trazar estos balances; pautas que serán diferentes a las utilizadas en la protección de la honra (por ejemplo, normas pertinentes aquí son: la naturaleza comercial –o personal– del uso o si se trata de uso solo para consumo o si es productivo; criterios que nada tienen que ver con las otras instancias de expresión examinadas).

Finalmente, aunque los intereses de expresión sobre material sexualmente explícito pueden ser más controversiales, es muy difícil –si no, imposible– justificar la pornografía infantil. Lo que sí es complicado, en muchos casos, es deslindar lo que es pornografía infantil de lo que no lo es. Son evidentes los casos en que empleados de establecimientos de fotografía han reportado a las autoridades a personas que someten a revelado películas con fotos de sus propios hijos menores, en contextos habituales de la niñez, que aunque técnicamente podrían considerarse pornográficas, no fueron generadas con interés lascivo¹¹; y casos en los que modelos adultos aparentan ser menores de edad¹². En estos casos, debemos examinar los intereses de expresión subyacentes a la pornografía no-infantil –intereses que podrían estar relacionados con la autonomía individual y el desarrollo de la personalidad–.

Así, pues, cada uno de los entornos expresivos refleja problemas internos (y diversos balances de intereses) y genera ambigüedad en torno a determinar cuál es exactamente la conducta por evitar. Precisamente esta vaguedad (en algunos casos más que en otros) es un factor importante para el

10. Meléndez Juarbe, Hiram, *Tecnopolítica y Derechos de Autor*: [en línea] <http://www.law.yale.edu/documents/pdf/sela/sela11_Melendez_pv_Sp_20110802.pdf>. [Nota del editor: consultada el 17/10/2011.]

11. «Photo Labs Part of Fight Against Child Porn?» en *ABC News*: [en línea] <<http://abcnews.go.com/2020/story?id=132673>>. [Nota del autor: visitado el 19 de septiembre de 2011.]

12. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

mencionado riesgo de sobreprotección: el peligro de que el intermediario, por evitar su responsabilidad, se dirija contra la conducta reprochable, pero que en el camino se lleve por delante conducta socialmente valiosa. La incertidumbre en torno a si el comportamiento que el intermediario facilita es lícita (y, por ende, la duda en torno a si será responsable o no) lo inducirá a ser conservador en torno a qué actividad permitir. Pero el tipo de ambigüedad y las razones para ella variarán en cada caso. Y en el esquema de responsabilidad de intermediario que escojamos ante esta incertidumbre, habrá un juicio valorativo subyacente sobre los intereses de expresión involucrados.

En el fondo, la selección de mecanismos que expongan a intermediarios a responsabilidad reflejará una estimación de riesgos que considere la magnitud de los costos de la sobreprotección (es decir, una determinación subyacente de los valores de expresión que queremos proteger y a qué grado). Así, si poco nos importan los riesgos de que un intermediario se exceda evitando el tráfico de pornografía infantil, tal vez podamos tolerar cierto tipo de reglamentación de intermediario, con obligaciones policíacas más onerosas, que no toleraríamos para el caso de los derechos de autor o la protección de la honra. La sobreprotección en estos últimos dos casos presenta el potencial de supresión de expresión política, de interés público o cultural que tal vez no ocurre en el primero (o que ocurre en menor grado). Esta evaluación sustantiva es, me parece, el primer paso conceptual que debemos hacer antes de proponer soluciones concretas.

III. Modos de regulación

Con ello en mente es que luego debemos considerar los diversos tipos de reglamentación que están disponibles. Para balancear los distintos intereses en juego, en cada contexto, podemos pensar en cuatro formas principales mediante las que el derecho se dirige a los intermediarios con varios regímenes posibles.

Primero, podríamos estructurar un sistema de *inmunidad absoluta* para los intermediarios, tal y como ocurre en los Estados Unidos regido por la sección 230 del Communications Decency Act¹³, que guarda relación con

13. 47 U.S.C. § 230.

la responsabilidad de intermediarios en Internet por daños a la honra y reputación ocasionados por terceros. De más está decir que esta alternativa, si bien es apoyada por amplios sectores como necesaria para fomentar el debate público y el desarrollo empresarial en Internet,¹⁴ es sumamente controversial y abundan sectores críticos que preferirían modificaciones que impongan a intermediarios deberes *ex ante* o *ex post*¹⁵. En el fondo, cabe resaltar, un régimen de irresponsabilidad como el descrito revela una valoración sustantiva muy alta de los intereses de expresión en juego (frente a los intereses de privacidad) de tal forma que el riesgo de la sobreprotección resulta intolerable.

Segundo, podríamos concebir un sistema de *responsabilidad estricta*, que obligue al intermediario por razones independientes a su diligencia o conocimiento del ilícito, obligándolo a reparar el daño que se produzca por usuarios, en todo caso, del servicio¹⁶. Sin embargo, como señalan Ruiz Gallardo y Lara Gálvez, esta no parece ser la tendencia en América Latina¹⁷ y, añadido, un régimen de este tipo exacerbaría el riesgo de sobreprotección. En casos extremos, elevaría el costo esperado de responsabilidad del intermediario a tal grado que estos costos superarían los beneficios de incurrir en esa actividad económica, induciéndolo a no proveer en primera instancia ese servicio.

Tercero, podemos pensar en sistemas de *responsabilidad subjetiva*, de modo que el intermediario se exponga a obligación civil por culpa o dolo, tras, por ejemplo, incumplir un deber de actuar con diligencia luego de haber tenido conocimiento o cuando debió haber conocido el acto ilícito. Al momento, este modelo parece predominar en países como la Argentina y Chile en atentados contra el honor y la honra¹⁸.

Finalmente, el sistema que predomina para la protección de derechos de autor en varias jurisdicciones en la región y en el mundo es el de regímenes de *inmunidad condicionada* al cumplimiento de diversas obligaciones,

14. Véase, por ejemplo, *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).

15. Levmore, Saul y Martha Nussbaum, *The Offensive Internet: Speech, Privacy, and Reputation; sine nomine et sine loco*, 2011.

16. Véase, en este volumen, Ruiz Gallardo, Claudio y J. Carlos Lara Gálvez, capítulo 1, «Responsabilidad de los proveedores de servicios de Internet (ISPs) en relación con el ejercicio al derecho a la libertad de expresión en Latinoamérica».

17. *Íd.*

18. *Íd.*

algunas más preocupantes que otras. Así, tenemos sistemas de *notificación y bajada*, que reclutan a intermediarios para facilitar la bajada de contenido tras la notificación por quien sostiene ser titular de derechos de autor o un tribunal (según sea el caso), y que, en principio, están incorporados en acuerdos de libre comercio en la región, como el futuro Acuerdo de Asociación Transpacífico de Libre Comercio¹⁹ y el Tratado de Libre Comercio entre Colombia y los Estados Unidos²⁰, este último sirve de base para la reciente propuesta de ley de responsabilidad de intermediarios de Colombia²¹. Dentro de esta opción de inmunidad condicionada, los detalles harán la diferencia: habrá que definir qué condiciones tienen que cumplir los intermediarios para ganarse la inmunidad (qué obligaciones de supervisión tienen o si deben fungir como policías activos, por ejemplo), si se contempla la retirada de contenido o la cancelación de cuentas de usuarios y qué tipo de procedimientos legales o privados precederán la bajada de contenido²².

Del otro lado, al implementar estos regímenes –particularmente en los sistemas de responsabilidad subjetiva y de inmunidad condicionada– en el derecho, encontramos mecanismos que imponen obligaciones de diversa índole. Siguiendo a Reinier Kraakman²³ y a Jonathan Zittrain²⁴, propongo considerar dos tipos de esquemas generales: *porteros* y *chaperones*.

Los intermediarios actúan como *porteros* cuando atienden la conducta no deseada bloqueando de plano, cerrando una puerta o negándose a tener relación con el presunto malhechor. Un *portero* de esta naturaleza, generalmente, podrá excluir a individuos cumpliendo con un deber de

19. Véase la discusión en Ruiz Gallardo y Lara Gálvez en *íd.* anterior.

20. Véase [en línea] <<http://www.ustr.gov/trade-agreements/free-trade-agreements/colombia-fta/final-text>>. [Nota del editor: consultada el 17/10/2011.]

21. Sobre el proyecto colombiano, véase Botero, Carolina, *Proyecto de ley sobre infracciones al derecho de autor en Internet*, 5 de abril de 2011 [en línea]: <<http://www.karisma.org.co/carobotero/index.php/2011/04/05/proyecto-de-ley-sobre-infracciones-al-derecho-de-autor-en-internet>>. [Nota del editor: consultada el 17/10/2011.]

22. La ley chilena requiere de la intervención judicial para ordenar bajar el contenido. Para esto, véase la Ley de Derechos de Autor de Chile, la Ley 17336, del 2 de octubre 1970, y la enmienda del 4 de mayo de 2010, la Ley 20435; disponibles en línea: <<http://www.leychile.cl/Navegar?idNorma=28933&idVersion=2010-05-04>>. [Nota del editor: consultada el 17/10/2011.]

23. Kraakman, Reinier H., «Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy», en *J. L. Econ. & Org.* 2 (1986), p. 53.

24. Zittrain, Jonathan, «A History of Online Gatekeeping», en *Harv. J. L. & Tech.*, 19 (2006), p. 253.

supervisión preciso y muy limitado (como pedir identificación para verificar edad antes de vender alcohol o, en el contexto de ISPs, cortar el acceso a Internet a usuarios luego de que un tribunal lo ordene o bajar el contenido con solo recibir una notificación dentro de un esquema de notificación y bajada).

Pero cuando los intermediarios detectan y limitan conducta de usuarios durante el transcurso de una relación continua, actúan más como *chaperones* y, en esa función, realizan tareas de monitoreo más complejas, que responden a deberes más difusos que los que tienen los *porteros* (por ejemplo, un deber de cuidado, como tomar medidas cautelares o filtros). En muchos casos, el derecho impone estas obligaciones y genera *porteros* y *chaperones* directamente. En otros, los intermediarios se autorregulan y constituyen sus propios regímenes.

La pregunta es si en cada uno de los renglones de expresión que hemos visto (derechos de autor, pornografía infantil y ataques a la honra) hay razones para preferir mecanismos de *responsabilidad objetiva*, *subjetiva*, *inmunidad condicionada* y, dentro de ellos, sistemas de *chaperón* o de *portero*, o si, en cambio, hay razones para no imponer responsabilidad alguna al ISP.

No hay contestaciones sencillas a esta pregunta, pero algunos factores deben inclinar la balanza.

Entre ellos, debemos considerar:

- (a) Primordialmente, el valor que la sociedad está dispuesta a atribuirle a la conducta del usuario y que está sujeta al potencial de sobreprotección (en términos de su valor para la libertad de expresión) para, de esa forma, evaluar los riesgos de las medidas del intermediario;
- (b) el costo de las medidas de monitoreo o de portería, y cuán factible es para el intermediario realizar la actividad exigida por la ley;
- (c) crucialmente, el nivel de certeza o incertidumbre en cuanto a si la conducta del usuario es constitucionalmente protegida;
- (d) el nivel de ambigüedad en el deber del *portero* o *chaperón*;
- (e) el costo para el intermediario de ser encontrado responsable;
- (f) el impacto de la supervisión del intermediario sobre otros intereses, como el anonimato y la privacidad.

Y es que, mientras más difícil resulte dilucidar si la conducta del usuario es ilegal o constitucionalmente protegida; mientras más alto es el costo de la potencial responsabilidad del intermediario y mientras más valoremos la conducta expresiva vulnerable, mayor es el riesgo de que se sobreprotejan intereses estatales en detrimento de valores expresivos importantes. Por su

importancia en el cálculo costo-beneficio del intermediario, de entre todos estos factores, me detendré en el efecto que tiene el nivel de incertidumbre en torno a si la conducta es constitucionalmente protegida o si, en cambio, puede ser proscrita.

IV. El rol de la ambigüedad

Nótese el rol que juega la ambigüedad en todo esto. El riesgo de sobreprotección no depende exclusivamente de que el intermediario tenga deberes especiales de supervisión (como sucede en sistemas de portería *notice and takedown*), o que se le imponga un deber afirmativo de identificar usuarios malhechores.

Como se ha dicho, un sistema de responsabilidad objetiva presenta graves riesgos ante la dificultad para un intermediario de conocer *ex ante* si lo que facilita es legal o no. Pero el problema no se limita a ese tipo de responsabilidad: basta que exista un sistema de responsabilidad subjetiva convencional unido a la incertidumbre sobre la extensión de la protección constitucional, para que los riesgos de sobreprotección se materialicen.

Esto es así pues si es difícil deslindar lo nocivo de lo constitucionalmente protegido, cualquier notificación de un supuesto perjudicado bastará para amedrentar al intermediario con la mera posibilidad de un litigio costoso, lo que genera el riesgo de sobreprotección.

Por ejemplo, los casos de la Argentina²⁵ y Chile²⁶ sobre la protección a la honra sugieren un estándar de culpa o negligencia convencional de responsabilidad (no objetiva) que, en la práctica, imponen de manera implícita un deber de supervisión constante, del tipo *chaperón*, en la medida en que el ISP es responsable tan pronto conozca (o cuando debió haber conocido) la existencia de actividades nocivas. En Chile, este

25. Cámara Nacional de Apelaciones en lo Civil, sala D, Expte. N° 99.620/2006 *D. c. v. c/ Yahoo de Argentina S.R.L. y otros/ Daños y Perjuicios* Recurso N° 541.482, Juzgado N° 75. Véase en el presente volumen la discusión en torno a este tema entre Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, *íd.* nota 18.

26. Corte de Apelaciones de Concepción, sentencia sobre recurso de apelación, Paulina Fuentes Almendra y otro *c/ ENTEL S.A.*; Carmen Gloria Yáñez Vargas, rol 1223-2003, sentencia del 21 de diciembre de 2007. Para observar la discusión entre Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, véase *íd.* nota 18.

sistema produce un deber (en la primera vida del caso Entel) de tomar providencias necesarias para identificar a usuarios responsables de las expresiones difamatorias, aunque, en apelación, el impacto de este deber es mitigado por el igualmente ambiguo principio de «libertad de la información que circula en la red». Un deber de cuidado razonable como este se puede traducir en una obligación por tomar medidas preventivas o de tomar acción *ex post* tras una notificación. Una vez es informado acerca del alegado ilícito, esa notificación (por deficiente que sea) torna al intermediario en un *portero*, por lo imposible (o costoso) que resulta evaluar la legitimidad del reclamo *ex ante*.

De esta forma, cuando hay ambigüedad, un sistema tipo *chaperón* en un régimen de responsabilidad subjetiva tiene el potencial de transformarse en un sistema de portería *de facto*, al estilo de notificación y bajada, es decir, cualquier notificación será suficiente para configurar el elemento subjetivo de conocimiento, lo que motivaría la bajada inmediata. Y dependiendo de nuestra valoración sobre los intereses constitucionales en juego, estos riesgos pueden resultar inaceptables.

En otros casos, sin embargo, cuando la ambigüedad en la ilegalidad de la conducta es menor y los riesgos contra la expresión que valoramos son más tolerables, un sistema tipo *portero* puede ser adecuado, como suceda, posiblemente, con la pornografía infantil. De hecho, así es en Brasil, al proveerse un sistema de notificación oficial y bajada²⁷.

Pero en la mayoría de los casos, no hay mucha ocasión para tirar líneas nítidas y cristalinas que permitan sistemas de *portería* a bajo costo, ni para sistemas de *chaperones* que no generen incentivos de sobreprotección. Por ejemplo, en los sistemas de notificación y bajada presentados en el caso de derechos de autor (para servicios de alojamiento), precisamente porque no es fácil determinar cuándo es que se violan derechos propietarios, la única opción razonable para el intermediario es bajar el contenido inmediatamente, lo que conlleva el alto riesgo de afectar intereses de expresión. Y esa predecible reacción del ISP, además, provee ocasión para una estrategia perversa de parte de alegados titulares de derechos, pues genera incentivos para someter notificaciones fatulas: un estudio encontró que el 30% de los requerimientos para retirar contenido eran solicitudes basadas en reclamos

27. Estatuto de la Niñez, artículo 241-A (inciso II). Para observar la discusión entre Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, véase *id.* nota 18.

legales débiles, así como también, que muy pocos usuarios se aprovechaban del procedimiento de respuesta provisto por la ley²⁸. Asimismo, se ha visto que titulares de derechos con asiduidad envían notificaciones a intermediarios sobre supuestos participantes en redes *peer-to-peer* aun cuando estos no descargan o comparten contenido con nadie²⁹.

En este sentido, al menos en los casos de difamación y derechos de autor por su ambigüedad, cualquier sistema que delegue (directa o indirectamente) la supervisión a los intermediarios (cuyos intereses son diferentes a los de usuarios) será problemático³⁰.

Entonces, si el problema es la ambigüedad, dos serán las opciones viables en términos generales: por un lado, se exime de responsabilidad absolutamente al ISP (como con la difamación online en los Estados Unidos) o, en otro caso, se genera un mecanismo de desambiguación, ya que se transfiere la responsabilidad de precisar organismos capaces de considerar los intereses libertarios del usuario (de modo de deslindar lo constitucionalmente protegido de la actividad ilegal) en tribunales de justicia u otros organismos administrativos, mediados por garantías procesales apropiadas (como por ejemplo, la ley de derechos de autor de Chile, en la que se requiere intervención judicial para ordenar la baja del contenido)³¹.

28. Urban, Jennifer, «Efficient Process or “Chilling Effects”? Takedown Notices under Section 512 of the Digital Millennium Copyright Act, en *Santa Clara Comp. & High Tech L. Journal*, 22 (2006), p. 621

29. Piatek, Michael, Tadayoshi Kohno y Arvind Krishnamurthy, «Challenges and Directions for Monitoring P2p File Sharing Networks -or- Why My Printer Received a DMCA Takedown Notice Why My Printer Received a DMCA Takedown Notice», en *University of Washington Technical Report*, UW-CSE-08-06-01 [en línea]: <<http://dmca.cs.washington.edu>>. [Nota del editor: consultada el 18/10/2011.] (En dos estudios separados, en 2007 y 2008, unos investigadores introdujeron «usuarios» con direcciones IP de la Universidad de Washington, tales como impresoras, en redes Bit-Torrent para monitorear el tráfico. Aun cuando esos «usuarios» no descargaron archivos, más de 400 notificaciones fueron recibidas.)

30. Incluso en los Estados Unidos, aun para los casos de ISPs que no tienen funciones de alojamiento y cuya inmunidad está casi garantizada, recientemente las principales compañías (AT&T, Cablevision, Comcast, Time Warner Cable y Verizon) establecieron un sistema de supervisión privada que consiste en *copyright alerts* y *medidas de mitigación*, cuya función es disminuir la velocidad de la conexión o suspender el servicio que está sujeto a que el usuario contacte al ISP –medidas que potencialmente afectan derechos de expresión–. Para saber más sobre esto [en línea]: <<http://www.copyrightinformation.org/alerts>>. [Nota del editor: consultada el 18/10/2011.]

31. *Id.* nota 21.

V. Hacia un modelo de inmunidad condicionada reformado

Tras la anterior discusión, resulta claro que al menos dos de los cuatro tipos de reglamentación mencionados (*inmunidad absoluta*; *inmunidad condicionada*; *responsabilidad objetiva* y *subjetiva*), tienen elementos desfavorables en aquellos casos en que la vaguedad prevalece. De un lado, el sistema de *responsabilidad objetiva* presenta riesgos muy altos de sobreprotección y, del otro, el sistema de *responsabilidad subjetiva* tiene el riesgo de convertirse en un modelo de notificación y bajada al presentarse cualquier notificación en situaciones de incertidumbre (la generalidad de los casos).

Ante ello, nos quedan los modelos de *inmunidad absoluta* o de *inmunidad condicionada*. El primero, como he sugerido, tal vez conviene solo si es que se entiende que los riesgos de una determinación errónea son demasiado altos respecto a la libertad de expresión, como es el caso de los Estados Unidos y la sección 230 del Communications Decency Act, que exime absolutamente de toda responsabilidad a intermediarios por actos difamatorios por usuarios. Personalmente favorezco esta alternativa para el caso de la responsabilidad del intermediario por difamación y ataques abusivos a la honra, pues el riesgo de que se menoscabe expresión valiosa es muy alto. Pero esta determinación dependerá de los balances de valores sustantivos que hagamos en América Latina en torno al choque de intereses de expresión y dignidad humana en esos casos, para lo cual no hay consenso universal.

Así, pues, si entendemos que la *inmunidad absoluta* no está disponible, será necesario un mecanismo independiente para desambiguar y con ello evitar los problemas de sobreprotección que presenta delegar al intermediario la supervisión de la actividad en línea. Para ello, el sistema judicial tiene una función vital que cumplir. Después de todo, si los derechos individuales están en juego; y si el riesgo de una retirada de contenido puede afectar la libertad de expresión, corresponderá a los tribunales tomar cualquier decisión que pretenda balancear los intereses del Estado que motivan la reglamentación con los intereses de expresión.

Por otra parte, el modelo de *inmunidad condicionada* (mediado por la intervención judicial previo a cualquier retirada de contenido) puede ajustarse para estos fines, pero solo si se complementa con procesos respetuosos de derechos individuales, como la privacidad, el debido proceso de ley y el derecho a acceso a la información. Algunos modelos de reforma

se han propuesto –los que anoto al margen³²– al mismo tiempo que enfatizan, entre otras cosas, elementos que provean al usuario la oportunidad real de cuestionar (antes de la retirada de contenido) reclamos de personas que se alegan afectadas y la imposición de sanciones para aquellos que abusen del sistema ante reclamos deficientes.

VI. Conclusión

En América Latina y en el resto del mundo debemos asumir con seriedad que, si bien tecnologías de información contemporáneas traen consigo un potencial expresivo abarcador, este potencial viene acompañado de oportunidades de control estatal y privado muy efectivo.

Entender el alcance de ambas –tanto de las posibilidades de expresión así como de su potencial reglamentación– es esencial para el ejercicio pleno de nuestras libertades civiles en la red. Por ello, dejarnos seducir acríticamente por la promesa de nuevas tecnologías, nos expone a que se enraícen limitaciones contemporáneas a nuestros derechos de expresión en el *statu quo*.

En este sentido es importante entender cómo sacamos provecho del potencial liberador que encierran las tecnologías de información, a la vez que consideramos reglamentar alguna conducta en línea a fines de proteger objetivos estatales importantes, tales como la protección de los derechos de autor, la limitación de la pornografía infantil y la atención de atentados contra el honor, la honra y la vida privada. Ese balance debe servir de guía a la hora de proponer reformas legales y de política pública en el entorno digital interconectado.

32. Véanse Chen, Dena, Musetta Durkee, Jared Friend y Jennifer Urban, *Copyright Reform Act: Updating 17 USC § 512's Notice and Takedown Procedure for Innovators, Creators, and Consumers* (2011), disponible [en línea] en < <http://www.publicknowledge.org/files/docs/cranoticketakedown.pdf> > [nota del editor: consultada el 18/10/2011] y Seltzer, Wendy, «Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment», en *Harv. J.L. & Tech.*, 24 (2010), p. 171.

Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet

Lorenzo Villegas Carrasquilla¹

Introducción

La información es poder, y la información económica es poder económico. La información tiene un valor económico y la capacidad de almacenarla y procesar ciertos tipos de datos puede darle a un país ventajas políticas y tecnológicas sobre otros países².

El desarrollo de las tecnologías de la información y las comunicaciones (TIC), así como diversos avances tecnológicos en medicina, computación y biología molecular, entre otros, han cambiado sustancialmente el panorama y el contexto de la privacidad y del flujo de información. Esta siempre ha sido un elemento esencial para la toma de decisiones y tiene una importancia sustancial en el desarrollo de los negocios³.

1. Se puede contactar al autor en la siguiente dirección de correo electrónico: lvc@lorenzovillegas.com. Los análisis y opiniones son enteramente responsabilidad del autor y no comprometen a ninguna institución. Todas las traducciones son libres.

2. Eger, John, «Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?», en *Law and Policy in International Business*, 10,4 (1978), pp. 1065-1066.

3. Remolina, Nelson, «¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?», en *International Law, Revista Colombiana de Derecho Internacional*, 16 (2010), p. 493.

Gran parte del desarrollo de Internet y de las transacciones de comercio electrónico encuentran su base en el flujo y compartición de información a nivel globalizado⁴. Las personas pasan gran parte de su tiempo en la red intercambiando información, perfiles y datos con otros usuarios, sean estas personas o actividades comerciales, mediante chats, blog, compras, transacciones, redes sociales, servicios de *cloud computing*, etcétera⁵. El desarrollo tecnológico ha permitido que el intercambio de información sea mucho más fácil.

Este importante tráfico de información también ha garantizado grandes beneficios económicos. El análisis de aquella, de los datos y los metadatos, *i.e.*, datos que se extraen de los ya recolectados, ha permitido que se disminuyan los fraudes con tarjetas de crédito; que se reduzcan los costos en las terapias genéticas y que los reclamos fraudulentos en seguros de salud se reduzcan sustancialmente⁶.

Precisamente, en la medida en que las tecnologías permiten una mayor transferencia de información, nuevos y potenciales riesgos que afectan a las personas y las empresas aparecen. Entre estos, se encuentran los peligros que pueden ir contra la intimidad de la personas⁷. Este intenso intercambio de información entre las personas y entre personas y negocios ha generado una especial preocupación en relación con la protección de la privacidad y la transferencia de los datos personales.

Si bien las preocupaciones sobre la privacidad se han manifestado desde el siglo XIX⁸, la protección de la intimidad y de los datos personales se convierten en un asunto de interés para el Estado, con el temor de los usos inadecuados que podría presentársele a la información que reposaba en archivos gubernamentales gracias al desarrollo de los procesamientos computarizados

4. Friedman, Thomas, *La Tierra es plana*, Madrid, Martínez Roca, 2006, p.162 y ss.

5. De acuerdo con el estudio de 2006 realizado en los Estados Unidos, el 61% de los adolescentes revelan su información de contacto en blogs. El 44% desvela su dirección de email; el 30%, su página web personal; el 55% indica su localización geográfica; el 39% divulga su fecha de nacimiento y el 20% publica su nombre. Véase Huffaker, David, *Teen Blogs Exposed: The Private Lives of Teens Made Public* (2006), disponible [en línea] en: <http://www.davehuffaker.com/papers/Huffaker-2006-AAAS-Teen_Blogs.pdf>. [Nota del editor: consultada el 29/10/11.] Estas estadísticas deben haber aumentado sustancialmente con el crecimiento de las redes sociales.

6. OECD, «Roundtable on Economics of Personal Data and Privacy», DSTI/ICCP/IE/REG (2011) 1, 21 de abril de 2011, p. 3.

7. OECD, «Report on the Cross-Border Enforcement of Privacy Laws», 2006.

8. Warren, Samuel D. y Louis D. Brandeis, «The Right to Privacy», en *Harvard Law Review*, IV, 6 (15 de diciembre de 1890).

de los datos, lo que podría vulnerar derechos de los ciudadanos⁹. En muchos países, sobre todo los europeos, se empezó a crear conciencia sobre la importancia de la protección de los derechos de privacidad, por lo que se crea comités de estudio para tratar estos asuntos¹⁰. Como resultado de estos esfuerzos gubernamentales de discusión y debate se expidieron varias leyes. Así se expidieron la Ley de Suecia de Datos (1973); la Ley de Países Bajos sobre datos personales y registro (1988); la Ley de Privacidad de los Estados Unidos (1974) y la Ley de Informática e Información (1978) de Francia, entre otras. Según la OECD, antes de 1980, más de 8 países de la OECD habían expedido legislación relacionada con la protección de los datos personales¹¹.

Este tipo de reglamentación se fundamenta, principalmente, en el derecho de cada individuo a su intimidad. Sin embargo, la noción de intimidad y vida privada, su fundamento como derecho y la manera de regularlo y protegerlo varían de región en región, de país en país.

Internet y los fenómenos asociados con las nuevas tecnologías de la información han implicado nuevos retos a los países, con el fin de proteger los datos personales y garantizar el derecho a la intimidad de las personas. El objetivo de este trabajo es estudiar los desafíos que imponen las nuevas tecnologías, particularmente Internet, a la protección de datos personales, desde el análisis de los diferentes sistemas de protección y en comparación. Así nos propondremos analizar los modelos jurídicos de cuatro países latinoamericanos (la Argentina, Chile, Colombia y México) con el fin de comprender cómo nuestras legislaciones abordan estas problemáticas y cómo se enfrentan a las complejidades que acarrea Internet para el desarrollo de los derechos fundamentales. En este trabajo se observarán los estándares que plantea cada legislación para la protección de datos, las condiciones legales para la transferencia internacional de datos personales y la manera en la que las autoridades judiciales o administrativas latinoamericanas protegen la privacidad en un ambiente de Internet, además de analizar las regulaciones sobre retención de datos personales en nuestros países. Finalmente, se presentará una sección de recomendaciones y conclusiones¹².

9. Bennet, Colin, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, 1992.

10. OECD, «The Evolving Privacy Landscape», DSTI/ICCP/REG (2010) 6/FINAL, p. 7.

11. *Íd.*

12. Este estudio no analizará los problemas de la privacidad de niños, niñas y adolescentes en la medida en que se involucran otros intereses y bienes jurídicos particulares.

I. Los modelos de protección de datos personales

El derecho a la intimidad y la vida privada ha sido considerado un derecho universal de las personas. La Declaración Universal de los Derechos Humanos de 1948 establece en el artículo 12 que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques»¹³.

Para el interés de nuestro estudio, hemos identificado tres visiones sobre el tratamiento y protección de los datos personales: el sistema de los Estados Unidos, el sistema europeo y el sistema latinoamericano.

En primer lugar, el sistema de los Estados Unidos responde al problema de la privacidad mediante mecanismos de autorregulación principalmente; no obstante, está parcialmente protegida la privacidad por la cuarta enmienda de la Constitución:

La privacidad solo se considera «fundamental» cuando se ve amenazada por un abuso gubernamental en el trato de la información personal y, por tanto, la ley federal interviene solo frente a él o, también, cuando se trata de negocios que almacenan información personal sensible. Salvadas estas circunstancias, la protección de los datos se considera un elemento disponible por parte de los ciudadanos¹⁴.

Sin embargo, la privacidad como derecho se encuentra bastante limitada, particularmente, por la protección a la libertad de expresión consagrada en la enmienda primera de la Constitución¹⁵.

En especial, el modelo de los Estados Unidos se desarrolló a partir de decisiones jurisprudenciales que dieron alcance a un ámbito personal que

13. Véase [en línea]: <<http://www.un.org/es/documents/udhr>>. [Nota del editor: consultada el 29/10/11.]

14. Guerrero Picó, María del Carmen, *El impacto del Internet en el derecho fundamental a la protección de datos de carácter personal; sine loco*, Thomson-Civitas, 2006, p. 347.

15. Igualmente, Richard Posner y Lawrence Lessig han criticado la protección a la privacidad como un elemento que reduce la eficiencia de los mercados, ya que limita la información. Véanse Posner, Richard, «The Economics of Privacy», en *The American Economic Review*, 71(2) (1981), pp. 405-409 y Lessig, Lawrence, *Code: Version 2.0*, Nueva York, Basic Books, 2006.

no podía ser intervenido por el Estado¹⁶, lo que tuvo como consecuencia la expedición del *Privacy Act* de 1974, cuyo alcance está limitado al tratamiento de datos por parte del Gobierno federal. Sin embargo, en los Estados Unidos existe legislación federal y estatal sectorial que regula ámbitos específicos de protección del *privacy right*¹⁷.

En segundo lugar, el modelo europeo está fundamentado, a partir del artículo 8 del Convenio Europeo de Derechos Humanos de 1950 que garantiza el respeto al derechos a la vida privada y familiar, como un derecho fundamental: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia»¹⁸.

Se considera que el modelo europeo garantiza un alto nivel de protección de datos personales por ser garantista, riguroso y efectivo¹⁹. Así se expidió en primer lugar el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal de 1981 y, posteriormente, la Directiva 95/46/CE sobre la protección de datos personales. Esta norma tiene como finalidad establecer estándares uniformes de protección de datos con el fin de garantizar el flujo de información entre los países miembros de la Unión Europea, el cual se veía obstaculizado. A partir de esta directiva, los Estados miembros han expedido sus legislaciones nacionales²⁰.

Finalmente, el tercer modelo es el modelo latinoamericano, el cual se ha basado principalmente en el derecho fundamental del *habeas data* y,

16. Véase Corte Suprema de Justicia de los Estados Unidos, *Meyer v. Nebraska* (262 u.s. 390 [1923]) y *Pierce v. Society of Sisters* (268 u.s. 510 [1925]). Véase, igualmente, *Whalen v. Roe* (429 u.s. 589 [1977]).

17. Entre otros, véanse: Cable Communications Policy Act; Video Privacy Protection Act; Omnibus Safe Streets and Crime Control Act; Electronic Communications Privacy Act; Health Insurance Portability and Accountability Act (HIPAA); the Children's Online Privacy Protection Act (COPPA) y Fair and Accurate Credit Transactions Act (FACTA).

18. Véase [en línea]: <http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf>. [Nota del editor: consultada el 29/10/11.]

19. Remolina, *supra* nota 3. No obstante, esta postura ha sido criticada en la medida en que no ha sido tan efectiva esta protección europea por falta en la aplicación y ejecución de las normas. Véase Burghardt, Buchmann, Böhm, *et. ál.*, «A Study on the Lack of Enforcement of Data Protection Acts Proceedings», en *3rd int. conference on e-democracy*, 2009.

20. Véase, por ejemplo, la Ley Orgánica de Protección de Datos, de España, de 1998 [en línea], en: <<http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>>. [Nota del editor: consultada el 29/10/11.]

posteriormente, se ha inclinado hacia un modelo de protección influenciado fuertemente por el de la directiva europea de 1995²¹. El *habeas data*, además de ser un derecho fundamental, es una herramienta de protección jurídica de los titulares de datos personales creada con el fin de conseguir la protección frente al tratamiento indebido o ilegal de sus datos de carácter personal por parte de bases de datos o archivos públicos o privados. Como se verá posteriormente, las legislaciones latinoamericanas se han movido hacia el modelo europeo máxime con el objetivo de ser consideradas marcos legales con nivel adecuado de protección por parte de Europa y que, además, puedan ser parte de negocios que implican transferencia internacional de datos desde Europa²².

De este primer análisis, podemos resumir las principales diferencias en los modelos europeo y estadounidense: (1) el enfoque del modelo de los Estados Unidos se basa, en esencia, en el concepto de libertad como respuesta a la intromisión del Estado en la vida de los individuos y el modelo está dirigido hacia la autorregulación y regulaciones sectoriales; (2) el enfoque europeo se manifiesta como una protección más general y uniforme, partiendo del concepto del derecho fundamental a la intimidad, en la cual el Estado debe intervenir activamente para proteger al individuo²³.

Estas importantes diferencias, en particular la no existencia de una legislación uniforme que garantice un nivel adecuado de protección según el estándar del artículo 25 de la directiva europea de 1995, hizo que existiera una controversia en torno a si las personas europeas podían transferir datos hacia los Estados Unidos, lo que crea un riesgo jurídico alto. Para responder a esta situación, el Departamento de Comercio de ese país creó el *International Safe Harbor Privacy Principles Certification Program*²⁴ (o Principios de Puerto Seguro). El programa de Puerto Seguro resuelve la falta de una ley uniforme de protección de datos: es un sistema

21. Pucinelli, Oscar, *El habeas data en Indoiberoamérica*, Temis, Bogotá, 1999.

22. Remolina, *supra* nota 3.

23. Para profundizar en las diferencias entre el modelo europeo y el americano, se sugiere que se vea Gregorio, Carlos, «Protección de datos personales: Europa v. Estados Unidos, todo un dilema para América Latina», en Concha Cantú, Hugo, Sergio López-Ayllón y Lucy Tacher Epelstein (eds.), *Transparentar al Estado: la experiencia mexicana de acceso a la información; sine nomine et sine loco*, 2004.

24. Véase [en línea]: <<http://export.gov/safeharbor>>. [Nota del editor: consultada el 29/10/11.]

voluntario del Departamento de Comercio en el que las organizaciones que se registren, cumpliendo con los estándares de dichos principios, son considerados adecuados para la transferencia de datos de conformidad con el artículo 25 de la directiva europea. El Puerto Seguro fue aprobado por la Comisión Europea en la Decisión 2000/520/CE como programa que otorga nivel adecuado de protección de datos²⁵.

II. Protección de datos personales y los retos de Internet

El panorama de la utilización de los datos ha cambiado de manera sustancial en los últimos veinte años. El avance de la informática, que nos ha conducido a lo que conocemos como la Sociedad de la Información, en la cual Internet es la pieza fundamental de este proceso, permite el planteo de diferentes problemas jurídicos en relación con el uso y recolección de los datos personales. En esa medida, por un lado, nos encontramos ante un ordenamiento jurídico que garantiza (de modos distintos) al ciudadano el control de sus datos personales y, a la vez, nos hallamos en un ambiente en el cual la relación del usuario con Internet implica una interacción en la cual el ciudadano entrega gran cantidad de información con el solo hecho de navegar en ella: la navegación, tal como la conocemos, funciona en la medida en que se van recogiendo datos que le permitan trabajar de manera correcta, rápida y efectiva (*e.g.*, *cookies* que habilitan la identificación de comportamientos de navegación, para, así, garantizarle al usuario una navegación más personalizada).

Algunos autores han visto todo este desarrollo como un potenciador de peligros hacia los ciudadanos.

Internet ha servido a intereses sibilinos. Es un vehículo especialmente poderoso a través del cual cualquier persona puede perpetrar atentados criminales contra cuatro tipos de derechos, bienes e intereses jurídicos básicos: la intimidad, la imagen, la dignidad, el honor de las personas y la libertad sexual [...]²⁶.

25. Véase [en línea]: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>>. [Nota del editor: consultada el 29/10/11.]

26. Guerrero Picó, *supra* nota 14, p. 334.

Esta postura, que en nuestra opinión es *peligrosista*, reduce las ventajas de Internet y se concentra en potenciales riesgos. Esta posición deja de lado que la red ha sido una oportunidad para fortalecer, replantear y explorar nuevas formas de desarrollo de otros derechos fundamentales, como la libertad de expresión, el derecho a la información, el derecho a la educación y al conocimiento, entre otros. Quienes sostienen esta postura sobre los peligros de Internet en el derecho a la intimidad consideran esencial que el Estado regule de manera anticipada el uso de Internet, con el fin de prevenir posibles peligros.

El surgimiento de nuevos recursos que ofrece la red para expresarse (Web 2.0), como Facebook, YouTube, blogs, Twitter, LinkedIn, tiene sentido en la medida en la que los usuarios de dichas plataformas ponen a disposición pública de forma voluntaria información muchas veces catalogada como privada. Los usuarios libremente entran a estas plataformas, de manera voluntaria suscriben las condiciones del servicio y empiezan a interactuar con otros usuarios y dan a conocer información personal. Fotos, videos, datos sobre su vida personal y profesional, sobre sus gustos y preferencias, etcétera llenan millones y millones de páginas web en las cuales las personas exponen su «intimidad», con el fin de desarrollar nuevas oportunidades que les son otorgadas por Internet²⁷.

Además, la red ha funcionado, en general, como la oferta «gratuita» de servicios, que ciertamente condicionan el uso gratuito en muchos casos a los modelos de publicidad online con el fin de financiar los contenidos y los servicios de alojamiento, entre otros. Este tipo de publicidad recurre a la recolección de información de los usuarios con el fin de proveer publicidad que se encuentre más acorde a los consumidores y conforme a los intereses de los internautas y sus objetivos²⁸.

Este fenómeno que cada día tiene más fuerza obliga a replantearse la importancia real que tienen los datos personales y el valor que cada persona le otorga a ellos. ¿Son tan valiosos para sus titulares como para que requiera una acción inmediata del Estado para regular Internet?

27. Para profundizar sobre tendencias en el uso de redes sociales, véase: Instituto Nacional de Tecnologías de la Comunicación (INTECO) y Agencia Española de Protección de Datos (AEPD), *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, febrero de 2009.

28. OECD, *supra* nota 6, p. 5.

Igualmente, las TICs y, particularmente, la globalización fortalecida por Internet, que ha permitido esquemas de colaboración global como el *outsourcing*, la deslocalización, el comercio electrónico y el *off-shoring*, han profundizado el fenómeno del tratamiento internacional de los datos personales, en especial, la transferencia internacional de datos y su recolección internacional²⁹. A continuación analizaremos dos aspectos que involucran Internet y la protección de datos personales.

II.A. *Cloud computing* y protección de datos

Una de las más importantes tendencias en el desarrollo de servicios en Internet es el *cloud computing*. Este puede entenderse como cualquier ejercicio de la computación que se haga en Internet³⁰, proveyendo acceso flexible, independiente de la locación, a recursos informáticos de manera rápida, pronta y económica. Los servicios que se ofrecen a través del *cloud computing* están virtualizados y corresponden a una compartición de recursos tecnológicos y de automatización que pueden encontrarse en cualquier lugar del mundo. Estos servicios pueden ir desde almacenamiento de correo electrónico hasta infraestructura y plataformas tales como servicios, entre otros.

Con el desarrollo de Internet, los servicios de *cloud computing* se encuentran asociados plenamente con la transferencia internacional de datos y su recolección, lo que genera presión en los sistemas jurídicos nacionales. Usualmente las reglas de transferencia internacional de datos y recolección internacional son un apéndice secundario de los estatutos de protección de datos personales. Sin embargo, la creciente tendencia a la utilización de servicios virtualizados en Internet obligará a los hacedores de políticas públicas a analizar con detenimiento cuáles son los mejores estándares de protección.

La transferencia internacional de datos personales puede definirse como la «importación o exportación de esa información de un país a otro»³¹. Así,

29. Friedman, *supra* nota 4.

30. Hon, Kuan, Christopher Millard e Ian Walden, «The Problem of “Personal Data” in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1», en *Legal Studies Research Paper N°. 75/2011*, p. 6, Queen Mary University of London, School of Law.

31. Remolina, *supra* nota 3, p. 495.

los datos se recogen en un país por parte del encargado o responsable del tratamiento de los datos personales y los traslada a otro país donde, a la vez, sufren un tratamiento. En el día a día, miles de empresas y Gobiernos movilizan datos personales más allá de las fronteras de los países: asuntos de seguridad nacional e internacional, cooperación judicial entre países, controles migratorios, soporte comercial o técnico de empresas a través de *call centers*, transacciones financieras, etcétera.

Por otro lado, la recolección internacional de datos es un fenómeno distinto particularmente fortalecido por Internet en la medida en que ha permitido fácilmente la comunicación entre personas de cualquier lugar del mundo. Un individuo puede recoger datos de otro que se encuentre en otro país y que haya ingresado a su página web. En este evento, no hay una transferencia internacional de datos, comoquiera que los datos no se recogen en un país y se trasladan a otro sino que se recolectan directamente en otro país. La recolección internacional de datos mediante Internet se realiza casi siempre con cualquier actividad que realice un usuario al interactuar en la red. Esta recolección de datos puede darse de manera consentida o no. Por ejemplo, mediante html, redes sociales, *cookies*, *web bugs*, *spyware*, *phishing*, virus y troyanos o caballos de troya³².

Estos tratamientos de datos han sido transferidos a proveedores de *cloud computing*, comoquiera que los límites nacionales y las jurisdicciones para la aplicación y garantía de los derechos se exceden, es esencial preguntarse sobre el modelo jurídico que debe regir este tipo de transacciones y la protección de los datos personales. En el estado actual de la regulación de datos personales, el modelo más conveniente para la regulación de su tratamiento en *cloud computing* es mediante cláusulas contractuales con el objetivo de preservar la integridad de los datos, la seguridad y confidencialidad de la información, así como el acceso en cualquier momento por parte de titular, a la vez que se genera responsabilidad contractual en la cabeza del responsable del tratamiento por los daños que se ocasionen al titular³³. Veremos más adelante cómo las legislaciones latinoamericanas regulan lo correspondiente a la transferencia internacional de datos.

32. Guerrero Picó, *supra* nota 14, pp. 339-344.

33. Consejo de Europa, *Protection of privacy and personal data on the Internet and online media report*. Comité sobre Cultura, Ciencia y Educación, relatora: Andreja Rihter. Documento 12021, Referencia 3608 del 2 de octubre de 2009. Reporte aprobado el 12 de mayo de 2011.

II.B. Acceso a la información en Internet: privacidad frente a libertad de expresión y libertad de información

Internet revolucionó el acceso a la información. La capacidad cada vez mayor de los buscadores en Internet ha permitido que la información existente en el mundo pueda ser accesible para todas las personas de una manera relativamente fácil. Mucha de esta información, aun siendo pública, como las decisiones judiciales o las gacetas oficiales, no tenía necesariamente pretensiones de difundirse de manera global. Esto ha planteado un nuevo reto para el derecho, particularmente en torno al alcance de la libertad de expresión y el derecho a la intimidad.

Internet ha permitido consultar de una manera expedita y amplia información gubernamental que siendo pública puede contener datos personales (nombre, sexo, identidad política, antecedentes penales o disciplinarios, entre otros). Ahora bien, ¿esta información accesible en Internet es considerada información o dato público? ¿Cuál es el tratamiento que debe dársele a esta información? ¿Cuál es el rol de Internet y de los buscadores en relación con la información indexada en ella?

Estas preguntas complejas no han encontrado una respuesta satisfactoria en la legislación latinoamericana³⁴. Por un lado, debe garantizarse que el acceso a la información sea transparente y abierto a todas las personas, en la medida en que no se coarte la libertad de expresión³⁵. Por otro lado, debe quedar claro cuál es el alcance de la información y el tratamiento que se debe dar en caso de contener datos personales. La Declaración de Principios sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos establece que «10. Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público [...]»³⁶.

34. Hay un esfuerzo doctrinal denominado Reglas de Heredia o Reglas Mínimas para la Difusión de Información Judicial en Internet. El objetivo de estas reglas es la de apoyar a la Justicia y a las instituciones responsables de la divulgación de jurisprudencia de todos los países de América Latina en el tratamiento de los datos personales contenidos en las sentencias y despachos judiciales en Internet sin vulnerar el principio de transparencia de las decisiones judiciales ni el derecho a la información. Véase [en línea]: <http://www.cej.org.co/component/docman/doc_view/389-reglas-de-heredia-comentadas>. [Nota del editor: consultada el 29/10/11.]

35. Véase Declaración Conjunta sobre Libertad de Expresión e Internet ONU, OSCE, OEA y CADHP de 2004 y 2011, entre otras.

36. Véase [en línea] en: <<http://www.cidh.oas.org/basicos/basicos13.htm>>. [Nota del editor: consultada el 29/10/11.]

Esta tensión ha sido resuelta de distintas formas por parte de legislaciones extranjeras y decisiones jurisdiccionales de la región, como se verá más adelante. No obstante, consideramos que tanto en las decisiones judiciales como en las legislaciones no existe claridad entre los diferentes roles que tienen quienes participan de este proceso de acceso de la información, particularmente Internet.

La posición mayoritaria europea, particularmente la española, ha sido la de no considerar Internet como un medio de comunicación ni como fuente accesible al público³⁷, particularmente en lo que se refiere a los motores de búsqueda³⁸. En ese sentido, en cuanto al tratamiento de datos personales, se ha considerado en Europa que los motores de búsqueda, al actuar como intermediarios tecnológicos, son responsables del tratamiento de datos personales, aunque no sean los responsables principales³⁹. Bajo esta interpretación, los motores de búsqueda se encuentran vinculados con la directiva europea de 1995, de conformidad con el principio de proporcionalidad. En consecuencia, el buscador de Internet tiene obligaciones en relación con el tratamiento de datos, como la de eliminar información desactualizada o retirarla de su índice. En este escenario, la obligación no recae en la fuente de la información, sino en el buscador.

Esta solución, controversial en nuestra opinión, surge de la inexistencia en la legislación del concepto de intermediario que se diferencie de los responsables o encargados del tratamiento. Como veremos en América Latina, las posturas son diversas, siguiendo principalmente la influencia europea.

III. La regulación de la protección de los datos personales y la intimidad en América Latina

III.A. El sistema constitucional latinoamericano

El sistema de protección de datos en América Latina tiene, en general, una característica particular que lo diferencia de los modelos europeo y

37. Agencia de Protección de Datos, *Memoria año 2001*. Igualmente véase decisión de la Commission Nationale de l'Informatique et des Libertés (CNIL) del 26 de mayo de 2004.

38. Groupe De Travail «Article 29» Sur La Protection Des Données, *Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche*, 4 de mayo de 2008. 00737/FR WP 148, véase [en línea] en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_fr.pdf>. [Nota del editor: consultada el 29/10/11.]

39. *Íd.*, p. 15.

estadounidense. En cuanto al modelo europeo, se diferencia principalmente por el hecho de que no existe un tratado internacional o normativa regional supranacional (ni en el Mercosur ni en CAN) que regule la protección de los datos personales ni la transferencia de estos. En cuanto al modelo estadounidense, la diferencia sustancial recae en el carácter constitucional de esta protección en una gran cantidad de países y sistemas jurídicos latinoamericanos.

Según el estudio elaborado por el profesor Nelson Remolina⁴⁰, el 65% de los países latinoamericanos incorpora en su Constitución normas expresas en relación con la protección de los datos personales, el *habeas data* y la intimidad. Este fenómeno de constitucionalización de la protección de los datos personales en las cartas magnas latinoamericanas surge particularmente en la década de los ochenta y se consolida en los noventa y primera década del siglo XXI. Los países de nuestro estudio, con excepción de Chile, tienen disposiciones de protección de los datos personales en aquellas.

Sin embargo, estas provisiones constitucionales enmarcan de manera más o menos limitada este derecho.

De los países en estudio, solo la constitución mexicana en el artículo 6 establece expresamente el derecho a la protección de los datos personales (reforma de 2009): «Toda persona tiene derecho a la protección de sus datos personales».

No obstante que las demás constituciones no tienen provisiones tan explícitas, esto no implica que no delimiten y le den contenido a este derecho fundamental. Los aspectos sobre protección de datos personales protegidos por las constituciones latinoamericanas objetos de nuestro estudio van desde el derecho a conocer datos contenidos en bases de datos públicas y privadas (la Argentina, Colombia, México); pasando por el derecho a conocer datos contenidos solamente en bases de datos públicas (México); el derecho a conocer la finalidad del uso de los datos (la Argentina); el derecho a conocer el uso que se le da a los datos; el derecho a exigir actualización de los datos (la Argentina, Colombia); el derecho a solicitar rectificación o corrección (la Argentina, Colombia, México); el derecho a solicitar supresión, eliminación, destrucción o cancelación del dato (la Argentina, México); el derecho a exigir confidencialidad sobre los datos (la Argentina); el derecho de oposición (México); el tratamiento de

40. Remolina, Nelson, *Retos de la recolección internacional de datos personales para los países latinoamericanos* (marzo de 2011). Sin publicar.

datos, circulación y recolección (Colombia); la acción de *habeas data* (el Perú) y la acción de amparo o tutela (la Argentina y Colombia)⁴¹.

Tabla 1 | **Normas constitucionales**

País	Norma constitucional
Chile	No tiene
Argentina	Artículo 43
México	Artículos 6 y 16
Perú	Artículo 2
Colombia	Artículo 15

Otro fenómeno particular de los sistemas jurídicos latinoamericanos es que, a pesar de estas disposiciones constitucionales, la mayoría de los países no tiene normas legales que desarrollen estos preceptos constitucionales o, al menos, ha tenido un desarrollo legislativo tardío⁴².

Chile fue el primer país latinoamericano que estableció una normatividad general sobre la protección de los datos personales. En 1999, se expidió la Ley 19628, que regula la protección a la vida privada o protección de datos de carácter personal.

Posteriormente, la Argentina resolvió su marco legal constituido principalmente por la Ley 25326, de 2000, que cobija la

protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados, destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, así como, también, el acceso a la información que sobre las mismas se registre [...].

Este marco legal se desarrolló particularmente con el Decreto 1558 de 2001.

En julio de 2010, la ley de protección de datos personales fue expedida en México, a pesar de existir desde 2002 la Ley Federal de Transparencia y Acceso a la Información Pública Federal.

41. *Íd.*, tabla 3.

42. *Íd.* Según el estudio de Remolina, solo el 20% de los países tienen normas legales al respecto.

En cuanto al Perú y Colombia, dos eventos recientes modifican su panorama legal sobre protección de datos personales.

En diciembre de 2010, el Congreso colombiano aprobó el proyecto de Ley estatutaria 046 de 2010 Cámara y 184 de 2010 Senado que regula el derecho fundamental a la protección de los datos personales, el cual se encuentra actualmente en revisión automática de constitucionalidad por parte de la Corte Constitucional. Anteriormente, se había aprobado la Ley 1266 de 2008, cuyo alcance estaba limitado a los datos personales de carácter comercial o financiero y, por otro lado, mediante la acción de tutela, el juez constitucional había regulado vía jurisprudencia varios aspectos de este derecho fundamental.

En Perú, el 7 de junio de 2011, el Congreso aprobó el proyecto de Ley N° 4079/2009-PE relativo a Protección de Datos Personales.

Tabla 2 | **Leyes sobre protección de datos personales**

País	Legislación
Chile	Ley 19628
Argentina	Ley 25326
México	Ley Federal de Transparencia y Acceso a la Información Pública Federal
Perú	Proyecto de ley N° 4079/2009-pe
Colombia	Ley 1266 de 2008 y Proyecto de Ley estatutaria 046 de 2010 Cámara y 184 de 2010 Senado

III.B. Regulación del tratamiento de datos personales en la Argentina, Colombia, México y Chile

El concepto de dato personal o de información de carácter personal cambia sutilmente en estos países; sin embargo, estos tienen como característica común la amplitud del concepto que permite, de alguna manera, concluir que un dato personal puede ser cualquier tipo de información relacionada con una persona. Así se ha definido en los países en estudio.

En la Argentina, el dato personal es «Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables» (artículo 2 de la Ley 25326). Para la legislación chilena y mexicana, dato personal se lo considera a cualquier información concerniente a personas

naturales, identificadas o identificables (artículo 2 f de la Ley 19628 y artículo 3 v de la Ley Federal mexicana). En Colombia, la Ley 1266 de 2008 define dato personal como «cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica» (artículo 2), definición que cambia en la nueva Ley Estatutaria aprobada en diciembre de 2010, pasando a ser «cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables» (artículo 3 c).

Como se puede observar, la noción de dato personal se define de manera amplia en las legislaciones estudiadas. Este concepto crucial determina tanto el alcance como el ámbito de aplicación de la protección al derecho. En ese sentido, ante una noción amplia, las existentes leyes de protección de datos se extienden en su alcance y podrían ser interpretadas respecto de todo tipo de información o dato que «pueda relacionarse» con un individuo determinado o determinable. Es decir, bajo una interpretación amplia, un dato o información se convierte en personal (y, por lo tanto, protegido) no solo cuando concierne a una persona o se relaciona con ella, sino que dicha información pueda vincularse de alguna manera con esa persona. En ese sentido, un ejercicio de interpretación podría llevar a extender la protección razonable de los datos personales (aquellos que están relacionados con la intimidad de las personas, con su privacidad) a cualquier dato que mediante distintos medios pueda relacionarse con alguien. Una interpretación en este sentido, preocupante, por cierto, puede generar mucha inseguridad jurídica y graves problemas de aplicación, particularmente al aplicarlo a Internet.

Así, el concepto de dato personal en nuestras legislaciones no tiene límites claramente determinados. En consecuencia, establecer con precisión qué se entiende por dato personal y, por lo tanto, cuál es alcance de la protección a la intimidad no es fácil de esclarecer.

Definiciones tan amplias y tan inciertas permiten llegar a debates complejos en el mundo de Internet. Como se vio anteriormente, en la navegación cotidiana, los proveedores de Internet, sea con fines técnicos, comerciales o para facilitar la este acto, recogen piezas de información. ¿Estas piezas de información son consideradas datos personales dentro de las definiciones que se establecen en nuestras legislaciones? ¿Deben considerarse datos personales y, por lo tanto, recibir protección legal especial?

La respuesta a estos interrogantes no es sencilla. Son varios puntos que pueden ser controvertidos en Internet respecto de la noción amplia de dato personal. Sin embargo, debe tenerse en cuenta que hacer extensiva la noción de dato personal a cualquier información que se recoja en la red puede ser

complicado para el funcionamiento y desarrollo en la red. Un ejemplo nos permite ilustrar esta problemática: las direcciones IP.

La dirección IP es un número único o una etiqueta numérica que permite identificar lógicamente y jerárquicamente un dispositivo (*e.g.*, una computadora), de modo que se conecta a una red que utilice el protocolo IP, lo que corresponde al nivel de red del protocolo TCP/IP. Esta puede ser estática o dinámica. La dirección IP dinámica permite identificar cuál es el ISP que tiene asignada la reserva de direcciones de la cual es parte; la dirección IP estática, por su parte, permite reconocer qué dispositivo conectado tiene asignado. Si bien las direcciones IP permiten identificar una computadora o un dispositivo, ¿pueden ser considerados datos personales? En nuestra opinión, en la medida en que no permiten distinguir a una persona directamente, no debería ser considerada un dato personal. Sin embargo, en Europa, la Agencia Española de Protección de Datos⁴³ y el Grupo del art. 29⁴⁴ sí lo han considerado dato personal, ya que el ISP «puede establecer un vínculo entre la identidad del usuario y las direcciones IP asignadas»⁴⁵. Una posición en este sentido podría hacerse extensiva a los países latinoamericanos (por la influencia evidente de la APED) y afectar el desarrollo de Internet. Esta, para su funcionamiento, requiere recoger este tipo de información en la navegación de los internautas. Sin embargo, considerarlo un dato personal exigiría extenderle todas las reglas de protección al tratamiento de la dirección IP, dato que, como máximo, permite reconocer una máquina. Esto sería desproporcionado, ya que no permite identificar a un individuo.

Este ejemplo puede trasladarse a otros temas, tales como las *cookies*, las direcciones de correo electrónico, los perfiles dentro de las redes sociales, etcétera. Esto obliga a preguntarse hasta dónde va el alcance de nuestras normas de protección de datos personales, qué es realmente lo que buscamos proteger y si una normatividad excesiva genera efectos perversos para los usuarios o consumidores y para los mercados. Estos puntos merecen una reflexión más profunda.

Del análisis realizado de manera comparativa, podemos evidenciar la profunda influencia que ha tenido la regulación europea en las legislaciones

43. Agencia Española de Protección de Datos, Informe 327/03.

44. Dictamen 2/2002 del 30 de mayo de 2002 sobre el uso de identificadores únicos en los equipos terminales de telecomunicaciones.

45. *Id.*

latinoamericanas estudiadas. Igualmente, se evidencia influencia de las guías de la OECD⁴⁶ y APEC⁴⁷ y, más recientemente, de la Resolución de Madrid de 2009⁴⁸.

III.B.I. La Argentina

La regulación de la protección de los datos personales se encuentra desarrollada a partir de una serie de principios previstos en los artículos 4 a 12 de la Ley 25326. Es importante recalcar que la regulación que ha desarrollado la Argentina le ha permitido ser considerado el único país de América Latina que la Comisión europea reconoce con un adecuado nivel de protección, lo cual fue constatado en el Dictamen 4 de 2002 y posteriormente refrendado en la decisión 30/06/2003 de la Comisión Europea. Esto le ha posibilitado a la Argentina ser el mayor destinatario de datos personales transferidos de España a países latinoamericanos⁴⁹.

Particularmente, con el fin de proteger los datos personales, este país ha desarrollado los principios de finalidad, calidad de los datos y proporcionalidad, transparencia en el tratamiento, seguridad, acceso, rectificación y oposición y restricciones a las transferencias sucesivas a terceros países.

El tratamiento y transferencia internacional de datos ha sido regulado por el artículo 12 de dicha ley, que establece como regla general que la transferencia se encuentra prohibida a otro país u organismo que no otorgue un nivel de protección adecuado, lo cual será evaluado por la Dirección Nacional de Protección de Datos, conforme lo dispone el Decreto 1581 de 2001. Se entiende, además, que el nivel adecuado de protección no solo estará condicionado a la existencia de un marco legal apropiado, sino que puede darse con la existencia de autorregulación o cláusulas contractuales⁵⁰.

46. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 de septiembre de 1980.

47. Marco de Privacidad del APEC.

48. Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, acogida favorablemente por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, España. La influencia de esta propuesta conjunta es evidente en el caso de Colombia, ya que la motivación del debate legislativo en Colombia se fundamenta en este texto (*Gaceta del Congreso* N° 1023, diciembre de 2010).

49. Remolina, *supra* nota 3, p. 504.

50. Pucinelli, Oscar, *Protección de datos de carácter personal*, Buenos Aires, Astrea, 2004.

Esta prohibición tiene como excepciones la colaboración judicial, policial y lucha antiterrorista, el intercambio de datos de carácter médico, transferencias bursátiles y bancarias, o cuando la transferencia se hubiera acordado en el marco de un tratado internacional. Igualmente, el Decreto 1581 de 2001 prevé que la prohibición de transferir datos personales a un país que no tenga el nivel adecuado de protección no opera cuando el titular del dato hubiera dado su consentimiento.

En cuanto a la recolección internacional de datos personales, la ley argentina no contiene ninguna disposición especial que regule la materia, ni tampoco contiene normas que estén dirigidas a regular el tratamiento de datos en Internet.

En lo que se refiere a la transferencia internacional de datos, la Disposición 2 de 2006 de la Dirección Nacional de Protección de Datos Personales ha determinado que esta debe realizarse dentro del siguiente marco de condiciones mínimas:

- a) identificación plena del exportador e importador (nombre, número de identificación, dirección, teléfono, fax y correo electrónico);
- b) ubicación de la base de datos y representante;
- c) precisión de las categorías y subcategorías de datos personales que se transfieran;
- d) la declaración jurada del exportador manifestando que el tratamiento de los datos que van a transferir se realiza en un total acuerdo con la Ley N° 25326;
- e) indicación de la finalidad a la que serán destinados dichos datos, de conformidad con la ley;
- f) precisión de las medidas de seguridad a las que se sujetará la transferencia y el tratamiento de datos personales;
- g) tratamiento de los datos como un todo y sin excepciones;
- h) el exportador y el importador responderán solidariamente frente a los titulares de los datos;
- i) la garantía de que el titular de los datos podrá ejercitar los derechos de acceso, rectificación, supresión y demás derechos contenidos en el capítulo III, arts. 13 al 20 de la Ley N° 25326;
- j) permitir a la Dirección Nacional de Protección de Datos Personales cumplir con sus facultades de inspección y sanciones;
- k) la obligación de destruir, y en su caso también de reintegrar al exportador, los datos personales objeto de la transferencia cuando se produzca la finalización del contrato o la imposibilidad de cumplimiento de las disposiciones de la Ley N° 25326 o la extinción de la finalidad por la que se transmitieron los mismos.

Así se puede desprender de las anteriores disposiciones la importancia sustancial que tiene en la legislación argentina el consentimiento como elemento esencial del tratamiento de los datos personales. En ese sentido, el consentimiento va a determinar el alcance del tratamiento, las finalidades de la recolección y tratamiento de los datos. Así el tratamiento de datos personales es lícito siempre que se hubiera prestado el consentimiento expreso, previo, libre e informado, y que los datos estén utilizados para las finalidades que motivaron su obtención y sobre la cual se informó al titular.

No se encuentran en la legislación argentina normas especiales sobre el derecho a la intimidad y privacidad en relación con Internet. En ese sentido, los tribunales de justicia argentinos han considerado equiparable el tratamiento que se le debe dar a estos derechos en Internet al tratamiento que se le otorga en otros medios, tales como la prensa o la televisión⁵¹; así como han considerado que puede equipararse Internet y los servicios prestados en la red con «archivos, bases de datos u otros medios técnicos de tratamientos de datos» de que trata la ley (artículo 1 de la Ley 25326, así como la definición del artículo 2 de archivo, registro, base o banco de datos), debido a la amplitud de dichos conceptos.

En este punto, es interesante analizar cómo algunos fallos judiciales argentinos han dado alcance a la ley de protección de datos personales a Internet, particularmente en relación con el acceso a información mediante buscadores. En un controversial caso (*Virginia Da Cunha contra Google y Yahoo*), una modelo y cantante demandó a dos grandes buscadores de Internet, ya que al buscar su nombre aparecían referencias a páginas pornográficas o con contenido sexual, así como la utilización comercial no autorizada de su imagen. El juez de primera instancia condenó a estas dos empresas, obligándolas a la «eliminación de las vinculaciones entre los buscadores de las demandadas y los sitios de contenido sexual, erótico y/o pornográfico que contengan el nombre, imagen y fotografías»⁵², por lo que se consideró a los buscadores de Internet responsables por permitir el acceso a dichos contenidos.

Otro caso reciente, involucra las redes sociales. En el caso *P.O. contra Facebook*, el juez de primera instancia provincial de Rafaela condenó a

51. Juzgado Nacional de Primera Instancia en lo Civil N° 75. Fallo *Da Cunha Virginia c/ Yahoo de Argentina Srl S/Daños y Perjuicios*. Buenos Aires, 29 de julio de 2009.

52. *Íd.*

Facebook ordenándole retirar los contenidos hechos públicos por un usuario en la medida en que hacía referencias calumniosas contra un político argentino. El juez consideró que la libertad de expresión se veía limitada por el derecho a la honra y buen nombre y que no permitía el trato calumnioso o injurioso⁵³.

En cuanto al primer precedente, es interesante ver cómo esta decisión judicial no afecta la fuente de la información, aquel que la hace pública, sino a los buscadores de Internet que se limitan a hacerla accesible. Estos últimos son intermediarios en la cadena de información.

En el segundo caso, la resolución judicial busca imponer cargas a la red social, igualmente intermediaria, y no a quien genera el contenido.

Estos casos, que se han repetido en varias oportunidades, dan cuenta de cómo los jueces han valorado especialmente el derecho a la intimidad por encima del derecho a la libertad de expresión⁵⁴ y determinan un precedente complejo en nuestra opinión sobre la responsabilidad de los proveedores de Internet por el contenido de sus usuarios⁵⁵. Este resultado de las decisiones judiciales no es conveniente para el desarrollo de Internet, ya que las cargas que se imponen a los proveedores de Internet son desproporcionadas y pueden implicar restricciones a la libertad de expresión y al derecho a la información. ¿Por qué se imponen restricciones a los intermediarios tecnológicos y no a quienes han creado la información y la han hecho pública? Evidentemente, hay una confusión entre tercero, intermediario y responsable que la legislación no resuelve.

53. Juzgado de Primera Instancia en lo Civil de Rafaela, Exp. N° 1113/2010 *P. O. c/ Facebook Inc. s/med. autosatisfactiva*.

54. Véanse los siguientes autos, a saber: en el Juzgado Federal de Rosario, *Treviño Susana c/ Google Argentina s/ Daños y Perjuicios*, Expte. N.° 86 630, Medidas Cautelares Innovativas; en el Juzgado Nacional de Primera Instancia en lo Civil N.° 95: *Rodríguez María Belén c/ Google Inc. s /Daños y Perjuicios*, Buenos Aires, 4 de marzo de 2010 y Rafaela, 29 de setiembre de 2010; en el Juzgado de Primera Instancia en lo Civil de Rafaela: Exp. N° 1113/2010 *P. o. c/ Facebook Inc. s/med. autosatisfactiva*; en el Juzgado Nacional en lo Civil N.° 50: *Mazza Valeria Raquel c/ Yahoo* de Argentina S.R.L. s/Medidas Precautorias*, Buenos Aires, julio de 2008.

55. Sin embargo, en agosto de 2010, el tribunal de apelación revocó la responsabilidad de Google y Yahoo en el caso de Virginia Da Cunha. La sala D de la Cámara Nacional de Apelaciones en lo Civil falló a favor de los buscadores, determinando que no son responsables por los contenidos puestos en Internet por terceros. Cámara Nacional de Apelaciones en lo Civil, sala D, D. C., v. *c/ Yahoo de Argentina S.R.L. y otro*, 10/08/2010. 2ª Instancia. Buenos Aires, 10 de agosto de 2010.

III.B.II. Colombia

El régimen jurídico colombiano sobre protección de datos personales es sumamente particular. Si bien existe una norma de carácter constitucional (artículo 15) que regula el derecho a la intimidad, a la honra y al buen nombre y que posee el *habeas data* protegido mediante la acción de tutela, durante más de diecisiete años no se expidieron normas legales que desarrollaran este derecho.

En todo este tiempo, el derecho a la intimidad y a la privacidad fue desarrollado de manera jurisprudencial, por medio de las decisiones de la Corte Constitucional, que empezaron a delimitar su núcleo esencial, de modo de definir los principios para su tratamiento y sus alcances, en particular al entrar en conflicto con otros derechos fundamentales, como el de la libertad de expresión.

Esta situación se mantuvo hasta el año 2008, momento en el que se expidió la Ley Estatutaria 1266 de 2008. Esta norma, inicialmente con pretensiones generales al ser estudiada por la Corte Constitucional, fue considerada sectorial, exclusivamente dirigida a los datos personales de carácter comercial y financiero⁵⁶.

En diciembre de 2010, se aprobó en el Congreso de la República el Proyecto de Ley Estatutaria número 146 de 2010 Cámara, 184 de 2010 Senado, por medio de la cual se dictan disposiciones generales sobre la protección de datos personales. Al ser una ley que regula y define el alcance de un derecho fundamental, siguió el trámite de ley estatutaria y, en esa medida, recibió control automático de constitucionalidad por parte de la Corte Constitucional⁵⁷. Este proyecto de ley estatutaria recoge en gran parte la doctrina desarrollada por la Corte Constitucional, en relación con el tratamiento de datos personales.

En general, podemos indicar que este proyecto sigue la tendencia del esquema europeo y con frecuencia, la finalidad de la ley es establecer un marco legal que permita a Colombia ser un país considerado por Europa con un nivel adecuado de protección de los datos personales, para, de este modo, ser un receptor de datos e información proveniente de Europa y de España en particular.

A diferencia de la Ley 1266 de 2008, este proyecto de ley tiene pretensiones mucho más amplias y generales de regulación de los datos personales.

56. Corte Constitucional, sentencia c-1011 de 2008.

57. Actualmente, el proyecto se encuentra en la Corte Constitucional, en revisión.

En lo que se refiere al tratamiento y transferencia internacional de datos, Colombia presenta un modelo sumamente proteccionista. En primer lugar, todo procesamiento de datos está sujeto al consentimiento previo, expreso e informado. Este estándar es sumamente alto y no se encuentra, ni siquiera, en los modelos europeos. En segundo lugar, de acuerdo con el artículo 26, la transferencia internacional de datos se encuentra prohibida, a excepción de que se realice a países con niveles adecuados de preservación, los cuales serán definidos por la autoridad administrativa de protección de datos personales (Superintendencia de Industria y Comercio), que, además, emitirá los certificados de adecuación.

El aporte de la jurisprudencia constitucional al desarrollo del derecho a la intimidad y a la protección de los datos personales es inmenso. En especial, como se ha explicado, por el hecho de la inexistencia de regulación en la materia. Por este hecho, la Corte Constitucional mediante los fallos de tutela, estableció las reglas para el tratamiento de datos personales, particularmente aquellos que se refieren a datos financieros o crediticios. No obstante, los principios desarrollados por la jurisprudencia se han venido incorporando tanto en la Ley 1266 como en el proyecto de ley estatutaria que se encuentra actualmente en revisión a cargo de la Corte Constitucional.

En cuanto al acceso a la información personal a través de Internet, llama la atención la prohibición que contiene el proyecto de ley estatutaria que establece que «los datos personales, salvo la información pública, no podrán estar disponibles en Internet» (artículo 4 f). Esta norma presupone que Internet es únicamente un medio de comunicación y olvida los múltiples servicios que se brindan mediante esta red, así como los otros varios derechos fundamentales que se desarrollan por su intermediación. En ese sentido, estaría prohibida la transferencia o el almacenamiento de datos mediante Internet y *cloud computing* o, incluso, la puesta a disposición de información privada, tales como hojas de vida o información personal en redes sociales. Evidentemente, la norma colombiana no está hecha para un mundo con Internet, es una legislación obsoleta. No se evidencia, lamentablemente, que en los debates legislativos el tema del desarrollo de Internet tenga alguna incidencia.

Sin embargo, en materia de información accesible en Internet y de protección de la intimidad, en un caso similar a los referenciados en la Argentina, podemos observar la diferencia en la manera en que ha decidido el juez constitucional colombiano. En el auto 371A/10 del 30 de noviembre de 2010, la Corte Constitucional decidió un recurso interpuesto por una persona que siendo víctima de violencia paramilitar, había sido parte de un proceso judicial en el que se le reconocían sus derechos. Como

consecuencia de esto, al introducir su nombre en Google, la información encontrada refería a las decisiones judiciales en las que se identificaba plenamente como víctima, por lo cual, solicitó el amparo con el fin de proteger su intimidad y su seguridad personal. La Corte Constitucional decidió proteger al accionante y ordenó retirar el nombre de la persona de las decisiones judiciales que se encontraban en Internet. La Corte, así, ordena «adoptar todas las medidas conducentes a reservar y proteger la identidad de la solicitante [...]. En consecuencia, la identidad de la señora xxxxx debe retirarse de las copias de las providencias respectivas y de cualquier otra referencia pública».

Este interesante ejemplo permite observar cómo el juez no restringe las acciones en Internet (puede entenderse que el proveedor de Internet funge como tercero intermediario y no responsable del tratamiento de datos), sino que recurre a la fuente original de la información (el tribunal de justicia que publicó la decisión judicial), y es ahí donde se toman medidas para preservar la intimidad de las personas. Este estándar utilizado por el juez colombiano nos parece más conveniente con el desarrollo de Internet, en la medida en que no impone limitaciones desproporcionadas a los proveedores de Internet (en este caso, los buscadores).

III.B.III. Chile

La Ley 19628 sobre Protección de la Vida Privada, o protección de datos de carácter personal, es la norma vigente en Chile que regula el tratamiento de datos personales en registros o bases de datos, que sean mantenidos por organismos públicos o privados. Esta ley establece la normatividad para el tratamiento de datos que incluye tanto la recolección, procesamiento y traspaso a terceros de la información personal, así como su almacenamiento. Al no existir una regla particular, esta ley regula la recolección y tratamiento de datos recogidos en Internet.

Puede afirmarse de manera general que esta ley sigue el mismo esquema de desarrollo que la directiva europea, ya que se inscribe dentro del sistema de *opt-in*. Así, el artículo 4 establece que el tratamiento de los datos personales solo podrá efectuarse cuando la ley lo autorice o cuando el titular (la persona) manifieste de manera expresa su autorización.

La ley chilena prevé la realización de una notificación o aviso de la recolección de datos personales. El artículo 5 señala que «frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de: a) la individualización del requirente; b) el motivo y el propósito y c) el tipo de datos que transmiten».

Igualmente, el consentimiento del titular debe darse de manera previa e informada respecto del «propósito del almacenamiento de sus datos personales y su posible comunicación al público» (artículo 4). La ley también reconoce los derechos de oposición, acceso y rectificación (artículos 6, 12 y ss.).

En cuanto a la transferencia internacional de datos personales, la ley no establece un patrón particular, como se puede observar en los otros países estudiados. Sin embargo, puede desprenderse que la transferencia internacional de datos, al incluirse dentro de la noción de tratamiento, se encuentra permitida en la medida en que se ajuste a lo definido en la ley para el tratamiento de datos. Vale la pena anotar que el texto original presentado a la Cámara de Diputados preveía la prohibición para dicha transferencia a países o terceros que no tengan niveles de protección similares a los chilenos, texto que no fue aprobado en el trámite legislativo.

Un punto que ha resultado controvertido dentro de la ley chilena es la ausencia de consagración del principio de finalidad en el tratamiento de datos personales, lo cual, a consideración de algunos autores, implica la ineficacia de la ley. Actualmente, se encuentra en curso un proyecto de ley para incluir el principio de finalidad dentro de la Ley 19628⁵⁸. Sin embargo, la norma en el artículo 1 dispone que «toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga [...] para las finalidades permitidas por el ordenamiento jurídico». En ese sentido, la finalidad es amplia y garantiza que el tratamiento de datos personales puede hacerse dentro de estándares lícitos, finalidades que, de conformidad con el artículo 4, se pueden enmarcar dentro de lo aceptado por el titular del dato al momento de otorgar el consentimiento (artículo 9) y de conformidad con el aviso de privacidad.

En cuanto al acceso a la información en Internet y a la privacidad, es interesante analizar el caso *NN contra la Corporación Administrativa del Poder Judicial* ante la Corte de Apelaciones de Santiago⁵⁹, en materia de datos personales accesibles por Internet. En este caso, NN solicitó amparo a su buen nombre e intimidad en la medida en que en el sitio web del Poder Judicial de Chile, al introducir su nombre en el sistema de búsquedas, aparecían individualizados sus datos personales como demandante en un

58. *Boletín* 7392-03.

59. Véase [en línea] en: <<http://www.ijlac.org/jurisprudencia/componentes.php?na me=Articulos&artid=103&idioma=spanish>>. [Nota del editor: consultada el 29/10/11.]

proceso de filiación, información que incluye su nombre y cédula, además de información sobre el reclamo de su hija de no ser reconocida por su padre. Para el tribunal, no existe vulneración de los derechos alegados por la accionante en la medida en que no se está revelando información reservada, sino información que, de acuerdo con el Código Civil, es pública por corresponder a procedimientos judiciales. Este fallo fue confirmado en apelación por la Corte Suprema.

III.B.IV. México

La ley federal sobre protección de datos personales es también una ley tardía. Expedida en 2010, surge como consecuencia de la modificación de la Constitución mexicana, que introdujo dentro de los derechos fundamentales la protección de datos personales como se vio anteriormente.

Al igual que otras leyes, la ley mexicana está basada en los principios de finalidad y consentimiento. En este punto, la ley mexicana dispone que cualquier tratamiento de datos personales (salvo las excepciones previstas) está sujeto al consentimiento del titular. Sin embargo, reconoce que existen diferentes maneras de manifestar el consentimiento y acepta que en el artículo 8 el consentimiento para el tratamiento puede darse tácitamente. Igualmente, el responsable de la administración deberá informar mediante un aviso de privacidad qué tipo de información se va a recoger y con qué finalidad (artículo 12 y ss.).

Estas disposiciones, en nuestra opinión, son convenientes para el tratamiento de datos personales en Internet. El funcionamiento cotidiano de Internet exige recoger gran cantidad de información, con el fin de que la navegación y las actividades que ahí se desarrollan puedan ejecutarse de manera óptima. En la medida en que los responsables hagan público un aviso de privacidad, el comportamiento del internauta garantiza que ha aceptado las disposiciones de dicho aviso (consentimiento tácito). Este sistema de *opt-out* es muy favorable para el desarrollo de Internet.

Este mismo estándar de protección se ve reflejado en lo que se refiere a la transferencia internacional de datos. De conformidad con el artículo 36, la transferencia internacional de datos está permitida, por lo cual, se hará de conformidad con el aviso de privacidad. Igualmente, la ley prevé varios supuestos en los cuales se permite la transferencia internacional de datos sin consentimiento del titular, eventos que son bastante más amplios de los que se encuentran en otras legislaciones de la región.

En ese sentido, la legislación mexicana parece ser una normatividad flexible, que puede adaptarse a las tendencias de Internet de una manera razonable.

En cuanto al acceso a la información personal en Internet, hay un caso reciente que merece análisis. Una persona inició un procedimiento laboral ante la autoridad competente y en la medida en que existía ese procedimiento, los datos de dicha persona eran de acceso público por estar contenidos en el Boletín Laboral. Sin embargo, al terminar el proceso, dicha persona solicitó que su información fuera eliminada del Boletín y que no pudiera ser encontrada a través de los buscadores de Internet. La autoridad laboral argumentó que la información que contiene el Boletín Laboral es de carácter público y que no es procedente hacer alteración alguna a los documentos a efecto de omitir datos que, por mandato de ley, deben encontrarse publicados, proponiendo modificar los archivos del Boletín con el fin de que no pudieran ser encontrados en un buscador y que se le solicitara a Google retirar la información de los buscadores. El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), que es la autoridad de protección de datos mexicana, revisó el recurso presentado por el particular y confirmó la acción de la autoridad laboral, decidiendo que si bien no se podía eliminar la información del Boletín Laboral, los datos personales del recurrente no podrían ser encontrados en los buscadores de Internet⁶⁰.

Esta decisión del IFAI la sitúa en un punto intermedio entre los estándares de decisión judicial vistos anteriormente. Por un lado, reconoce que la información que es pública y se encuentra en boletines oficiales no puede ser alterada, sin embargo, el archivo en el que se encuentra sí puede ser modificado por parte de la fuente de información con el fin de que el nombre de la persona afectada no pueda ser encontrado en el buscador. Además, decide solicitar al buscador de Internet que actualice la información indexada con el fin de que dentro del buscador no pueda encontrarse dicha información.

IV. Retención de datos, tensiones respecto al derecho a la intimidad

La retención (o conservación) de datos personales puede ser entendido como el almacenamiento de datos personales y registros de llamadas telefónicas e información de tráfico de Internet, incluso del contenido de

60. Instituto Federal de Acceso a la Información y Protección de Datos. Caso Junta Federal de Conciliación y Arbitraje. Expediente: 4198/09, 22 de marzo de 2011. Comisionada ponente: María Marván Laborde.

las comunicaciones, sea por entidades públicas o compañías comerciales. La custodia de datos personales puede considerarse como una forma de tratamiento de datos, de conformidad con varias legislaciones en la materia.

La mayoría de los sistemas jurídicos prevén la inviolabilidad de las comunicaciones, principio que está asociado a los mismos orígenes del Estado liberal en el siglo XVIII. Sin embargo, varios eventos recientes han servido como fundamento para que los países establezcan restricciones a este principio de la inviolabilidad de las comunicaciones y al derecho a la intimidad. A partir de los atentados terroristas del 11 de septiembre de 2001 en Nueva York, luego el del 11 de marzo de 2004 en Madrid y el 7 de julio de 2005 en Londres, las autoridades europeas y estadounidenses han considerado necesaria la retención de datos con el fin de evitar ataques terroristas y cooperar contra el delito organizado.

Estos desarrollos legales han generado grandes críticas: en primer lugar, se ha argumentado que son medidas excesivas que ponen en riesgo el derecho a la intimidad y la privacidad; en segundo lugar, se ha argumentado que son medidas desproporcionadas, ya que la afectación y la limitación a la privacidad no se compensan con la efectividad de dichas medidas. Es decir, los resultados de dichas medidas no justifican que se limite en alto grado la intimidad de las personas. Así se ha propuesto modificar el alcance de dichas acciones con el fin de encontrar un escenario más balanceado⁶¹.

IV.A Las directivas europeas 2002/58/CE, 2006/24/CE y 2009/136/CE

El Consejo Europeo incitó a las autoridades de la Unión Europea a expedir normativa que ayude a combatir el terrorismo. En esa medida, se expidió primero la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Esta norma sustituyó y derogó la Directiva 97/66/CE.

La Directiva 2002/58/CE define de manera amplia los datos de tráfico como «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación

61. Breyer, Patrick, «Telecommunications Data Retention and Human Rights», en *European Law Journal*, 11 (3 de mayo de 2005), p. 365.

de la misma» (artículo 2 b). Así, los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación; al protocolo utilizado; a la localización del equipo terminal del remitente o destinatario; a la red en que se origina o concluye la transmisión; al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación⁶².

El artículo 5 inciso 1 establece la garantía de confidencialidad de los datos de tráfico, prohibiendo el almacenamiento, intervención o vigilancia de aquellos, a excepción del almacenamiento técnico necesario para la conducción de la comunicación o que exista autorización en virtud del apartado 1 del artículo 15, el cual se refiere a la posibilidad de realizar retención de datos de tráfico, siempre que se establezcan garantías y con una finalidad limitada a la seguridad nacional⁶³. Igualmente, el artículo 6.1 fija el deber de eliminar o hacer anónimos dichos datos cuando ya no sean necesarios, a los efectos de la transmisión de una comunicación, sin perjuicio de la posibilidad de tratarlos para la facturación de los abonados (artículo 6 inciso 2); para la promoción comercial de servicios siempre y cuando el usuario haya dado su consentimiento (artículo 6 inciso 3) y la detección de fraudes (artículo 6 inciso 5).

Con posterioridad a los atentados de Madrid y Londres, las autoridades de la Unión Europea vieron la necesidad de reforzar las medidas dispuestas en la Directiva de 2002, con lo cual consideraron que la retención de datos era necesaria para la lucha criminal. En ese sentido, se expidió la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, con el objeto de modificar la Directiva 2002/58/CE. Posteriormente, esta fue modificada parcialmente por la Directiva 2009/136/CE.

El objetivo de esta directiva es que los proveedores de servicios de telecomunicaciones conserven ciertos datos con el fin de garantizar que estos

62. Considerando 15 de la Directiva Europea 2002/58/ce.

63. La restricción que establece la directiva, entre otras, es que la limitación a la confidencialidad de las comunicaciones constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa, la seguridad pública o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas.

estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves (artículo 1). El ámbito de aplicación de esta directiva cobija los datos de tráfico y de localización sobre personas físicas y jurídicas y los datos relacionados necesarios para identificar al abonado o al usuario registrado; sin embargo, no incluye el contenido de las comunicaciones (artículo 2.2). Los datos aquí referidos, de conformidad con el artículo 5, son aquellos necesarios para: 1) rastrear e identificar el origen de una comunicación; 2) identificar el destino de una comunicación; 3) identificar la fecha, hora y duración de una comunicación; 4) identificar el tipo de comunicación; 5) identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; 6) identificar la localización del equipo de comunicación móvil.

Igualmente, la directiva prevé un periodo de conservación de dichos datos no inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación.

Este modelo europeo ha sido objeto de múltiples críticas. Recientemente, el Supervisor Europeo de Protección de Datos manifestó que la directiva europea no está conforme respecto de los derechos fundamentales a la intimidad y a la protección de datos personales, comoquiera que establece medidas sumamente intrusivas y no se ha demostrado la necesidad de realizar esta retención de datos⁶⁴.

IV.B. Los Estados Unidos de América

En Estados Unidos, la retención de datos se encuentra reglada por varias leyes federales. En primer lugar, está la Ley de Protección de la Privacidad en la Comunicaciones Electrónicas o *Electronic Communication Privacy Act* (ECPA) de 1986. Esta norma protege las comunicaciones alámbricas e inalámbricas imponiendo condiciones para la interceptación de comunicaciones. En este sentido, exige que para acceder a información

64. Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 de mayo de 2011, véase [en línea] en: <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf>. [Nota del editor: consultada el 29/10/11.]

conservada o retenida por los operadores de comunicaciones electrónicas se requiere una orden judicial. Posteriormente, se expidió la *USA PATRIOT Act*, que modificó en varios aspectos la ECPA, la que permitía que el FBI, mediante Cartas de Seguridad Nacional (*National Security Letters*, NSL), requiriera a los ISP información de sus usuarios sin control judicial. Esta sección de la ECPA (sección 2709) fue declarada inconstitucional bajo la primera y cuarta enmienda de la Constitución en el fallo de *ACLU contra Ashcroft* de 2004 de la Corte Federal del distrito de Nueva York⁶⁵.

También la Ley sobre Protección a la Privacidad y Registro Telefónicos de 2006 (*Telephone Records and Privacy Protection Act*) prohíbe engañar con el objeto de vender, comprar u obtener registros personales telefónicos excepto cuando es realizado por agencias policiales o de inteligencia, e incluye penas hasta de diez por entregar información confidencial sobre sus usuarios.

Por otro lado, la Ley SAFETY (*Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act*) de 2009 exige a los proveedores de comunicaciones electrónicas o servicios de computación remota a retener durante un periodo de hasta dos años todos los registros y cualquier información pertinente para identificar al usuario de una dirección de red temporal que el proveedor de servicio haya asignado.

Por último, la Ley CALEA (*Under the Communications Assistance for Law Enforcement Act*), de 1995, exige a los proveedores de servicios de Internet y telecomunicaciones que permitan a las agencias de policía interceptar y retener datos de sus usuarios.

IV.C. América Latina

En cuanto a la retención o conservación de datos personales en América Latina, no encontramos una normativa similar a la directiva existente en Europa sobre retención de datos personales. Se puede observar que las legislaciones latinoamericanas en general tienen marcos legales que regulan la intervención en las comunicaciones (especialmente telefonía) cuando exista una medida judicial previa.

65. *American Civil Liberties Union v. Ashcroft*, 2004. Véase [en línea] en: <http://www.aclu.org/FilesPDFs/nsl_decision.pdf>. [Nota del editor: consultada el 29/10/11.]

Sin embargo, cada país tiene reglas particulares que determinan algunas obligaciones de conservación de información, especialmente en lo referente a la información crediticia y financiera y a las obligaciones de los bancos de datos referidos a este tipo de información y sus reportes. Esto se debe, en gran medida, a que en la mayoría de los países de América Latina no se han dado hechos terroristas de dicha magnitud que hayan obligado a estos países a establecer límites especiales para la conservación de registros telefónicos e información de tráfico de Internet que posibilite a las autoridades de policía acceder a dicha información.

Sin embargo, vale la pena detenernos en unos puntos concretos de análisis de las experiencias de nuestra región.

Aunque en Colombia no existe una ley que específicamente regule la retención de datos, la jurisprudencia constitucional ha establecido en materia de conservación de datos personales la noción de derecho al olvido o caducidad del dato personal. En esta medida, la Corte Constitucional ha dicho que

se han establecido (...) unos límites a la permanencia del dato en los archivos [...]. A juicio de esta Corporación, la mala conducta comercial pasada no debe ser mantenida en el archivo a perpetuidad. Sin embargo, un límite de los datos en el tiempo debe armonizarse con la necesidad de información sobre el comportamiento comercial que permita a las instituciones financieras calcular sus riesgos⁶⁶.

Igualmente, la Corte Constitucional ha reconocido que la competencia para establecer las limitaciones a la permanencia de datos personales en bases de datos y archivos corresponde al legislador y, así, esto solo ha sido desarrollado por la Ley 1266 de 2008, relativa a los datos de carácter personal financieros, crediticios, comerciales y de servicios.

Esta ley establece en su artículo 13 que

[l]a información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información. Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera y, en general, aquellos datos

66. Corte Constitucional, Sentencia T-176 de 1995, Magistrado Ponente: Nelson Cifuentes Muñoz.

referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida.

Al respecto de esta norma, la Corte Constitucional la declaró exequible condicionada «en el entendido [de] que la caducidad del dato financiero, en caso de mora inferior a dos años, no podrá exceder el doble de la mora, y que el término de permanencia de cuatro años también se contará a partir del momento en que se extinga la obligación por cualquier modo»⁶⁷.

El actual proyecto de ley estatutaria que se encuentra bajo revisión de la Corte Constitucional no tiene previsiones al respecto de la retención de datos, salvo que esta deba ajustarse a los principios de finalidad y libertad.

Otro caso interesante en Colombia es el referente a la Ley 633 de 2000, que establece en el artículo 91 que

[t]odas las páginas web y los sitios de Internet de origen colombiano que operan en el Internet y cuya actividad económica sea de carácter comercial, financiera o de prestación de servicios deberán inscribirse en el registro mercantil y suministrar a la Dirección de Impuestos y Aduanas Nacionales, DIAN, la información de transacciones económicas en los términos que esta entidad lo requiera.

Esta norma fue demandada ante la Corte Constitucional que decidió declararla exequible condicionada a que la información que puede requerir la DIAN es la directamente relevante y estrictamente necesaria para el cumplimiento de sus funciones en ejercicio de sus competencias legales⁶⁸.

En la Argentina, existe un caso interesante: la Ley 25873, que establecía la obligación de los prestadores de servicio de telecomunicaciones para retener ciertos datos personales por un plazo determinado. Esta ley

67. Corte Constitucional, Sentencia c-1011 de 2008, Magistrado Ponente: Jaime Córdoba Triviño.

68. Corte Constitucional, sentencia c-1147/01 del 31 de octubre de 2001.

modificaba la Ley 19798, con el objeto de introducir obligaciones a los operadores de telecomunicaciones, incluidos los proveedores de Internet: (1) los operadores de telecomunicaciones deben disponer, a su cargo, de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten para su observación remota a requerimiento de las autoridades competentes; (2) los operadores de telecomunicaciones deben registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y registros de tráfico de comunicaciones cursadas por ellos para consulta de las autoridades competentes y (3) los operadores de telecomunicaciones deben conservar por diez años la información personal recolectada.

Esta ley fue altamente cuestionada, ya que se consideró que lesionaba derechos fundamentales. Estos cuestionamientos fueron llevados ante las instancias judiciales correspondientes y en el caso *Halabi, Ernesto c/ Poder Ejecutivo Nacional*, la Corte Suprema de Justicia de la Nación declaró que los artículos 1 y 2 de esa ley y el decreto reglamentario 1563/04 eran inconstitucionales, pues

las comunicaciones a las que se refiere la Ley 25873 y todo lo que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional. El derecho a la intimidad y la garantía consecuente contra su lesión actúan contra toda «injerencia» o «intromisión» «arbitraria» o «abusiva» en la «vida privada» de los afectados [...].

Es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet, en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Se añade a ello la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales⁶⁹.

69. Fallo *Halabi c/ PEN*. Corte Suprema de Justicia de la Nación, 26 de junio de 2007.

En México, en materia de retención de datos personales, además de las normas que existen para protección de datos personales, encontramos la Ley de Seguridad Nacional⁷⁰, que establece que en los casos de inminente amenaza a la seguridad nacional, el Gobierno podrá hacer uso de los recursos que legalmente se encuentren a su alcance, incluyendo la información anónima (artículo 33), así como la posibilidad de intervenir comunicaciones privadas de cualquier tipo previa autorización judicial (artículo 34). La ley especifica que intervenir comunicaciones incluye la grabación y registro de la información. El artículo 42 de la ley especifica que los datos que se obtengan por la intervención de comunicaciones deben ser considerados información reservada. En la ley, no se encuentra una disposición relativa al tiempo máximo de conservación de la información recogida.

Otro interesante caso de recolección y retención de datos personales en México es el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT), el cual es un registro en el que se concentran los usuarios de telefonía móvil a través de la asociación del número de su línea telefónica móvil y su CURP, mecanismo establecido en el decreto del 9 de febrero de 2009. Esta disposición permite llevar un registro preciso sobre los usuarios de teléfonos móviles, con la debida protección de privacidad de los datos. El objetivo es conservar datos de tráfico y localización de las llamadas telefónicas, por lo que el registro inscribe los siguientes datos⁷¹: 1) tipo de comunicación, servicios suplementarios, de mensajería o multimedia empleados; 2) datos necesarios para rastrear origen y destino de las comunicaciones; 3) datos necesarios para determinar fecha, hora y duración de la comunicación; 4) fecha y hora de la primera activación del servicio y etiqueta de localización desde la que se haya activado el servicio y 5) ubicación digital del posicionamiento geográfico de las líneas telefónicas.

70. Ley de Seguridad Nacional, publicada el 31 de enero de 2005.

71. Del Conde Ugarte, Alejandro. *La seguridad y privacidad en el marco de las telecomunicaciones*. Seminario Iberoamericano de Protección de Datos «Nuevas Tecnologías, Seguridad y Privacidad». 2010. Disponible [en línea] en: <http://www.redipd.org/reuniones/seminario_2010_cartagena/common/Alejandro_CondeADCU_Proteccion_Datos_telecomunicaciones_Cartagena_julio_2010.pdf>. [Nota del editor: consultada el 29/10/11.]

V. Conclusiones y recomendaciones

América Latina ha estado altamente influenciada por la normativa europea de protección de datos personales, particularmente con la intención de adecuar su normativa a dichos estándares y así poder ser considerada como legislación con nivel adecuado de protección. Esto ha llevado a que en los últimos once años, la mayoría de los países latinoamericanos hayan pasado de un modelo de *habeas data* a legislaciones generales de protección de datos muy estrictas (especialmente las legislaciones colombiana y peruana).

A nivel regional, no se han encontrado proyectos puntuales de normativa estandarizada para los países latinoamericanos. Sin embargo, vale la pena traer a colación la reciente recomendación del Comité de Asuntos Jurídicos de la Organización de Estados Americanos⁷². Este documento busca ser una guía para los Estados miembros de la OEA para desarrollar sus legislaciones nacionales. Este documento parte de un estudio de las tendencias legislativas actuales con el fin de adecuar las normatividades de protección de datos personales a los restos de las nuevas tecnologías y se sitúa en un punto medio entre el modelo europeo y el de los Estados Unidos. Esta recomendación parte de una serie de principios que buscan regular el tratamiento de datos personales (finalidad, consentimiento, calidad, legalidad, etcétera), así como reglas para la transferencia internacional de datos. Particularmente, se evidencia la preocupación de la OEA por establecer reglas claras y uniformes en cuanto al flujo trasfronterizo de datos que permitan el desarrollo de negocios de Internet, a la vez que se garantizan estándares mínimos de protección de los datos personales. No obstante, estas son simples recomendaciones sin un valor jurídico concreto para los países miembros.

Así, más allá de esta iniciativa de la OEA, no se observa que en el corto o mediano plazo existan iniciativas regionales de armonización de la protección de datos.

En general, se observa una tendencia de las legislaciones latinoamericanas a establecer estándares de protección bastante altos (la Argentina, Colombia, el Perú) siguiendo el patrón europeo. Sin embargo, sería altamente recomendable que, teniendo en cuenta la dinámica y los retos de Internet,

72. Organización de Estados Americanos. Comisión de Asuntos Jurídicos y Políticos. «Draft preliminary principles and recommendations on data protection», 19 de noviembre de 2010. CP/CAJP-2921/10.

las legislaciones nacionales de los países de América Latina se tornaran más flexibles con el fin de reconocer este fenómeno y acomodarse a los desafíos que se avecinan. Como se ha visto anteriormente, la protección de los datos personales es un derecho fundamental que requiere de protección, pero esta debe ser razonable, flexible y proporcionada. Por ejemplo, la nueva ley colombiana establece que solo se podrá transferir datos a países que tengan niveles similares de protección. Sin embargo, los estándares de protección establecidos en la normatividad colombiana son más altos que, incluso, los niveles europeos y de los Estados Unidos. Esto presentará problemas al momento de hacer operativa la legislación de protección de datos.

Igualmente, es necesario que en los debates latinoamericanos se analicen los retos que impone Internet a la privacidad de las personas. Las discusiones que se realizan en torno a la privacidad en América Latina siguen girando alrededor de los temas tradicionales, especialmente lo relativo a la información crediticia y financiera. Llama la atención cómo la problemática de Internet no fue un punto de discusión en los procedimientos legislativos que se dieron muy recientemente en América Latina en los últimos seis meses: ni en el Perú ni en Colombia se encuentran en los debates legislativos análisis sobre el impacto de Internet en la privacidad y la manera en que las legislaciones latinoamericanas deberían abordar la protección de los datos personales en la actualidad en un mundo globalizado. Podría decirse que nuestras legislaciones tienen una tendencia local que no es compatible plenamente con los retos que impone Internet ni la globalización.

En este escenario, se vislumbra un protagonismo de los jueces que deberán aplicar en casos concretos las normas de protección de datos a situaciones en las que esté involucrada Internet, a partir del ejercicio de los recursos de *habeas data* (sea como acción especial o acción de tutela o amparo) previstos en las constituciones latinoamericanas. En este punto, se ha visto en la Argentina cómo mediante varias acciones judiciales se han tratado de imponer estándares de protección a la intimidad en Internet, particularmente restringiendo los buscadores y el ejercicio de la libertad de expresión en redes sociales. Este punto sensible, en el que se ponderan el ejercicio del derecho a la privacidad con otros derechos que se ejercen en la red (derecho a la información, libertad de expresión, etcétera), además de realidades técnicas y comerciales, no siempre son analizadas en profundidad por los jueces. Es rescatable la manera como el juez constitucional colombiano aborda la restricción al acceso a la información en Internet, imponiendo la carga de proteger el derecho a la intimidad de la fuente y no al intermediario de Internet que indexa la información disponible en la red.

Igualmente, se observa una tendencia al fortalecimiento de autoridades especiales para la protección de datos personales como parte de las políticas locales, siguiendo igualmente la tendencia europea. En este punto, cohabitarán estos sistemas de protección (judicial y administrativo), de modo que deberán tomar decisiones sobre privacidad en Internet a partir del marco legal existente. Este modelo de las entidades administrativas de protección de datos todavía es incipiente en América Latina y será menester monitorear su evolución.

En nuestra opinión, sería recomendable por lo tanto que los países latinoamericanos trabajaran en una política conjunta que permitiera establecer estándares de protección razonables adecuados a las problemáticas contemporáneas de privacidad y que garantizaran un marco regulatorio flexible que permita responder a los retos de Internet.

Por otro lado, consideramos necesario que en nuestros países se analice realmente el alcance de la protección a la intimidad y privacidad que debe otorgarse y cómo debe ponderarse dicho derecho con el ejercicio de otros derechos fundamentales, tales como el derecho a la libertad de expresión y de información. Es importante que el Estado se pregunte realmente qué tanto valoran las personas sus «datos personales» y si el nivel de protección debe extenderse de igual manera a todo lo que pueda ser considerado «dato personal». Ante definiciones amplias e indeterminadas de la noción de dato personal establecidas en las legislaciones regionales, se puede llegar a incluir dentro de este concepto informaciones que poco tienen que ver realmente con la intimidad y la vida privada de las personas. En ese sentido, debe volverse a una noción de derecho que proteja lo que está realmente asociado a la vida privada de las personas, como, por ejemplo, cierta información sensible o reservada. No obstante, extender las protecciones constitucionales a todo tipo de información que pueda asociarse o vincularse con una persona no es adecuado y puede restringir injustificadamente el ejercicio de otros derechos.

Como se vio anteriormente, una proporción importante de personas no valoran todos sus datos personales de la misma manera. Muchas están dispuestas a hacer pública su información, sus gustos, sus creencias, sus fotos⁷³, y no debería ser el Estado el que restrinja el ejercicio que hacen

73. Existen más de catorce millones de usuarios de Facebook en Colombia (a junio de 2011); veintiséis millones en México; veinte millones en Brasil y quince millones trescientos mil en la Argentina. Véase [en línea] en: <www.facebookcolombia.com>. [Nota del editor: consultada el 29/10/11.]

las personas de sus derechos. En ese sentido, un modelo de tratamiento de datos personales debería estar sujeto a un ejercicio de consentimiento tácito soportado por un aviso de privacidad (caso México) y no al consentimiento expreso (casos Colombia, la Argentina y Chile) para cualquier dato personal.

En cuanto al flujo transfronterizo de datos, que impacta sustancialmente sobre el desarrollo del *cloud computing* y otros servicios de Internet, se pueden identificar dos modelos en la región: un modelo que permite la transferencia internacional de datos (con excepciones) y otro modelo que no lo permite (con excepciones). Dentro del primer modelo, se encuentran México y Chile; dentro del segundo, Colombia y la Argentina. En el primero, la transferencia de datos es un aspecto positivo que debe darse bajo ciertas condiciones; en el segundo, la visión es negativa («se prohíbe la transferencia de datos de cualquier tipo...»). En nuestra opinión, teniendo en cuenta el impacto creciente de los procesos de *cloud computing* y de otros fenómenos asociados a la globalización (como la tercerización de servicios o el *offshoring*), consideramos que las legislaciones de la región deben estar abiertas a la transferencia internacional de datos, estableciendo condiciones mínimas de protección (no restringiéndolo exclusivamente a países con similar o mayor protección que la otorgada) e, incluso, contractuales. Sin embargo, hay que considerar que dado que el fenómeno rebasa las fronteras y las jurisdicciones nacionales, no puede ser controlado exclusivamente mediante leyes nacionales. En ese sentido, sería recomendable que los países de la región iniciaran procedimientos multilaterales que permitieran establecer estándares comunes de protección de datos basados en el principio de *accountability*, siguiendo la recomendación del borrador de recomendaciones de la OEA. Este se encuentra en el principio 5 y establece: «*The data controller is responsible for taking all the necessary steps to follow personal data processing measures imposed by national legislation and other applicable authority*» (*El controlador de datos es responsable de tomar todas las medidas necesarias para seguir el tratamiento de datos personales impuestas por la legislación nacional y la autoridad de aplicación*).

Finalmente, al igual que la tecnología impone retos, también provee soluciones. En la actualidad, existen herramientas tecnológicas que permiten disminuir la recolección de datos no deseada, así como mecanismos que permiten garantizar la privacidad (software que permite *anonimizar* la información personal, que limita el seguimiento de datos y controla el spyware, software antivirus, mecanismos de encriptación de

comunicaciones, etcétera). En esa medida, las personas pueden definir los niveles de protección que esperan obtener utilizando estas herramientas y decidiendo sobre la utilización de su información por terceros.

Esto implica, además, la posibilidad de abrir espacios y escenarios de autorregulación de las industrias, en las cuales los actores privados puedan definir estándares de protección, en lugar de esperar exclusivamente la protección estatal restrictiva (*e.g., privacy by design*).

Evidentemente, Internet y las nuevas tecnologías traen gran cantidad de retos que debe afrontar el derecho. Igualmente, esto le exige presentar soluciones actuales, novedosas y que favorezcan el desarrollo de estas nuevas tecnologías, de modo de garantizar la innovación sin menoscabar derechos fundamentales como la libertad de expresión, la libertad de información o el derecho a la intimidad y la vida privada. Este estudio no pretende abarcar todos los problemas jurídicos que plantea Internet en relación con la protección de datos personales ni tener las soluciones; busca abrir un camino, sembrar preguntas y analizar con sentido crítico la respuesta de algunos ordenamientos jurídicos.

Protección de datos personales y prestación de servicios en línea en América Latina¹

Alberto J. Cerda Silva

Introducción

Cuando el Gobierno de Chile anunció que monitorearía las redes sociales que operan en línea, tales como MySpace y Twitter, generó tan amplio rechazo ciudadano que se vio obligado a desechar la iniciativa. Desde el momento en el que Facebook modificó unilateralmente sus políticas de privacidad, con lo que dejaba al descubierto la participación de ciudadanos iraníes en grupos antigubernamentales, organismos de seguridad del Gobierno adoptaron medidas represivas contra esos usuarios y sus familiares. A partir de que el Gobierno de Venezuela publicó en Internet el listado de adherentes a una solicitud de referendo nacional, generó persecución cruzada entre sus partidarios y opositores. Con sus bemoles, cada uno de los casos recién reseñados deja en evidencia cómo la adecuada protección de los datos personales es una garantía para el ejercicio de la libertad de expresión y demás derechos fundamentales, así como el rol crítico que Internet tiene hoy en la preservación de esos derechos.

1. Este ensayo recoge con cierta coherencia la intervención del autor en el taller Libertad de Expresión e Internet: aspectos de regulación en América Latina, organizado por el Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo, que tuvo lugar en la ciudad de Buenos Aires los días 12 y 13 de septiembre de 2011. El autor desea expresar su profundo agradecimiento por la invitación extendida para ser parte de dicho evento.

La protección de los datos personales satisface fines de interés público inherentes a una sociedad democrática. Dicha protección no solo evacúa la necesidad individual de quien quiere excluirse de la vida social, sino que también actúa como salvaguarda para el libre ejercicio de sus derechos. Así, por ejemplo, al imponer limitaciones al tratamiento de datos relativos a nuestras opciones políticas, religiosas o sexuales, se fortalece el libre ejercicio del derecho de asociación, de la libertad de pensamiento y de la autodeterminación sexual, entre otros. En verdad, la posibilidad de excluirse de la sociedad en sus diversas vertientes jurídicas —llámese inviolabilidad del hogar y de las comunicaciones, derecho a la vida privada, derecho a la protección de los datos personales e, incluso, el derecho al voto secreto— preserva un espacio para la libre expresión y la plena realización de la personalidad, un objetivo propio del orden democrático.

Recientemente, una serie de argumentos han sido esbozados con el propósito de erosionar el derecho a la protección de los datos personales. Se ha sostenido que tal preservación debería estar circunscrita únicamente a la información que reviste carácter privado. Se ha dicho que el concepto de dato personal es excesivamente amplio, lo que genera incertidumbre jurídica. Se ha afirmado, también, que el simple consentimiento de las personas es suficiente para legitimar el procesamiento de información que les concierne, sin más. Para ser franco, dichos argumentos no son resultado de una preocupación en torno a la libertad de expresión, sino del afán de disponer de un entorno legal más proclive al tráfico inmune e impune de la información personal.

Los argumentos tendentes a socavar una protección adecuada a los datos personales han sido especialmente oficiosos cuando se los aplica a Internet; de hecho, han sido enarbolados con el propósito de brindar mayor flexibilidad a la prestación de servicios en línea; basta traer a colación algunos casos de los años recientes, tales como la publicidad contextual y las vistas callejeras de Google, los sistemas de localización geográfica de Apple, la modificación unilateral de políticas de privacidad de Facebook y el pasaporte de identificación en línea de Microsoft. Frente a ellos, las autoridades europeas en materia de protección de datos han reaccionado enérgicamente y, como era previsible, la progresiva adopción de medidas similares en América Latina suscita preocupación entre los prestadores de servicios en línea.

Este ensayo controvierte las líneas de argumentación por medio de las cuales se intenta mermar la obtención de un adecuado nivel de resguardo al derecho a la protección de los datos personales. La primera sección

se extiende sobre la verdadera naturaleza del bien jurídico protegido, rechazando que este sea solamente el derecho a la vida privada. La segunda sección impugna la acusación de que la legislación latinoamericana en la materia sea excesivamente proteccionista al conceptualizar qué es un dato personal. La tercera sección enfatiza acerca de que el simple consentimiento no es suficiente a los efectos de legitimar el tratamiento de información personal. La cuarta sección intenta develar el propósito ulterior de dichos argumentos y, en contrapartida, expresa su preocupación por el rol que los prestadores de servicios en línea tienen en la retención de datos en América Latina. Unos breves comentarios y conclusiones ponen fin al texto.

I. La protección de los datos personales como derecho autónomo

La legislación sobre protección de los datos personales se desarrolla a partir de la década de los setenta, como una reacción al creciente poder que las tecnologías proveen para procesar información personal y, consiguientemente, emplear esta para fines ilegítimos de control social por el Gobierno. Progresivamente, el ámbito de aplicación de dicha normativa se extendió a efectos de brindar una protección integral. Así, para evitar la elusión de la ley, en especial en áreas sensibles como el tratamiento de datos en el sector de la salud, renuente a la automatización y afincado en la cultura del papel, el ámbito de aplicación se extendió también al tratamiento manual de datos. Del mismo modo, a medida que las tecnologías estuvieron disponibles no solo para servicios gubernamentales, sino, también, para empresas y entidades del sector privado, la legislación extendió la protección de las personas al tratamiento de datos efectuados por estas. Así, hoy tenemos una legislación comprensiva, que brinda protección a las personas en relación con el tratamiento de sus datos, ya sea por medios manuales o automatizados, por el sector público y privado.

La legislación sobre protección de datos se articuló inicialmente en torno al derecho a la vida privada como bien jurídico. En parte, porque la preocupación central era resguardar la información personal, especialmente aquella sensible atinente a una esfera íntima, frente a su potencial mal uso. Y en parte, porque el desarrollo conceptual no encontraba otro bien jurídico más apropiado para sustentar la protección. Así, tal como en la obra de Warren y Brandeis, el derecho de propiedad sirvió de fundamento al derecho a la vida privada, este lo fue del derecho a la protección de los datos personales. Sin embargo, en la tradición del derecho continental de

la cual América Latina es parte, tanto el derecho a la vida privada como el derecho a la protección de los datos personales son categorías jurídicas claramente diferenciadas.

El derecho a la protección de los datos personales cobró autonomía propia a comienzos de la década de los ochenta. En 1983, el Tribunal Constitucional Federal Alemán, el cual ha sido especialmente acucioso en el control de las leyes que confieren poder al Gobierno para tratar información personal, declaró la inconstitucionalidad de la Ley de Censo, sosteniendo que «...el derecho general de la personalidad... abarca... la facultad del individuo, derivada de la idea de autodeterminación, de decidir, básicamente por sí mismo, cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida». Lo propio fue reconocido también por el Tribunal Constitucional de España en 1998, cuando identificó «un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona..., pertenezcan o no al ámbito más estricto de la intimidad, para, así, preservar el pleno ejercicio de sus derechos». Entonces, este derecho, conocido en doctrina como *autodeterminación informativa* o *libertad informativa*, faculta a las personas para controlar la información que les concierne, siendo irrelevante a efectos de su protección si dicha información es privada o pública.

En Europa, el derecho a la protección de los datos personales también ha tenido recepción normativa. De hecho, diversas cartas constitucionales han reconocido aquel como un derecho diferenciado del derecho a la vida privada. Todavía más, la Carta de Derechos Fundamentales de la Unión Europea, adoptada el 7 de diciembre de 2000, hace un claro distinguo. Así, tras reconocer en su artículo 7 el derecho a la vida privada, su artículo 8 reconoce que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan», y luego fija las exigencias mínimas impuestas al adecuado respecto de este derecho desde la perspectiva de los derechos humanos.

En América Latina, el derecho a la protección de los datos personales también ha tenido reconocimiento constitucional. En general, las constituciones de la región reconocen no solo el derecho a la vida privada, sino, también, el denominado *habeas data*, que no es más que el derecho a la protección de los datos personales. Esto último acontece, con diferentes matices, en las constituciones de la Argentina, Brasil, Colombia, México, el Perú, y Venezuela. Incluso en aquellos países en que la confusión conceptual aún persiste en el texto constitucional, esta ha sido superada por sus cortes constitucionales, las cuales reconocen el derecho a controlar la información

personal; así, recientemente, el Tribunal Constitucional de Chile reconoció expresamente el derecho a la autodeterminación informativa, pese a no estar explícito en la Constitución, al declarar la inconstitucionalidad de la ley que obligaba a los cibercafés a llevar registro de sus usuarios para fines de persecución penal.

Comparativamente, el constitucionalismo latinoamericano ha sido más eficiente en la salvaguarda del derecho a la protección de los datos personales. Primero, reconociéndolo como un derecho autónomo. Segundo, proveyéndolo de acciones constitucionales para su protección, ya sea a través de la *acción de amparo* –conocida como *acción de tutela* en Colombia; *recurso de protección* en Chile; y *mandado de segurança* en Brasil–, o bien, de una acción específica también denominada de *habeas data*. Tercero, a diferencia del constitucionalismo estadounidense y con mayor énfasis que el europeo, las cartas magnas de América Latina reconocen derechos y establecen procedimientos judiciales para su protección, no solo respecto del sector público, sino, también, respecto del sector privado. Así, pese a carecer de leyes especiales en la materia en diversos países de la región, el derecho a la protección de los datos personales ha tenido lugar en la sede constitucional, tanto cuando el Gobierno trata información personal como cuando empresas de telecomunicaciones o prestadores de servicio de reportes crediticios tratan datos personales con infracción a los derechos fundamentales reconocidos por la Constitución.

Sin embargo, la normativa constitucional no ha sido suficiente para garantizar un adecuado nivel de protección de los datos personales en América Latina. Esto sucede porque dicho resguardo se verifica preferentemente en sede judicial y ello trae aparejado una serie de limitaciones, tales como sus altos costos transaccionales; su ineficacia para prevenir infracciones y su falta de experiencia en temas que, en ocasiones, resultan altamente técnicos. Además, como en los demás países depositarios de la tradición del derecho civil, en los países latinoamericanos, los precedentes judiciales carecen de fuerza obligatoria en casos futuros, salvo limitadísimas excepciones. Así, en la práctica, ello obliga a (re)iniciar acciones judiciales individuales a cada uno de los titulares de datos personales afectados por un ilegítimo tratamiento de esos, efectuados, por ejemplo, por Equifax o algunas de sus filiales locales al emitir reportes de crédito.

Los preceptos constitucionales resultan aún demasiado generales y admiten un amplio margen de interpretación. En efecto, siguiendo a Robert Alexy, las disposiciones constitucionales establecen principios cuya aplicación al caso concreto puede redundar en reglas equívocas

o ambiguas. Así ha sucedido con el denominado *derecho al olvido*, en relación con el tratamiento de datos personales relativo a deudas incluso después de verificado su pago. Mientras para las Cortes Supremas de la Argentina y Costa Rica el tratamiento de datos sobre deudas pagadas infringe los derechos fundamentales, la Corte Suprema de El Salvador, frente a análogos preceptos constitucionales, ha determinado exactamente lo contrario. Esto pone en evidencia que la protección basada en puros preceptos constitucionales resulta en ocasiones insuficiente e introduce incertidumbre jurídica, tanto entre los titulares de datos personales como entre quienes los tratan.

América Latina está adoptando leyes que reglamentan el tratamiento de datos personales de un modo integral, esto es, en las que sea comprendido el procesamiento de información tanto por el sector público como por el privado. Diversas razones explican este fenómeno: los nuevos bríos democráticos, que invitan a brindar adecuada protección a los derechos de las personas; el afán de minimizar la incertidumbre de un modelo de protección basado solo en disposiciones constitucionales; pero más significativamente, la aspiración de transformarse en un país que brinda un nivel de protección adecuado, de acuerdo con los estándares promovidos por la Unión Europea, a efectos de acceder a la transferencia de datos personales desde esta y, con ello, facilitar la inversión en aquellos nichos de mercado que suponen tratamiento de datos provenientes de aquella. Así, al temprano reconocimiento de la Argentina como país seguro, se suma el inminente de Uruguay; en tanto, Colombia, Costa Rica, México y el Perú han modificado recientemente su legislación interna para tales efectos; mientras, Brasil y Chile cuentan ya con iniciativas legislativas en la materia.

El modelo latinoamericano de protección de datos personales está en un estadio de transición. Años atrás, se verificaba a través de disposiciones constitucionales, a las cuales se incorporaba un mayor o menor número de leyes, lo que hacía de ella una regulación fragmentaria y, en ocasiones, inconsistente. Hoy, en las principales economías de la región, esta protección constitucional se traslapa con una norma general que reglamenta el tratamiento de la información personal, sea o no privada. Como resultado de esa superposición de medidas constitucionales y legales, la protección de los datos personales aparece robustecida en América Latina, si bien aún resta fortalecer el efectivo cumplimiento de la ley.

Limitar la protección de los datos personales a aquellos que conciernen a la vida privada es, entonces, un error en lo tocante a la determinación del

bien jurídico protegido. Sostener que la protección de los datos personales debe limitarse a la información privada implica un desconocimiento del desarrollo histórico del amparo, con un argumento que retrotrae el desarrollo doctrinario y jurisprudencial más de treinta años. Además, introduce serias dificultades para fijar los límites de la protección, dada la multiplicidad de teorías respecto de qué se entiende por privado, un tópico sobre el cual se ha escrito bastante y cuyo análisis excede los propósitos de este ensayo. Pero aún más, limitar hoy la protección a la vida privada, junto con precarizar la protección de las personas, generaría un enorme retroceso en la armonización normativa internacional, un costo bastante elevado de cara a los efectos de la globalización. En cambio, el derecho a la protección de los datos personales garantiza a las personas el control sobre la información que les concierne, independientemente de su conexión con la vida privada, aspecto que, de hecho, se soslaya.

Naturalmente, sostener que el derecho a la protección de los datos personales resguarda más que la vida privada no obsta brindar un plus de protección a aquella información que devela aspectos particularmente íntimos de las personas. Precisamente, esto se logra por medio del establecimiento de una protección reforzada para los denominados *datos sensible*. Estos son aquellos datos que revelan información merecedora de especial resguardo por el mayor peligro que su tratamiento implica para las libertades y derechos ciudadanos. De acuerdo con los *Principios rectores para la reglamentación de los ficheros computarizados de datos personales*, adoptados por las Naciones Unidas (1990), estos datos pueden originar una discriminación ilícita o arbitraria. Entre estos se cuentan los datos relativos al origen racial o étnico de una persona, su color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, así como sobre la participación en una asociación o la afiliación a un sindicato. Algunos países, según su propia experiencia, agregan la información genética, la afiliación política u otros datos a este listado. Todos los países latinoamericanos que disponen de leyes en esta materia fijan normas que brindan una protección reforzada a los datos sensibles.

En suma, aun cuando existe algún traslape entre el derecho a la vida privada y el derecho a la protección de los datos personales, este último tiene una entidad autónoma, mediante el cual se garantiza a toda persona el derecho a controlar la información que le concierne, independientemente de si es pública o privada. Sostener lo contrario implica un serio retroceso en materia de derechos fundamentales en general y de protección de datos en particular.

II. La apropiada extensión del concepto *dato personal*

Una segunda línea de argumentación que intenta mermar la protección de los datos personales en América Latina asegura que aquellos países que han adoptado leyes sobre la materia yerran al extender de forma excesiva la protección no solo a los datos relativos a personas identificadas, sino, también, a aquellas que resulten identificables. Esto implica que no solamente quedan afectos a la ley el tratamiento de los datos asociados a una persona inequívocamente individualizada, sino, también, el de aquellos datos correspondientes a una persona no identificada pero susceptible de serlo. Este sería el caso, por ejemplo, de los datos personales asociados al rol único tributario en Chile; del número de seguridad social en Estados Unidos; del número de identificación fiscal en España o de las huellas dactilares de su titular. En todos estos casos, por medio de un procedimiento posterior, es posible llegar a identificar la persona a la que corresponden los datos.

En realidad, la protección de los datos personales se extiende a personas identificadas o identificables en todos los instrumentos internacionales y las legislaciones locales. En efecto, desde las *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales*, adoptadas en 1980 por la Organización para la Cooperación y el Desarrollo Económico (OCDE), pasando por la *Directiva sobre Protección de Datos Personales* de la Unión Europea de 1995, hasta el más reciente *APEC Privacy Framework*, adoptado en 2005 por el Foro de Cooperación Económica Asia-Pacífico, todos y cada uno de los instrumentos internacionales relativos al tema extienden su protección a personas identificadas e identificables. Lo propio acontece con la legislación comparada, inclusive la latinoamericana. Por consiguiente, sustentar que este es un equívoco de los países de América Latina es, por decir lo menos, errado.

La extensión del derecho a la protección de los datos personales a datos correspondientes a personas identificables apunta a garantizar la integridad de dicho acto. Se evita, así, que el propósito de la ley sea burlado mediante un subterfugio técnico que desvincule en apariencia los datos respecto de la persona a quien conciernen. Si esta es potencialmente identificable, tal como acontece en cada una de las hipótesis arriba mencionadas, la ley es aplicable, el titular goza de derechos, la entidad que trata los datos debe cumplir con sus obligaciones y queda ligada a las responsabilidades previstas por la ley. La protección es, pues, también efectiva sobre datos respecto de personas identificables.

La protección sobre datos correspondientes a personas identificables garantiza la adecuación de la ley al desarrollo de la tecnología. De este modo, las personas no quedan desamparadas de la ley por los progresos técnicos que permiten la asociación de ellas con determinados datos. Así, en la medida que sea posible correlacionar datos con personas –de acuerdo con el estado del arte de disciplinas como la dactiloscopia, la biometría, la genética o el simple cruce de bases de datos–, permitiendo su eventual identificación, dicho tratamiento de datos queda vinculado a cumplir con la ley sobre datos personales. Esto nos lleva a la raíz de este problema, al menos para los prestadores de servicio en línea: los números IP.

Un número IP es un identificador numérico mediante el cual se identifica un dispositivo conectado a Internet. Él es parte esencial del protocolo de comunicaciones en Internet, tal como un número telefónico lo es para las comunicaciones telefónicas. Sin embargo, a diferencia de este último, por lo general, un número IP no está asignado a un abonado en particular, sino que le es adjudicado al usuario cada vez que se conecta a la red por la empresa que le brinda la conexión de entre el conjunto de números que esta administra. Esto le permite al prestador correlacionar los números IP que asigna con el listado de sus abonados y, eventualmente, identificar al usuario que se ha conectado a la red. Consiguientemente, siendo un dato susceptible de vincularse a una persona determinable, su tratamiento debe cumplir con la ley sobre datos personales.

Los prestadores de servicio en línea sostienen que los números IP no constituyen propiamente datos personales y deberían ser excluidos de la aplicación de la ley. De acuerdo con ellos, los números IP no están concebidos para identificar usuarios, sino dispositivos; por ende, un número IP permite precisar desde qué equipo se verificó una comunicación, pero no establece la identidad de quién empleó dicho equipo.

Las autoridades europeas en materia de protección de datos personales, en cambio, sostienen que el tratamiento de números IP queda sujeto a las leyes sobre datos personales. En verdad, incluso si el propósito inicial de los números IP fuese tan solo facilitar técnicamente la comunicación en Internet, ello no es un impedimento para su empleo en la eventual identificación de ciertos usuarios; es tan cierto esto, que en diversos países se han adoptado normas especiales concernientes a la retención de datos de tráfico, incluyendo los números IP, a efectos de la persecución criminal, pues facilitan la labor de identificación del supuesto infractor. Este es el caso de la *Directiva sobre Retención de Datos* adoptada por la Unión Europea, de la Convención sobre Cibercrimen del Consejo de Europa, y hasta de la Digital Millenium Copyright Act de los Estados Unidos.

Con los nuevos estándares de comunicación sobre Internet, el potencial riesgo para las personas asociado al tratamiento de los números IP se incrementará. El actual protocolo IPv4 dispone de una limitada secuencia de números, lo que hace prácticamente obligatorio que su uso sea compartido entre los usuarios y administrado por el prestador de servicio de Internet. Sin embargo, el protocolo IPv6, que ya ha comenzado a ser implementado en varios países, ha incrementado exponencialmente el número de dichas secuencias. Esto permitirá que próximamente no solo nuestra computadora, así como, también, nuestros teléfonos celulares y GPS estén conectados a Internet, sino que, además, lo estarán nuestros vehículos, dispositivos de seguridad domiciliaria y hasta ciertos electrodomésticos. IPv6 permitirá la conexión continua a Internet y, con ello, un mayor tratamiento de datos personales de los usuarios de dispositivos conectados.

En suma, las legislaciones nacionales adoptadas en América Latina han hecho bien en conceptualizar los datos personales como aquellos concernientes a personas identificadas o identificables. Dicha noción garantiza la compatibilidad normativa con la legislación de otras latitudes; otorga una protección integral al derecho de toda persona de controlar su información personal; y permite la adecuación de la ley a los progresos de la ciencia y la tecnología, particularmente respecto de la identificación de los usuarios en Internet.

III. El consentimiento como legitimación para el tratamiento de datos

El derecho a la protección de los datos personales confiere a su titular la posibilidad de registrar la información que le concierne. Es ella quien determina a quién, cuándo y cómo suministra sus datos. Aún más, es ella quien define cuándo y cómo ejercer alguna de las facultades que le brinda la ley, tal como acceder a ellos, solicitar su modificación, eliminación o bloqueo, según los casos. Así, salvo las excepciones previstas legalmente, el tratamiento de datos personales puede verificarse solo cuando la persona a quien ellos se refieren lo ha autorizado. De hecho, aun habiendo autorización, el titular puede revocarla, lo que impediría el procesamiento ulterior de sus datos. Entonces, el consentimiento es esencial para el tratamiento legítimo de los datos personales.

Sin embargo, en ocasiones, el consentimiento no resulta suficiente para validar el uso de datos personales. Así, la aquiescencia de un empleado para

con su empleador en relación con que este acceda a su correo electrónico o de un consumidor respecto de su proveedor para con la transferencia de sus datos a terceros, aparece condicionada por la relación misma que tiene lugar. El consentimiento allí obtenido, cualquiera sea la fórmula contractual que revista, está constreñido. Esto ha llevado a diversos países a la adopción de reglas especiales que protegen a empleados y consumidores en relación con el tratamiento de la información personal que les conciernen por parte de sus empleadores y proveedores.

El permiso para tratar datos personales resulta aún más problemático en relación con Internet y la prestación de servicios en línea, particularmente cuando la validez de aquel descansa en haber sido entregado libre e informadamente. Es discutible el grado de información del que dispone un usuario promedio en relación con el opaco funcionamiento de las tecnologías de la información. Incluso es discutible la voluntad de un usuario avezado, si se considera la asimetría de información que media entre él y su proveedor de servicios. Otro tanto cabe agregar respecto de la libertad con que dicho consentimiento es brindado cuando la prestación de servicios no tiene carácter competitivo; en la mayor parte de la región, el mismo acceso a Internet es una prestación monopólica y, en el mejor de los casos, oligopólica. Esto pone al consumidor en el poco dichoso dilema de consentir al tratamiento de sus datos para acceder a Internet o resguardarlos y permanecer desconectado.

Las redes sociales en línea presentan problemas específicos en torno a cuán efectivo es el permiso brindado por sus usuarios. Este dilema se explica con las denominadas *economías en red*, ya que en ellas no es necesariamente el mejor prestador de servicios el que prevalece, sino aquel capaz de aglutinar una masa crítica de la demanda por servicios y proveer acceso no solo a este, sino a su red. Así, por ejemplo, un usuario puesto ante la disyuntiva de escoger un proveedor de telefonía, entre oferentes con igualdad de condiciones económicas, elegirá a aquel que le brinda acceso preferencial a una más amplia red de abonados o que le otorga servicios adicionales. Este ha sido el caso de los usuarios del paquete de ofimática de Microsoft, de los servicios de mensajería instantánea de Gmail o de los aplicativos de dispositivos Apple. En Chile, este es el caso de Facebook, la red social que congrega al 50% de los chilenos; naturalmente, los nuevos usuarios del país tienden a escoger dicho servicio por la ventaja comparativa de acceder a una red tan amplia de usuarios, haciendo caso omiso de la política de privacidad de la compañía.

Dado que el consentimiento brinda una limitada protección al titular de los datos personales, se han adoptado ciertos correctivos. Una de estas medidas es que el tratamiento de la información personal debe verificarse de

acuerdo con la finalidad que justificó su colecta, aquella que en su momento fue informada al titular y respecto de la cual este consintió. Así, el uso de datos personales en un proceso de reclutamiento laboral debe extenderse a información pertinente, a efectos de establecer la idoneidad laboral del candidato; requerir datos que excedan dicha finalidad, aun cuando sea consentido, implica un tratamiento ilícito de datos personales. Parafraseando las ya mencionadas recomendaciones de las Naciones Unidas en la materia, el tratamiento de datos personales debe ser adecuado, pertinente y no excesivo en relación con una finalidad legítima. Esto plantea preocupación respecto de ciertas prácticas de tratamiento de información personal en línea, tales como la publicidad contextual de Google o el reconocimiento facial de usuarios de Facebook.

Adicionalmente, la aspiración a reconducir toda la legitimidad del tratamiento de información personal a los términos de un contrato evade la responsabilidad pública en el resguardo de los derechos fundamentales de los usuarios. El costo transaccional de hacer cumplir la ley en un caso individual es altísimo, y dejar librado el respecto de los derechos del titular a las leyes del mercado es abandonarlo a su suerte. Esto es particularmente funesto si se ven forzados contractualmente a resolver cualquier conflicto con su proveedor de servicio ante jurisdicciones ajenas. Es precisamente la necesidad de enfatizar la protección que requieren las personas en relación con sus datos personales lo que ha llevado a la mayor parte de los países desarrollados, y progresivamente a los de América Latina, a establecer una autoridad pública que supervisa el cumplimiento de la ley.

En suma, salvo las excepciones previstas en la ley, el consentimiento de la persona concernida por la información es necesario para su tratamiento legítimo, pero no es suficiente. El tratamiento de datos personales debe cumplir con los demás preceptos de la ley sobre su protección, pero especialmente debe ser adecuado, pertinente y no excesivo en relación con una finalidad legítima.

IV. El riesgo del tratamiento de datos personales por prestadores de servicio en línea

La intención de reducir la protección que se brinda a los datos personales sobre la base de limitarla solo a los privados, concernientes a personas identificadas y sujetos a meras disposiciones contractuales, no es infundada. Por medio de dichos argumentos, los prestadores de servicios en línea

procuran disponer de un entorno legal más favorable para su prestación, removiendo los obstáculos jurídicos que pesan sobre el funcionamiento de Internet. Es, en ciertos casos, el entorno de que han dispuesto en su país de origen: los Estados Unidos. Con el afán de promover la extensión de Internet, en su día, el legislador estadounidense garantizó inmunidad a los prestadores de servicio en relación con los contenidos provistos por terceros, a excepción de aquellos que infringen la propiedad intelectual. En la práctica, este hecho ha conferido no solo inmunidad, sino, también, impunidad a los prestadores de servicio en relación con toda infracción cometida por terceros, incluso si dicho prestador está al corriente de ella. El derecho a la privacidad y el derecho a la protección de la información personal han resultado seriamente menoscabados como consecuencia de dicha política.

Las características de Internet sugieren que es necesario adoptar algunas reglas específicas respecto del tratamiento de datos personales que tiene lugar en la red. La colecta automatizada de información inherente al funcionamiento técnico de Internet hace necesario cierto tratamiento de esa, así como en el caso de números IP y *cookies*. El alojamiento de contenidos por terceros suscita dudas en cuanto a la responsabilidad que, eventualmente, cabe a quien provee servicios de almacenamiento para dicha información. La expresión de consentimiento, la individualización de usuarios, la adopción de normas especiales en protección de la infancia, entre otros, requieren del establecimiento de reglas certeras para el entorno en línea.

Sin embargo, la adopción de normas específicas en relación con el procesamiento de datos personales en Internet no implica derogar el derecho a su protección. En ciertos casos, será necesaria la introducción de flexibilidades, salvaguardias o limitaciones. Por ejemplo, ya hemos aludido al *derecho al olvido*, que supone que se prescinda del tratamiento de información personal en determinados casos, tales como sanciones criminales y administrativas ya cumplidas o deudas ya pagadas. En aquellos casos, su uso estaba fundado en una finalidad legítima, el cobro de un crédito o la imposición de una pena; sin embargo, una vez que se ha cumplido, los datos deben ser eliminados o bloqueados, según la opción legislativa que se adopte. Dicha eliminación o bloqueo también debería tener lugar en Internet. Sin embargo, el reconocimiento del *derecho al olvido* debe dejar a salvo ciertas excepciones, tales como aquellas resultantes del tratamiento de información personal para fines de investigación periodística y científica. Mediante esas flexibilidades, salvaguardias o limitaciones, el derecho a la protección de datos personales queda a resguardo, pero reconociendo ciertas excepciones a los efectos de cumplir con fines de interés público.

El establecimiento de reglas específicas en lo que concierne al tratamiento de datos personales en Internet, como se ha sugerido, también requiere precisar la responsabilidad a la que está sujeto un prestador de servicio en línea ante infracciones cometidas en la red. Dicha responsabilidad resulta relativamente clara cuando es el propio prestador de servicios quien realiza un uso indebido de datos personales, por ejemplo, al coleccionar datos de sus usuarios subrepticamente. Algo más complicada es la hipótesis cuando se trata de escindir responsabilidad entre dicho prestador y quien provee los contenidos; garantizar inmunidad absoluta es repulsivo para el resguardo de los derechos de terceros, tanto como forzar a los prestadores a censurar contenidos críticos a simple requerimiento de quien es objeto de los reproches, sin siquiera poseer orden judicial. Sin embargo, en América Latina, un problema más serio parece ser el relativo a la retención de datos personales por los prestadores de servicios en línea y el posterior uso que se hace de dichos datos.

A diferencia de la normativa sobre protección de datos, en América Latina existe menos progreso en lo relativo a la reglamentación de la retención de datos por los prestadores de servicio en la red, es decir, a la colecta y preservación de datos relativos al uso de Internet por sus usuarios, tales como los números IP asignados, fecha y hora de conexión, entre otros. Aunque varios proveedores se han visto forzados a procesar dicha información a los efectos de la tarificación y el control de acceso a sus servicios, otros solo lo hacen como resultado de obligaciones impuestas por la ley a efecto de facilitar la eventual identificación de usuarios.

Desafortunadamente, en América Latina, esta reglamentación no es uniforme; de hecho, no existe en todos los países, y en aquellos en los que existe, obedece a distintos impulsos legislativos. Así, por ejemplo, en la Argentina, se carece de regulación, tras la decisión de la Corte Suprema de Justicia, en el bullado caso *Halabi*, de declarar inconstitucional la ley y reglamentación adoptadas en la materia. Naturalmente, tanto las disposiciones constitucionales como las normas sobre protección de datos resultan aplicables en la materia, pero ellas son esquivas para la completa y acertada regulación de la retención de datos. En México, es la ley federal de telecomunicaciones la que reglamenta la materia. En Chile, en cambio, el código procesal penal fija normas al respecto, en el contexto de la individualización de responsables por delitos de pornografía infantil y otros crímenes. Este distingo en el impulso legislativo no es baladí, pues él incide obviamente en el mayor o menor celo del legislador al reglamentar.

Uno de los aspectos críticos al legislar sobre retención de datos por los prestadores de servicios en línea es la adopción de medidas de resguardo para los derechos fundamentales de las personas concernidas por la información. No solo es necesario precisar qué tipo de prestador de servicios es el obligado a retener, sino, también, qué información, cómo y por cuánto tiempo debe retener dicha información. Es igualmente crítico establecer a quién y bajo qué condiciones suministra dicha información. Establecer una apropiada normativa no es una tarea fácil; de hecho, los cuestionamientos a la constitucionalidad de la regulación son frecuentes. A la reciente declaración de inconstitucionalidad formulada por el Tribunal Constitucional Federal Alemán respecto de varias leyes que reglamentaban la materia, cabe agregar la ya mencionada decisión de la Corte Suprema de Justicia de la Argentina en el caso *Halabi*, y el también reciente fallo del Tribunal Constitucional de Chile en el que se resuelve la inconstitucionalidad de un sistema de registro de usuarios de cibercafés, el cual pretendía servir de complemento a la obligación legal de los prestadores de servicio de Internet de retener datos de sus usuarios. Todos ellos enfatizan la necesidad de resguardar apropiadamente los derechos de las personas atañidas por la información, a la hora de imponer en los prestadores de servicio la obligación de reservar datos personales de sus usuarios.

En los años venideros, los países de América Latina, especialmente aquellos que han suscrito tratados de libre comercio, se verán forzados a adoptar normas especiales sobre retención de datos personales a efectos de hacer cumplir las leyes sobre propiedad intelectual. De hecho, Chile ya ha implementado dicho compromiso, conduciendo a la inconsistente decisión de que la retención de datos tiene lugar para fines de persecución criminal de delitos graves y de infracciones a la ley de derechos de autor cualquiera sea su entidad. En Colombia, el denominado proyecto de Ley Lleras, a través del cual se intenta implementar dichas normas, ha suscitado un fuerte rechazo ciudadano, lo que obligó al Gobierno a su reformulación y dilación legislativa. Lo propio deberá tener lugar en otros países de la región, que han adoptado tratados de libre comercio (*e.g.*, Perú, República Dominicana y el Salvador) o consideran su adhesión a nuevos instrumentos en materia de protección a la propiedad intelectual (*e.g.*, México).

En suma, el tratamiento de datos en Internet plantea serios desafíos no solo a los prestadores de servicio de Internet, sino, también, a los Poderes Legislativos de la región, en orden a adoptar prácticas y normas que satisfagan legítimos fines de interés público y el adecuado respecto del derecho a la protección de los datos personales. La reglamentación de la retención de dichos datos sea, quizá, el más crítico en los próximos años.

V. Conclusiones

El derecho a la protección de los datos personales satisface más que simplemente la aspiración individual de una persona a excluirse de la vida social, por medio de su protección se salvaguarda el interés público envuelto tanto en el respeto de los derechos fundamentales de las personas, como en la preservación de condiciones de desarrollo inherentes a una sociedad democrática.

Los países de América Latina han hecho significativos avances en materia de protección a los datos personales, transitando progresivamente desde un modelo de protección preferentemente constitucional a un modelo que es complementado por legislación comprensiva. Este proceso ha brindado una protección más integral, con lo que se incrementa la certidumbre jurídica y avanza en la armonización normativa internacional.

Internet plantea nuevos desafíos para la protección de los datos personales en el entorno en línea. La adopción de normas especiales parece necesaria. En este contexto, se ha sugerido que la protección debería limitarse a los datos privados, referentes a personas identificadas, y dar preeminencia a soluciones contractuales. En este ensayo, hemos discutido cada una de dichas sugerencias, que, en vez de instar a la adopción de normas de adecuación al entorno en línea, limitarían ostensiblemente el derecho a la protección de los datos personales, sacrificando cada uno de los logros habidos hasta la fecha en la materia.

Dentro de los múltiples temas de relevancia, en los próximos años será crítico para los países latinoamericanos el acogimiento de leyes referidas a la retención de datos por los prestadores de servicio en línea, por medio de las cuales se procura la identificación de los usuarios. Sin embargo, cualquiera sea el interés que empuje dicha regulación, no debe omitirse la adopción de medidas de resguardo apropiado para las personas referidas por la información. Incrementar la eficacia de la ley no puede hacerse a cualquier precio. El derecho a la protección de los datos personales no puede ser sacrificado, pues su menoscabo afecta no solo a la persona a quien la información refiere, sino a la pervivencia de los derechos humanos y a los supuestos mismos del sistema democrático.

Filtrado de contenido en América Latina: razones e impacto en la libertad de expresión

Joana Varon Ferraz, Carlos Affonso Pereira de Souza,
Bruno Magrani, Walter Britto¹

Introducción

En diciembre de 2010, el parlamento venezolano aprobó un proyecto de ley para reglamentar el acceso a contenido y el uso de Internet en el país. El proyecto reforma la ley Resorte, que restringe el contenido transmitido por las estaciones de radio y televisión e intenta delimitar, entre otras cosas, la difusión de mensajes que pudieran «constituir manipulaciones mediáticas dirigidas a fomentar zozobra en la ciudadanía o alterar el orden público». La ley permite, a su vez, que se limite el acceso a sitios web que distribuyan mensajes o informaciones que «pudieran ser contrarios a la seguridad de la Nación» y a aquellos destinados a «desconocer a las autoridades legítimamente constituidas». El artículo 212 de la ley reformada dispone que «el Estado creará un punto de interconexión o punto de acceso a la red de los proveedores de servicios de Internet en Venezuela con la finalidad de manejar el tráfico con origen y destino en Venezuela, con el objeto de utilizar de manera más eficiente las redes del país dado el carácter estratégico del sector». Los proveedores de acceso tendrían, entonces, la obligación de establecer mecanismos que permitan restringir la difusión de mensajes, acceso a portales y de proporcionar información sobre las acciones sujetas a

1. Agradecemos a Carmen Eugênia Varon por la revisión del texto.

las regulaciones. De acuerdo con la organización Reporteros Sin Fronteras, «un dispositivo como este abriría camino a un filtrado en la red en detrimento de la libertad de información en línea»². Conforme el diagnóstico de la organización no gubernamental Espacio Público, «el proyecto incurre en graves deficiencias de técnica legislativa que permiten que los funcionarios que tengan la responsabilidad de aplicar este instrumento legal puedan actuar arbitraria y discrecionalmente, lo que constituye en sí mismo una vulneración del derecho humano a la libertad de expresión y permite su aplicación selectiva e interesada»³.

En México, el Partido de la Revolución Democrática ha presentado un proyecto de ley para monitorear y reglamentar el uso de las redes sociales en el país. Según el proyecto, el simple intercambio de información que ayude a otros a incumplir la ley pasaría a ser un crimen. Nazario Norberto Sánchez, el proponente del texto, defendió la creación de una policía en línea para monitorear y dificultar la manera en que los carteles de narcotraficantes están utilizando la red. Los internautas mexicanos han reaccionado al proyecto de manera crítica. Muchos afirman que la ley sería solo una excusa para que el Gobierno actúe con más vigilancia, y hasta han utilizado el término *Big Brother* para designar el tipo de posicionamiento que la policía ha intentado tomar.

De manera semejante, en abril de 2011, el Ministro de Justicia de Colombia presentó al Congreso un proyecto de ley para regular Internet y contenido en línea. El proyecto permite a los proveedores de servicios de Internet (ISPs) retirar o bloquear el acceso a contenido de forma *preventiva* en caso de que alguien alegue que esos contenidos violan derechos de autor. La sociedad civil se ha manifestado en contra de ese proyecto de ley, llamándolo «Ley Hadopi», como la ley francesa que prevé un mecanismo de 3 *strikes* para el corte de conexión de Internet por infracción de derechos de autor. En Brasil, una decisión judicial ya fue capaz de bloquear todo el acceso a YouTube en el país, en razón de un proceso en el que es parte una *top model* muy famosa que fue expuesta en el portal por medio de un video amateur que registró escenas de la *top model* con su novio en la playa, que eran al menos inapropiadas para menores. A pesar de no ser muy reciente,

2. Véase [en línea]: <<http://www.rsf-es.org/news/venezuela-la-ley-resorte-se-extiende-a-internet>>. [Nota del editor: consultada el 6/11/11.]

3. Véase [en línea]: <<http://espaciopublico.org/index.php/noticias/1-libertad-de-expresi/937-ley-resorte-restringe-la-libertad-de-expresion-en-internet-y-medios-electronicos>>. [Nota del editor: consultada el 6/11/11.]

el caso Cicarelli se volvió paradigmático entre los juristas del país porque provocó la discusión sobre por qué y cómo regular Internet y proteger el derecho de acceso de los ciudadanos.

El derecho del ciudadano de buscar, recibir y compartir información está protegido tanto por la Declaración Universal de Derechos Humanos como por el Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por su sigla en inglés). Si tratamos específicamente los países latinoamericanos, tenemos el Pacto de San José, conocido oficialmente como la Convención Americana sobre Derechos Humanos, ratificada por la mayor parte de los países de la región, que trata, en su artículo 13, sobre reglas contra la censura. De la misma manera, la Agenda de Túnez también fundamenta estos derechos en el ámbito de la Sociedad de Información, reafirmando, en su ítem 42, el compromiso con «la libertad de investigar, recibir, difundir y utilizar información, en particular, para la creación, compilación y diseminación del conocimiento». Más importante aún, el mismo ítem afirma que «las medidas tomadas para asegurar la estabilidad y seguridad de Internet, combatir la *ciberdelincuencia* y contrarrestar el correo basura deben proteger y respetar las disposiciones en materia de privacidad y libertad de expresión contenidas en las partes relevantes de la Declaración Universal de Derechos Humanos y en la Declaración de Principios de Ginebra».

Pero, conforme hemos visto, a pesar de que la libertad de expresión depende de la circulación libre de información, existe una tendencia en las legislaciones nacionales y regionales a intervenir en la arquitectura *end-to-end* de Internet de forma de imposibilitar la libre circulación de información y así deteriorar los derechos ciudadanos de libertad de expresión y privacidad.

Hay que acompañar de cerca la posible tendencia a aumentar la censura de información en línea. Varios Gobiernos latinoamericanos, y del mundo, han propuesto textos legales que imponen la criminalización de expresiones legítimas; la responsabilidad de los intermediarios; la desconexión del usuario con el pretexto de tratarse de violaciones de derecho de autor o de transmisión de información ilegal (como pornografía, narcotráfico, *ciberataques*, etcétera), o que, simplemente, permiten mecanismos arbitrarios de filtrado, bloqueo y remoción de contenido en la red y dan una protección inadecuada a los derechos a la privacidad y a los datos personales.

Todas esas disposiciones son bastante criticables porque ponen en riesgo los derechos fundamentales a la privacidad y a la libertad de expresión de los ciudadanos, y porque representan una amenaza a los elementos clave de la arquitectura de la red, como la neutralidad y la apertura. Por otro lado, es posible intuir que mientras que los países desarrollados ya establecieron

un marco jurídico para Internet, en Latinoamérica este movimiento aún es reciente. Este contexto en Latinoamérica nos otorga más espacio para la reflexión, tanto si observamos las críticas que han recibido las regulaciones extranjeras (por ejemplo, las reacciones negativas a la Ley Hadopi), como si nos esforzamos por evaluar y pensar cuestiones de acceso y libertad frente a nuestro escenario específico a nivel regional. Como la naturaleza de Internet no obedece fronteras, la introducción de regulación influye en la libertad de acceso y uso en otros países, lo que torna importante que los estándares establecidos por los países en desarrollo sean evaluados y debatidos a nivel global.

Frente a la posibilidad de aprovechar el espacio para la reflexión sobre el futuro de Internet en América Latina, este estudio explorará la legislación, las decisiones judiciales y las políticas de Internet en Brasil, Argentina, Chile, Colombia, México y Venezuela⁴, con un enfoque en casos de filtrado y remoción de contenido. El estudio intentará determinar si los abordajes más recientes de las leyes, jurisprudencia y las prácticas cotidianas son compatibles con la protección garantizada al derecho a la libertad de expresión. Este ensayo está organizado en 5 secciones: (i) una breve consideración sobre el concepto de filtrado y su tenue frontera con la violación de la libertad de expresión; (ii) un breve análisis de los estudios que aportan datos de la situación actual de la libertad de expresión en línea en esos países y tendencias futuras (iii) un análisis de las disposiciones legales de estos países sobre (1) el acceso al servicio de Internet, en términos de infraestructura y (2) la regulación de contenido; (iv) la actuación de los proveedores de servicios en las prácticas de filtrado; (v) conclusiones.

I. El concepto de filtrado

Así como los avances de la tecnología permiten un acceso inédito e inmensurable a la información, las innovaciones técnicas también posibilitan maneras de controlar el flujo de esa información en las redes. Hay que tener

4. Seleccionamos esos seis países porque son los que están en una mejor posición en el ranking del PIB nominal en Latinoamérica (1º, Brasil; 2º, México; 3º, la Argentina; 4º, Venezuela; 5º, Colombia y 6º, Chile). Al principio, esta lista incluía cinco; Chile fue sumado luego, ya que es el primer país que aprobó una ley de neutralidad de la red. Cuba también podría haber sido una alternativa interesante frente al tema, pero fue rechazado por carecer de datos disponibles.

en cuenta que en parte este control viene de la necesidad de mantener y mejorar la calidad y seguridad de los servicios en la red, como evitar *spam* y *virus*. Así que, la pregunta clave es: ¿en qué medida se puede permitir tal control en el flujo de información de forma que se garantice tanto el funcionamiento de la red como los derechos fundamentales? Por otro lado, han existido esfuerzos por utilizar esa tecnología para bloquear contenido considerado no deseado. Entonces, la segunda cuestión que tenemos que considerar es ¿cuál sería realmente el contenido «no deseado», ya que la democracia se fundamenta, entre otras cosas, en el espacio para que se formulen críticas sociales o morales que, en principio, serían «deseadas»?

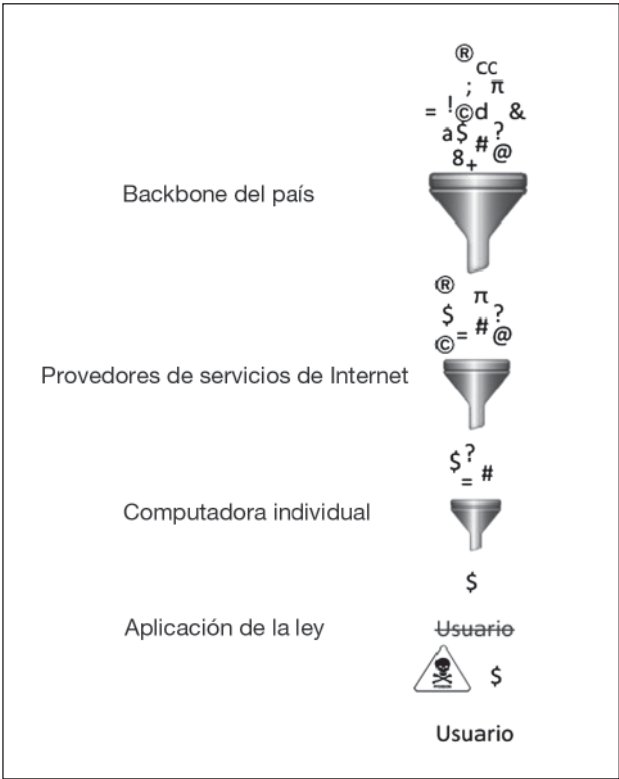
Según el informe de la UNESCO titulado *Freedom of Connection, Freedom of Expression, the changing legal and regulatory ecology shaping the Internet*, en la medida en que la información y comunicación es transmitida en la red, ese contenido utiliza varios protocolos de Internet y pasa por varios puntos en la red hasta llegar a los dispositivos de acceso de los usuarios. Teniendo esto en cuenta, el informe indica que las prácticas de filtrado ocurren más comúnmente en los siguientes puntos por los que pasa la información⁵:

- a) puertas para el *backbone* de Internet: es posible que el Estado intervenga directamente en el nivel de *backbone* de Internet mediante la utilización de tecnologías de filtrado o bloqueo. Por ejemplo, puede eliminarse el acceso a determinado contenido en todo un país a través de la utilización de puertas internacionales.
- b) proveedores de Servicios de Internet: hay una tendencia peligrosa a obligar o incentivar a los ISPs a que filtren contenido ilegal o inmoral, o a eliminar a ciertos sitios web de los resultados de búsqueda. Los Gobiernos también filtran *spam* e intentan evitar infecciones por *malware* para mantener la estabilidad y proteger al usuario;
- c) instituciones: las empresas, bibliotecas, escuelas, etc., pueden filtrar contenido según su criterio o en cumplimiento de directrices de autoridades gubernamentales;

5. Dutton, William H., Anna Dopatka, Ginette Law y Victoria Nash, *Freedom of Connection, Freedom of Expression: the Changing Legal and Regulatory Ecology Shaping The Internet*, París, UNESCO, 2011. Esta imagen responde a una adaptación de Zittrain, J., «A history of online gatekeeping», en *Harvard Journal of Law and Technology*, 19 (2) (2006), p. 253, disponible [en línea] en: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=905862>; y de Callanan, C. et ál., *Internet blocking balancing cybercrime responses in democratic societies* (2009), disponible [en línea] en: <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf>. [Nota del editor: ambas consultadas el 6/11/11].

- d) computadoras individuales: las personas pueden instalar en su máquina software de filtrado para restringir el acceso a determinado contenido o por razones de seguridad; y
- e) cumplimiento de la ley: pueden tomarse medidas contra usuarios que incurran en actividades ilícitas en la red como fraude, intercambio ilegal de música, etcétera.

Figura 1 | Puntos de imposición de medidas de filtrado



Fuente: Elaboración propia con base en el informe de la UNESCO.

La regulación del contenido de Internet es viabilizada por esos abordajes técnicos implementados en distintos niveles de acceso a la red. Parte de lo que se quiere averiguar en ese estudio es justamente si las regulaciones que tratan de contenido establecen límites claros y razonables para una eventual práctica de filtrado y si las prácticas de filtrado han tenido en cuenta solo las disposiciones legales o han sido extendidas para influenciar la cultura y

la política, al determinar qué contenido debe ser controlado, consumido o producido, promoviendo motivaciones excusas, como la censura al discurso político, la protección exagerada del derecho de autor, etcétera.

La mayor parte de estas prácticas requiere alguna inspección del contenido, sea solo para identificar la identidad de la fuente o para verificar el contenido del mensaje propiamente dicho, analizando todas las capas de los paquetes de datos. La tecnología moderna ha posibilitado el mecanismo de «Deep Packet Inspection» (DPI)⁶, o sea, la utilización de sistemas de computador que permiten que una tercera parte, que no es el emisor o el receptor del mensaje, pueda inspeccionar paquetes TCP/IP enviados por la red. Según Ben Wagner⁷, ese mecanismo puede ser «comparado a un sistema automatizado del servicio postal que abre cada carta, verifica su contenido, modifica lo que considere necesario, la sella nuevamente y la envía a su destino».

Lo que diferencia al filtrado hecho por DPI es la precisión y el volumen de tráfico que puede ser filtrado, ya que la tecnología permite que el filtrado sea realizado por una serie de características del paquete, como palabras clave, tamaño y otras propiedades. Los proveedores de servicios de Internet (ISPs) y los Gobiernos han utilizado ese mecanismo como medida de seguridad, para, por ejemplo, combatir ataques de *Denial of Service* (DOS) o para gestión de redes, pero ese mecanismo también ha sido utilizado para satisfacer el interés económico de los actores privados por medio de diferenciación de servicios, publicidad conductual, o con el pretexto de garantizar la aplicación de la ley. El mecanismo se ha utilizado con fines de vigilancia, censura y monitoreo. Hay quien afirma que el DPI abre puertas para métodos aun más sutiles de censura, ya que permite ir un paso más allá del filtrado, hacia la edición de contenidos⁸.

Conforme alerta Lawrence Lessig,

ese *design* de DPI no es algo dado, es el resultado de decisiones políticas y tecnológicas, de manera que el DPI tiene potencial

6. En oposición al concepto de «Shallow Packet Inspection», más trivial y que solo permite analizar superficialmente.

7. Wagner, Ben, «Deep Packet Inspection and Internet Censorship: International Convergence on an “Integrated Technology of Control”», presentado en el Tercer Simposio Anual de Giganet, en diciembre de 2008. Puede ser consultado [en línea], en <<http://www.scribd.com/doc/30663972/Study-Deep-Packet-Inspection-and-Internet-Censorship>>. [Nota del editor: consultada el 6/11/11.]

8. *Íd.*

para afectar las propiedades fundamentales de Internet como una infraestructura pública global, o sea, también tiene la capacidad de alterar la capacidad de la gobernanza global de Internet⁹.

Hay que recordar que más allá del DPI también existen otros mecanismos de filtrado, como los bloqueos por direcciones de IP¹⁰, por Identificadores Uniformes de Recursos (URI) y el bloqueo o manipulación de la extensión de nombre de dominio, la retirada de sitios web del servidor donde esté hospedado o la utilización de otras tecnologías de filtrado que excluyen de resultados de búsquedas las páginas web que contengan palabras clave u otros contenidos específicos¹¹. El ejemplo paradigmático de ese último caso es China, que adoptó sistemas de filtrado que bloquean el acceso a sitios web que contengan palabras como ‘democracia’ y ‘derechos humanos’¹². Finalmente, es importante resaltar que todas esas técnicas de filtrado no son precisas, o sea, es casi imposible bloquear solo un determinado contenido sin afectar otros. Y que, además, muchos de esos mecanismos utilizados para regular y censurar información son cada vez más sofisticados, utilizando, a veces, muchas capas de control que generalmente están escondidas del usuario común, quien probablemente ni se dará cuenta de que la información a la que accede ha sido objeto de filtrado. Persisten, por lo tanto, preguntas como ¿es el filtrado de hecho necesario? ¿si lo es, en qué circunstancias? ¿qué tipo de contenido debe ser controlado? ¿de qué manera? ¿con qué medidas de transparencia? Ese balance entre la necesidad técnica de las prácticas de filtrado, la necesidad política-social y el respeto a la libertad de expresión son los temas que pretendemos considerar a continuación en el análisis de las políticas, leyes, jurisprudencia y prácticas de los seis países bajo consideración.

9. Lessig, Lawrence, *Code and other Laws of Cyberspace*, Nueva York, Basic Books, 1999, p. 32.

10. Véase Protocolo de Internet.

11. Véanse informes de Frank La Rue y de la UNESCO.

12. Reporteros sin fronteras, «Enemies of the Internet», marzo de 2010, pp. 8-12; se encuentra disponible [en línea] en: <http://en.rsf.org/IMG/pdf/Internet_enemies.pdf>. [Nota del editor: consultada el 6/11/11.]

II. Breve panorama de la libertad de expresión en Latinoamérica: referencias a estudios que mapean datos de la situación actual y tendencias futuras

Antes de pasar al estudio comparado de las leyes, jurisprudencia y políticas de los países, parece pertinente mapear brevemente los principales estudios que han recogido datos sobre el tema de la libertad de expresión en línea en la región. El objetivo es entender el contexto político en el que estamos debatiendo las prácticas de filtrado y tener en mente las tendencias en esos países al tratar el tema de la libertad de expresión en la red.

La investigación más profunda y actual que tenemos fue elaborada por Freedom House en colaboración con el Fondo de las Naciones Unidas para la Democracia (UNDEF). El informe *Freedom on the Net, a Global Assessment of Internet and Digital Media*¹³ considera los desarrollos sobre el tema de la libertad de la red entre el 1 de enero de 2009 y el 31 de diciembre de 2010. El estudio fue elaborado a partir de una serie de entrevistas y consultorías en 37 países, y tuvo como base un conjunto de 21 preguntas y cerca de 100 subítems, organizados en tres grupos temáticos muy parecidos, quizás un poco más amplios, a los que trata nuestro análisis:

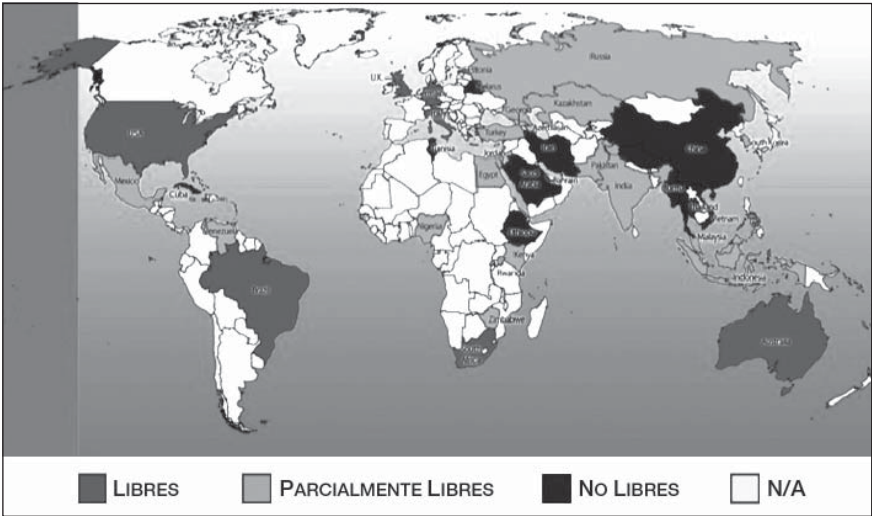
- a) obstáculos al acceso: se refiere a las barreras económicas y de infraestructura al acceso a Internet;
- b) límites de contenido: incluye el filtrado, bloqueo de sitios web y otras formas de censura; y
- c) violaciones de los derechos de los usuarios: incluye protecciones legales y restricciones a la actividad en línea; vigilancia y límites a la privacidad y punibilidad de las actividades en línea.

La respuesta a cada pregunta fue puntuada entre 0 (mejor) a 100 (peor) de manera comparativa con las respuestas de los otros países. Sumando la puntuación de las preguntas, Freedom House realizó un ranking sobre la libertad en la red. Tomó como definición de libertad de expresión el artículo 19 de la Declaración Universal de Derechos Humanos, o sea, el

13. Kelly, Sanja y Sarah Cook, (editoras), *Freedom on the Net, a Global Assessment of Internet and Digital Media*, sine loco, Freedom House, abril de 2011.

proyecto evalúa la libertad de trasmisión e intercambio de noticias y otras informaciones políticamente relevantes, así como la protección de los usuarios en lo que se refiere a la privacidad y su libertad de exponer sus ideas en la red, tanto en los aspectos legales como extralegales de sus actividades en línea. Considera que alguna limitación a la libertad de expresión puede ser implementada solo en circunstancias muy específicas y limitadas, de manera transparente y compatible con los patrones internacionales de derechos humanos, seguridad jurídica y con los principios de necesidad y proporcionalidad, cuestiones que también son destacadas por el Relator Especial de la ONU en libertad de expresión, Frank La Rue. Así, los países que obtuvieron un puntaje de entre 0 y 30 puntos fueron clasificados como «libres»; los que obtuvieron ente 31 a 60 puntos, como «parcialmente libres» y los que obtuvieron entre 61 y 100, como «no libres». Por supuesto que los rankings siempre traen generalizaciones cuestionables, pero el mapa de abajo nos permite tener una visión global de cómo algunos países de América Latina se posicionan en el mundo en relación con la libertad de expresión en la red.

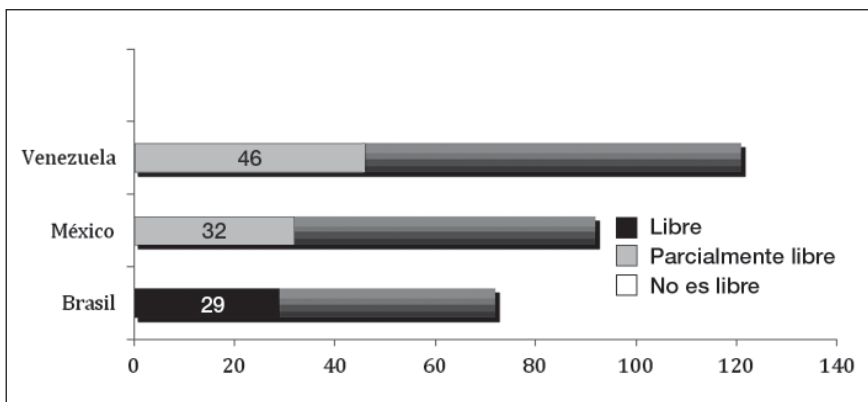
Figura 2 | Evaluación global de Internet y medios digitales



Fuente: *Freedom on the Net 2011, Global Assessment of Internet and Digital Media*, Freedom House.

Como se puede notar en el mapa, considerando a América Latina, los datos de la investigación de Freedom House incluyen solo a Brasil, México, Venezuela y Cuba. El estudio solo apunta a Cuba como un país «no libre», mientras que, según el estudio, México y Venezuela presentan restricciones a la libertad y Brasil respeta los límites posibles de la libertad de expresión, comparado con las leyes y prácticas de otros países, como, por ejemplo, China, Irán, Arabia Saudita y Cuba (que, como se sabe, son países extremadamente represores en el tema, lo que llega el padrón de 100 a límites totalmente inaceptables, y, por tanto, a algunas críticas sobre lo que podemos considerar de hecho un país libre en el ranking). El gráfico de abajo presenta la puntuación de cada uno de los países Latinoamericanos que participaron del informe, donde se puede observar que existieron diferencias significativas entre la puntuación de Brasil, México y Venezuela.

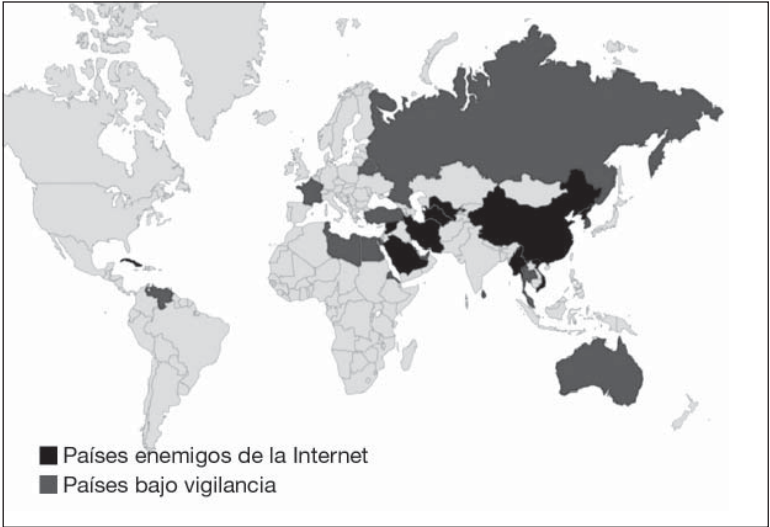
Figura 3 | Libertad de expresión online en América Latina



Fuente: *Freedom on the Net 2011, Global Assessment of Internet and Digital Media*, Freedom House.

Con una metodología menos refinada, pero basado en un levantamiento de casos empíricos de censura en la red, los Reporteros Sin Fronteras también publicaron un informe en marzo de 2011, donde, entre los países Latinoamericanos, Cuba figuraba como país enemigo de Internet y Venezuela como un país bajo vigilancia, conforme el mapa que está a continuación.

Figura 4 | **Enemigos de Internet, 2011**



Fuente: Reporteros sin fronteras (Reporters without Borders for Press Freedom), «Enemigos de Internet», marzo de 2011.

A pesar de que no tenemos datos definitivos sobre la libertad de expresión en Internet para toda Latinoamérica, tratando solo de la libertad de prensa en toda la región, los Reporteros Sin Fronteras han publicado un ranking que tomó en cuenta eventos ocurridos entre el 1° de septiembre de 2009 y el 1° de septiembre de 2010, además de distribuir cuestionarios respondidos por 178 países. El estudio no toma en cuenta violaciones de derechos humanos en general, solo de la libertad de prensa, o sea, violaciones que afectan directamente a los periodistas (como asesinatos, encarcelamientos, ataques físicos o amenazas). El estudio evaluó las violaciones a la libertad de prensa en los nuevos medios de comunicación, como la violación de la libre circulación de noticias en Internet, y también la impunidad de los que violan esas libertades.

Figura 5 | Libertad de prensa en América Latina, 2010



Fuente: Reporteros sin fronteras, *Freedom of Press Worldwide in 2010*.

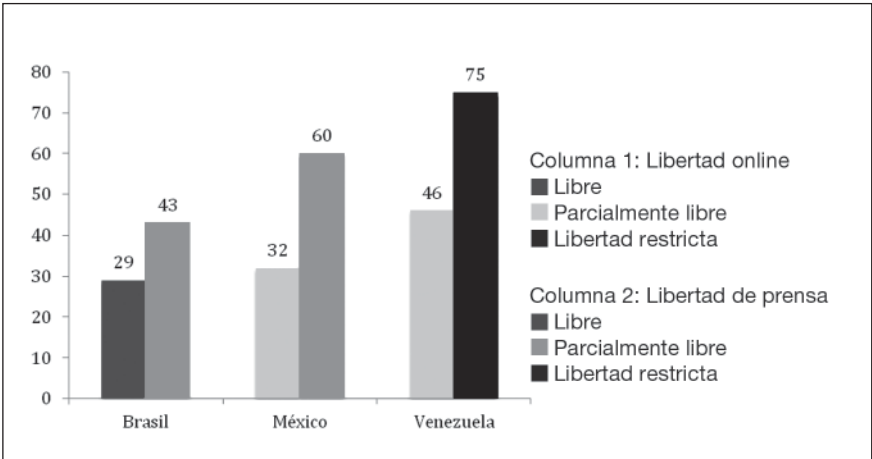
El mapa muestra que no hay ningún país en la región en buena situación. Entre los países objeto de este estudio, a pesar de que Chile y la Argentina presentan una situación satisfactoria, es notable que Brasil presente problemas, mientras que Venezuela, Colombia y México son considerados países en situaciones difíciles. Cuba, una vez más, se presenta como un país en situación muy grave.

De hecho, como muestra el mapa, la censura a la libertad de prensa ya representa una preocupación en la región. En la medida en que la región amplía sus índices de penetración de la red entre la población, hay que estar atentos para evitar que las actividades criticables se extiendan a la red y a todos los ámbitos de la libertad de expresión, que van más allá de la libertad de prensa.

Es en ese sentido, de manera interesante, la investigación de Freedom House compara sus índices de libertad de expresión en la red con otra investigación, de metodología semejante, que trata solo de la libertad de prensa. El gráfico a continuación resalta que existe una diferencia relevante entre el desempeño de esos países en los índices de esas dos investigaciones,

de manera que la censura a la libertad de prensa aún presenta números más preocupantes. En la medida en que disminuye la brecha digital y que las actividades de prensa y el intercambio de información dependen cada vez más de la red, nos queda la pregunta de si esos altos índices de represión a la prensa no pueden representar una amenaza en potencia al futuro de la libertad de expresión en línea de la región. Esta es una posible tendencia que tenemos que tener en mente y vigilar de cerca para que no se convierta en realidad.

Figura 6 | **Libertad de expresión en Internet contra libertad de prensa en algunos países latinoamericanos**



Fuente: *Freedom on the Net 2011, Global Assessment of Internet and Digital Media*, Freedom House.

El simple hecho de que no existan investigaciones con datos completos de toda Latinoamérica sobre el tema de la libertad de expresión en Internet ya es preocupante. Aunque otras regiones del planeta hayan inspirado más preocupación al respecto del tema por presentar severas violaciones a los derechos humanos, no debemos ignorar lo que ha pasado y lo que puede pasar en el futuro del Internet en Latinoamérica, sobre todo estudiando temas más específicos como el filtrado, la privacidad en la red y su impacto para la protección de derechos esenciales, más aún en el contexto actual de redefinición de marcos regulatorios para Internet en la región.

III. Análisis de las disposiciones legales sobre prácticas de filtrado

III.A. Las políticas de acceso a servicios de Internet y su impacto en las prácticas de filtrado

Atenuar la brecha digital entre los países de Latinoamérica y los países desarrollados sigue siendo un gran desafío para la región. Según el Observatorio Regional de Banda Ancha (ORBA), inaugurado en mayo de 2011 por la Comisión Económica para América Latina y el Caribe (CEPAL), el porcentaje de suscriptores de banda ancha móvil frente al total de habitantes de Latinoamérica y el Caribe aumentó de 0,2% en 2005 a 4,7%, en 2009, mientras que entre los países de la OCDE elevaron su proporción de 5% a 49% en el mismo periodo. Sin embargo, las diferencias de acceso dentro de los mismos países también son impresionantes. En Brasil, por ejemplo, el acceso a Internet por parte de la población más rica es del 2%, mientras que entre los más pobres es del 1,7%.

De acuerdo con la CEPAL, uno de los principales factores que determinan la adopción de la banda ancha es su precio. La Comisión evaluó que en marzo de 2011 el valor del servicio de banda ancha fija fue de US\$72,8 por Mbps, mientras que entre los países de la OCDE el precio fue de US\$5,9, una diferencia brutal. Esta situación se constituye como el principal obstáculo para que se acceda libremente a los contenidos de la red, restringiendo el acceso antes de cualquier práctica de filtrado.

Frente a esto, todos los países que pretendemos analizar están intentando adoptar regulación para garantizar el derecho de acceder al servicio de Internet. El tema es prioritario ya sea como tema de políticas públicas, por leyes que acaban de entrar en vigor o por proyectos de ley que están en debate. Es importante resaltar que aún existe una situación de poca competitividad entre los proveedores de acceso a Internet en Latinoamérica, característica común frente a los procesos de privatización no siempre muy bien realizados, o frente al monopolio de proveedores estatales. Así que, a veces, las estrategias de gobierno para ampliar el acceso pueden ser contradictorias, porque algunas de ellas ceden demasiado espacio a proveedores de servicios de Internet y terminan violando principios fundamentales para mantener una Internet libre y que respete principios básicos para asegurar la libertad de expresión, como el de la neutralidad de red. Eso es lo que se pretende averiguar en esa sección, a través de un análisis de las políticas para asegurar el derecho a la conexión y neutralidad de la red.

III.A.I. Derecho de conexión

III.A.I.a. BRASIL. En los últimos meses, Brasil ha pasado por un momento de regulación y establecimiento de directrices para ampliar el acceso a Internet en el país. Aunque no haya una ley específica sobre el derecho de acceder a la red, está en trámite la aprobación del Marco Civil del Internet, que pretende establecer los derechos y deberes de usuarios y proveedores de servicios de Internet. Entre sus disposiciones, el artículo 3° asegura como su objetivo: «*garantizar a todos los ciudadanos el acceso a Internet*». Además, el Proyecto de Enmienda Constitucional n° 6/2011 pretende modificar el artículo 6° de la Constitución Federal en relación con la siguiente disposición: «*son derechos sociales la educación, la salud, la alimentación, el trabajo, la vivienda, el ocio, el acceso a la Red Mundial de Computadores (Internet)...*»

De manera más concreta, con acciones prácticas, está en marcha la discusión del Plan Nacional de Banda Ancha (PNBL), que pretende triplicar el acceso a la banda ancha en el país para el 2014, con el objetivo de que llegue al 72% de los domicilios. Según el informe TIC domicilios, elaborado por el Comité Gestor de Internet (CGI/CETIC), en Brasil solo el 27% de los domicilios tienen Internet, de los cuales más del 50% tiene una conexión de menos de 1 Mbps.

El acceso a Internet en el país también proliferó por medio de las *Lan houses* (o locutorios privados de acceso a la red). Estas son pequeñas empresas que dan la oportunidad de acceso a Internet en áreas remotas o pobres a precios accesibles. De acuerdo con el informe del Comité Gestor de Internet en Brasil, las *Lan houses* fueron responsables por 1/3 del acceso a Internet en el país, en gran parte para la población de menor poder adquisitivo. Desafortunadamente, esos locutorios no han sido considerados como centros de inclusión digital a pesar de que lo son. En consecuencia, sufren limitaciones legales para el acceso de niños y adolescentes y para la formalización del negocio, como la obtención de préstamos o incentivos para cambio de equipos. Pero el escenario ha cambiado un poco, y se encuentra en debate un proyecto de ley para otorgar incentivos a esos emprendimientos.

Considerando en parte esos datos, en los últimos meses, el Ministerio de las Comunicaciones ha firmado acuerdos para la realización del PNBL. Mientras que trae algunas directrices esenciales, el Plan ha sido criticado por el acuerdo que el Ministerio de las Comunicaciones firmó con las empresas de telefonía. En él se delimitó un plan de 1Mps por R\$35 mensuales o R\$29 donde los gobiernos estatales exentan el cobro de ICMS.

La coordinación de los Movimientos Sociales¹⁴ criticó el acuerdo por no garantizar el cumplimiento de la velocidad de 1Mbps (que se considera una meta baja para banda ancha), por permitir la venta casada de Internet con línea telefónica (algo prohibido por el Código de Defensa del Consumidor), entre otras críticas. Lo peor es que las empresas de telecomunicaciones podrán disminuir esta velocidad en el caso de que el usuario sobrepase los 300 Mbytes de *download* o 500 Mbytes por mes. O sea, que, por un lado, el acuerdo crea restricciones para el usuario, y por otro flexibiliza las reglas para las empresas.

El 30 de junio de 2011 también se firmó el Decreto 7512, que establece el Plan General de Metas de Universalización (PGMU)¹⁵. El decreto dispone, en su artículo 2º que la Agencia Nacional de Telecomunicaciones (ANATEL) deberá adoptar, hasta el 31 de octubre de 2011, las medidas regulatorias necesarias para establecer patrones de calidad para los servicios de telecomunicaciones de acceso a Internet de banda ancha, definiendo parámetros de velocidad, disponibilidad de servicios y reglas de publicidad y transparencia.

Frente a ese Decreto, la ANATEL inauguró en consulta pública una propuesta de masificación y mejoría de Internet de banda ancha fija. La propuesta estará disponible para el debate por 30 días y el objetivo es que sea aprobada antes del 31 de octubre. La norma prevé que la velocidad media de los accesos nunca sea menor al 60% del pactado en el contrato, y que ese porcentaje se eleve gradualmente. Actualmente no existe una disposición legal sobre el tema, y la práctica es que se garantice solo el 10%. En un principio esa propuesta trata solamente sobre los accesos fijos, pero ANATEL pretende extender esa disposición también para los servicios móviles. La medición será hecha por los propios usuarios con un software que los proveedores tendrán que tornar disponible. Si el texto es aprobado, la medida entrará en vigor en julio de 2012.

El reglamento también tiene disposiciones sobre neutralidad de la red. En cuanto a esto, establece que «queda prohibido que la prestadora realice bloqueo o tratamiento discriminatorio de cualquier clase de tráfico, como

14. Véase Red de asociaciones de la sociedad civil por la democratización del acceso a Internet.

15. Véase [en línea] <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7512.htm>. [Nota del editor: consultada el 6/11/11.]

voz, datos o video, independientemente de la tecnología utilizada». Pero el primer párrafo genera dudas en cuanto a la efectividad de la disposición toda vez que no permite la adopción de medidas de bloqueo o administración de tráfico que resulten indispensables para mantener la seguridad y estabilidad del servicio y de las redes.

ANATEL trabaja conjuntamente con el Consejo Administrativo de Defensa Económica (CADE), por medio de acuerdos de cooperación, bajo la Ley General de Telecomunicaciones. El objetivo es asegurar que las tecnologías de información y comunicación operen de manera independiente, libre y justa. Aunque el CADE tenga la prerrogativa legal de tratar cuestiones de *antitrust*, como la concentración de mercado y el establecimiento de precios, la falta de competencia aún es problemática en el país. Como en la mayor parte de los países de Latinoamérica, los planes de privatización implementados en los 90 crearon una tendencia hacia la concentración del mercado de telecomunicaciones y de proveedores de servicios de Internet (ISPS). En un intento por cambiar el escenario, ANATEL inauguró una consulta pública para el Plan General de Metas de Competitividad¹⁶ con el objetivo de disciplinar la competitividad entre prestadores de servicios en mercados competitivos y no competitivos. Así que, en los próximos meses, Brasil promete tener nuevos marcos regulatorios para garantizar la calidad de conexión.

III.A.I.b. ARGENTINA. La política del Gobierno argentino para Internet está basada en dos declaraciones de principios y está organizada en tres ejes:

El primero es el Decreto 554/97 que declaró de Interés Nacional el acceso de sus habitantes a Internet, «en condiciones sociales y geográficas equitativas, con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciones de la multimedia». Ese decreto también concede a la Secretaría de Comunicaciones (SECOM) el poder para desarrollar planos estratégicos para la expansión de Internet en Argentina.

Frente a ese decreto, otras regulaciones se sucedieron, como el Decreto 1293/98 que crea el proyecto Internet 2 Argentina y el Decreto 1018/98 que instituye el Programa para el Desarrollo de las Comunicaciones Telemáticas (argentin@internet.todos). Estas regulaciones pretenden promover el

16. Véase [en línea] <<http://www.anatel.gov.br/Portal/exibirPortalNoticias.do?acao=carregaNoticia&codigo=23243>>. [Nota del editor: consultada el 6/11/11.]

desarrollo de la infraestructura de telecomunicaciones buscando el acceso universal. Para eso, se estipuló que dentro de la SECOM sea instituida una unidad de coordinación responsable de planificar y evaluar la ejecución del programa, y se facultó a la SECOM a que celebre un convenio con la Unión Internacional de Telecomunicaciones (UIT) para desarrollar el programa argentin@internet.todos.

Sin embargo, esos decretos no tratan sobre la regulación de telecomunicaciones. La privatización de las compañías de telecomunicaciones en los 90 dividió a la compañía estatal Entel en dos empresas privadas, cada una responsable de parte del territorio del país. Luego, empresas extranjeras compraron parte de sus acciones.

Para garantizar que se invirtiera en tecnología moderna, el Gobierno concedió el monopolio de los servicios básicos de telefonía de voz a esas empresas, en sus respectivos territorios. También concedió un monopolio para el tráfico internacional de datos y voz *inbound* y *outbound* a Telintar. A pesar de haber finalizado esas concesiones, el monopolio se presenta como un problema hasta el día de hoy, y los representantes de proveedores de servicios de Internet (ISPS) frecuentemente critican el comportamiento de las empresas por distorsionar la competencia.

III.A.I.c. VENEZUELA. Venezuela también tiene su marco regulatorio. El Decreto 825 de mayo de 2000 establece una «Internet prioritaria» y declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político del país. En sus artículos, el decreto encarga a los Ministerios a presentar financiamientos e incentivos fiscales a quienes instalen o suministren bienes y servicios relacionados con el acceso y el uso de Internet tanto para los órganos del Estado como para los ciudadanos. El país también tiene un Plan Nacional de Ciencia, Tecnología e Información que establece metas para el periodo entre 2005 y 2030, entre ellas: «7. Contribuir con la creación de una red del Estado integrada e interconectada, incorporando a la misma proyectos de acceso a Internet, voz, datos y video».

Mientras tanto, aún es preocupante la concentración del número de accesos a Internet en el operador del Estado CANTV. La Superintendencia para la Promoción y Protección de la Libre Competencia en Venezuela (Procompetencia) declaró que CANTV concentra cerca del 75-80% de los accesos residenciales a Internet. Peor aún, toda la capacidad del satélite Simón Bolívar también será administrada por CANTV y los servicios de Internet asociados serán prestados por ese operador. Este

control estatal sobre la conexión de Internet que se verifica por CANTV debe ser subrayado como algo importante que podría limitar el acceso a determinados contenidos e informaciones en la red. CANTV también planea instalar en Venezuela un punto de acceso a la red o NAP. Los NAP son puntos donde confluyen las redes de las distintas empresas proveedoras de servicios de Internet. A través de ellos, se intercambia el tráfico entre los diferentes proveedores de servicios de Internet (ISPs). Por lo tanto, el NAP debería ser administrado por una empresa independiente, que tenga la neutralidad de red como norma, y no por un operador que, además, ya tiene el control de mercado.

III.A.I.d. COLOMBIA. En Colombia, la ley 1341 de 2009 definió principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones en el país. Además, determinó la creación de la Agencia Nacional de Espectro. En relación con esa misma ley, se debate el proyecto de ley 149 de 2010, que pretende garantizar el acceso público a Internet. Ese texto propone que Internet sea reconocido como servicio de valor agregado, objeto del artículo 69 de la Ley 1341 incluyéndolo como objeto de subsidios. Además propone que sean generadas bandas de acceso generalizado y uso gratuito, al proponer que la «Agencia Nacional del Espectro deberá determinar algunas bandas que sean de acceso gratuito, que puedan ser utilizadas para la prestación del servicio de Internet, en especial en los grandes conglomerados urbanos». Establece que «dichas bandas podrán ser utilizadas por los proveedores de TIC a tarifas especiales para que los usuarios atiendan sus necesidades básicas de conectividad». El Ministerio de las TICs también contribuyó con la apertura de una subasta, sobre el espectro de banda ancha de 2,5 GHz (giga hercio) para ampliar la competencia e incluir una cuarta empresa que preste servicios de acceso fijo y móvil.

III.A.I.e. CHILE. En Chile un proyecto de reforma constitucional propone: «La libertad y el derecho a acceder, en condiciones de igualdad, a las tecnologías de información, comunicaciones e Internet, cualquiera sea el medio utilizado o la localización geográfica de los usuarios».

Una ley determinará la forma en que el Estado garantizará el ejercicio de este derecho y las condiciones respecto a calidad y precio. El plan por parte del Ministerio de Transporte y Comunicaciones para bajar los costos del servicio es alcanzar un 60 por ciento de cobertura en el año 2014 y lograr la universalidad en ocho años.

III.A.I.f. MÉXICO. En México, se presentó una reforma a la Constitución para adicionar el párrafo 10º al artículo 4º, que consagra que «toda persona tendrá derecho de contar con acceso a Internet». También hay un reconocimiento de la responsabilidad del Estado para plantear y promover el desarrollo del acceso a tecnologías de información y comunicación, lo que en mayo de 2010 se concretizó con la previsión de una inversión de US\$115,5 millones para extender el acceso a Internet en áreas remotas.

Así como en los otros países, en México la falta de competitividad del sector sigue contribuyendo a unos precios altos, y hay pocos incentivos para que las empresas de telecomunicaciones inviertan en la expansión de sus servicios para áreas rurales. A pesar de que existen algunos proveedores de Internet independientes, la empresa Telmex domina el mercado. Eso se atribuye en parte a la legislación de telecomunicaciones del país, que, elaborada en 1960, otorga a COFETEL y a la Comisión Federal de Competencia (CFC) la tarea de regular el sector. Las asociaciones de libertad de prensa han criticado a COFETEL por su falta de independencia del Departamento de Comunicaciones y Transportes.

Es importante observar que todos los países han caminado hacia pensar Internet como un derecho del ciudadano, y han intentando viabilizar políticas de acceso, algunas más exitosas que otras.

Aunque la mayor parte de los países estudiados consideren que acceder al servicio de Internet es un derecho, observamos que existen grandes problemas de acceso a infraestructura de Internet y en la calidad de conexión. Pero más allá de estas cuestiones de naturaleza técnica y económica que impiden el acceso universal a la red, tenemos restricciones legales al acceso a contenido.

III.A.II. Neutralidad de la red

Hay una tendencia entre los países bajo estudio a debatir leyes sobre la neutralidad de la red. Aunque la neutralidad de la red sea un concepto técnico de administración de la red, este principio tiene una clara influencia en el acceso a contenidos, y, aunque no sea su fin original, puede, cuando está garantizado, proteger la libertad de expresión. Para estudiar cómo el principio de la neutralidad de red ha sido implementado y debatido en los diferentes países, describiremos brevemente el concepto general y el problema básico al que este principio se refiere para, luego, presentar un cuadro comparativo de cómo el principio se implementó o qué se está discutiendo en los distintos países incluidos en este estudio con respecto a este principio. Finalmente, concluiremos con un análisis comparativo de las alternativas.

La neutralidad de la red es un principio de arquitectura de la red que establece que los datos que viajan en Internet deben tratarse igualmente, o sea, sin preferencia entre cualquier aplicativo, contenido o proveedor de servicio¹⁷. De esa manera, se garantiza que la información fluya libremente, sin discriminación alguna en función de origen, destino, protocolo o contenido. Para posibilitar la implementación de ese principio, las operadoras de acceso y servicios de Internet deben transportar paquetes de datos de manera neutral, sin favorecer o perjudicar a unos contenidos por encima de otros¹⁸. Mientras que los proveedores de Internet no tienen un incentivo general para discriminar entre los paquetes de datos que viajan en su red¹⁹, hay estudios que han demostrado que los proveedores de acceso han discriminado tráfico al menos por tres razones: para ampliar su propio lucro, para gestionar el ancho de banda en su red o para excluir contenidos contrarios a las políticas de la empresa²⁰.

Frecuentemente, la neutralidad de la red se ve amenazada por operadoras que establecen acuerdos comerciales para privilegiar o degradar el contenido conforme la relación comercial de este con la operadora. Por ejemplo, los servicios de voz sobre IP (VOIP) pueden competir directamente con el proveedor de acceso a Internet que ofrece también servicios de telefonía. Otro caso se da cuando el proveedor de acceso es también una empresa de TV a cable y, al sentirse amenazado por los contenidos de video en línea, disminuye la velocidad de tránsito de esos paquetes. Además, con la excusa de gestionar el tráfico, los proveedores también pueden discriminar entre paquetes y establecer niveles de calidad de determinado servicio, en detrimento de otros, hasta cobrando más, como peajes para determinada clase de contenidos, como por ejemplo planes más caros para conexiones más rápidas específicamente para paquetes de videos. Hay quienes defienden que

17. Schewick, Barbara van, «Towards an Economic Framework for Network Neutrality Regulation», en *Telecomm. & High Tech. L.* 5 J, *sine data*, p. 329.

18. Véase el debate entre Tim Wu y Christopher Yoo: «Keeping the Internet Neutral?», *sine data, sine loco et sine nomine*.

19. Si los usuarios ven la libertad de acceder a contenidos y servicios como un factor de agregación de valor al producto, ellos tendrán una mayor libertad para elegir migrar a donde el proveedor ofrece el mejor servicio.

20. Schewick, Barbara van y David Farber, *Point / Counterpoint: Network Neutrality Nuance; sine data, sine nomine et sine loco*.

las prácticas de competencia garantizarían que aunque los proveedores no respeten la neutralidad de red, los usuarios podrían optar por aquellos que ofrezcan los servicios que necesitan por el precio más justo. Sin embargo, es un hecho que en nuestros países, dado lo que fue analizado en la sección anterior sobre infraestructura y acceso, y frente a la falta de transparencia de cómo se da la gestión de tráfico, no existe un nivel de competencia que garantice los derechos de consumidor del usuario. Por lo tanto, el principio de la neutralidad de la red tiene como objetivo garantizar la libertad de los usuarios de la red para acceder al contenido, servicios y aplicaciones de su elección y evitar el bloqueo o filtrado indebido de contenido por razones políticas y económicas, entre otras.

Frente a esas cuestiones, y de manera paradigmática, Chile fue el primer país del mundo en tener una ley específica sobre el tema. A pesar de haber sido pionero al aprobar esa ley, desde el año 2004, los Estados Unidos ya tenían reglas de neutralidad de la red establecidas por su organismo regulador de telecomunicaciones, la *Federal Communications Commission* (FCC). La FCC estableció los principios rectores de la industria de las telecomunicaciones. Los principios están basados en las cuatro libertades que componen un núcleo básico para futuras leyes de neutralidad. Ellas son: (a) los consumidores deben tener acceso a los contenidos legales de su elección... (b) [deben ser capaces de] ejecutar aplicaciones de su elección... (c) conectar cualquier dispositivo que deseen [a su servicio de acceso a Internet de banda ancha] y (d) deben recibir información comprensible acerca de sus planes de servicio²¹.

Para visualizar cómo gran parte de las reglas de la FCC y de la legislación chilena han influido sobre las propuestas legislativas de los países analizados, elaboramos el cuadro que está a continuación. Las tres primeras columnas hacen referencia a la legislación y propuestas legislativas de la Argentina, Chile y Colombia. En el cuadro, estas se muestran con el mismo color para indicar la fuerte influencia de la legislación chilena. Brasil y México han adoptado diferentes enfoques y fueron destacados con otros colores en el cuadro.

21. *Notice of Proposed Rulemaking 09-93*, Federal Communications Commission, véase [en línea]: <[HTTP://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf)>. [Nota del editor: consultada el 6/11/11.]

Cuadro 1 | Cuadro comparativo de las legislaciones y propuestas legislativas sobre neutralidad en la red en la Argentina, Brasil, Chile, Colombia, México y Venezuela

Chile	Argentina	Colombia	Brasil	México	Venezuela
Ley 18168/2010	<p>Proyecto de Ley de la Cámara de Diputados de la Nación 1159-D-2011</p> <p>Artículo 24 H.- Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos; entendiéndose por tales, toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet:</p> <p>a) no podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red.</p> <p>b) No podrán limitar el derecho de los usuarios de incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen ni perjudiquen la red o la calidad del servicio.</p> <p>c) Podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan</p>	<p>Ley 1450/2011</p> <p>Artículo 56. Neutralidad en Internet. Los prestadores del servicio de Internet: 1. Sin perjuicio de lo establecido en la Ley 1336 de 2009, no podrán bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos. Los prestadores del servicio de Internet podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación.</p> <p>2. No podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los</p>	<p>Proyecto de Ley-Marco Civil de Internet</p> <p>Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, sendo vedada qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços, conforme regulamentação. Parágrafo único. Na provisão de conexão à Internet, onerosa ou gratuita, é vedado monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, ressalvadas as hipóteses admitidas em lei.</p> <p>Reglamento Anatel</p> <p>Art. 59. É vedado à Prestadora realizar bloqueio ou tratamento discriminatório de qualquer tipo de tráfego, como voz, dados ou vídeo, independentemente da tecnologia utilizada.</p> <p>§ 1º A vedação prevista no caput deste artigo não impede a adoção de medidas de bloqueio</p>	<p>Proyecto de Ley para la modificación de la Ley Federal de Telecomunicaciones</p> <p>Artículo 44 <small>XVI</small>: Cuando presten servicios de acceso a Internet, fijo o móvil, garantizar el libre tráfico en la red y abstenerse de bloquear, discriminar, entorpecer o restringir el derecho de los usuarios a acceder, consultar, transmitir, recibir, contratar u ofrecer cualquier contenido, servicio o aplicación de carácter lícito.</p> <p>Los proveedores de acceso a Internet que no sean concesionarios, pero que hagan uso de una red pública de telecomunicaciones, se sujetarán asimismo a lo dispuesto por esta fracción.</p>	No hay

(Continúa)

Chile	Argentina	Colombia	Brasil	México	Venezuela
<p>Con todo, los concesionarios de servicio público de telecomunicaciones y los proveedores de acceso a Internet podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan afectar la libre competencia.</p> <p>Los concesionarios y los proveedores procurarán preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red. Asimismo, podrán bloquear el acceso a determinados contenidos, aplicaciones o servicios, solo a pedido expreso del usuario, y a sus expensas. En ningún caso, este bloqueo podrá afectar de manera arbitraria a los proveedores de servicios y aplicaciones que se prestan en Internet.</p> <p>b) No podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio.</p> <p>c) Deberán ofrecer, a expensas de los usuarios que lo soliciten, servicios de controles parentales para contenidos que atenten contra la ley, la moral o las buenas costumbres, siempre y cuando el usuario reciba información por adelantado y de manera clara</p>	<p>afectar la libre competencia. Asimismo, podrán bloquear el acceso a determinados contenidos, aplicaciones o servicios, solo a pedido expreso del usuario, y a sus expensas. En ningún caso, este bloqueo podrá afectar de manera arbitraria a los proveedores de servicios y aplicaciones que se prestan en Internet.</p> <p>Artículo 2.- Todos los ISP deberán publicar en su sitio web toda la información relativa a las características del acceso a Internet ofrecido, su velocidad (tanto de bajada como de subida), calidad del enlace, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio.</p> <p>Proyecto de Ley s-1491/11</p> <p>Artículo 1º.- Las prestadoras de servicio de telecomunicaciones y proveedores que presten el servicio de acceso a Internet, no podrán bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. Estará prohibido establecer jerarquías o prioridades en la información o servicios en Internet. No podrán perjudicar la calidad de servicio contratado a través de medidas de gestión de tráfico. Los usuarios podrán tener acceso a todo el contenido sin la intermediación de los proveedores de acceso a Internet.</p>	<p>mismos no dañen o perjudiquen la red o la calidad del servicio.</p> <p>3. Ofrecerán a los usuarios servicios de controles parentales para contenidos que atenten contra la ley, dando al usuario información por adelantado de manera clara y precisa respecto del alcance de tales servicios.</p> <p>4. Publicarán en un sitio web, toda la información relativa a las características del acceso a Internet ofrecido, su velocidad, calidad del servicio, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio.</p> <p>5. Implementarán mecanismos para preservar la privacidad de los usuarios, contra virus y la seguridad de la red.</p> <p>6. Bloquearán el acceso a determinados contenidos, aplicaciones o servicios, solo a pedido expreso del usuario.</p> <p>Parágrafo. La Comisión de Regulación de Comunicaciones regulará los términos y Condiciones de aplicación de lo establecido en este artículo. La regulación inicial deberá ser expedida dentro de los seis meses siguientes a la entrada en vigencia de la presente ley.</p>	<p>ou gerenciamento de tráfego que se mostrarem indispensáveis à garantia da segurança e da estabilidade do serviço e das redes que lhe dão suporte.</p> <p>§ 2º Os critérios para bloqueio ou gerenciamento de tráfego de que trata o § 1º deste artigo devem ser informados previamente a todos os Assinantes e amplamente divulgados a todos os interessados, inclusive por meio de publicação no site da Prestadora na Internet</p> <p>§ 3º O bloqueio ou gerenciamento de tráfego deve respeitar a privacidade dos Assinantes, o sigilo das comunicações e a livre, ampla e justa competição.</p>		

(Continúa)

Chile	Argentina	Colombia	Brasil	México	Venezuela
<p>y precisa respecto del alcance de tales servicios.</p> <p>d) Deberán publicar en su sitio web, toda la información relativa a las características del acceso a Internet ofrecido, su velocidad, calidad del enlace, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio. El usuario podrá solicitar al concesionario o al proveedor, según lo estime, que le entregue dicha información a su costo, por escrito y dentro de un plazo de 30 días contado desde la solicitud.</p>	<p>Artículo 2°.- Las prestadoras de servicio de telecomunicaciones deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor que no distinga arbitrariamente contenidos, aplicaciones o servicios.</p> <p>Artículo 3°.- Las prestadoras de servicio de telecomunicaciones y los proveedores de acceso a Internet podrán tomar las medidas para la gestión de tráfico y administración de red, exclusivamente en el ámbito que han sido autorizadas, siempre que ello no afectar la libre competencia.</p>				

Complementando el análisis anterior, los cuadros a continuación muestran cómo los principios generales de la regulación de la FCC han influido en los diferentes modelos de regulación de neutralidad de la red en la región.

Cuadro 2 | Cuadro comparativo entre el modelos de libertades básicas para neutralidad de red del FCC y las Legislaciones y propuestas legislativas de Chile, la Argentina, Colombia, Brasil, México y Venezuela

Libertades básicas sobre neutralidad de la red de la FCC	Chile	Argentina	Colombia	Brasil	México	Venezuela
Libertad de acceso a cualquier contenido legal	Art. 24, H, a)	PL 1159-D-2011 Art. 1, a)	Ley 1450/2011, Art. 56, 1.	Proyecto de Ley - Marco Civil de Internet Art. 9	PL para modificación de la Ley Federal de Telecomunicaciones Art. 44	No hay*
		PL S-1491/11 Art. 1		Reglamento Anatel, Art. 59		
Libertad de ejecutar cualquier aplicativo lícito	Art. 24, H, a)	PL 1159-D-2011 Art. 1, a)	Ley 1450/2011, Art. 56, 1.	Proyecto de Ley - Marco Civil de Internet Art. 9.	PL para modificación de la Ley Federal de Telecomunicaciones Art. 44	No hay
		PL S-1491/11 Art. 1		Reglamento Anatel, Art. 59.		

(Continúa)

Libertades Básicas sobre neutralidad de la red de la FCC	Chile	Argentina	Colombia	Brasil	México	Venezuela
Libertad de conectar cualquier dispositivo que no interfiera con el funcionamiento de la red (carterfone)	Art. 24, H, b)	PL 1159-D-2011 Art. 1, b)	Ley 1450/2011, Art. 56, 2.	No consta en norma específica de neutralidad**	No consta en norma específica de neutralidad	No hay
				No consta en norma específica de neutralidad.		
Acceso a información exhaustiva sobre planes de servicio (transparencia)	Art. 24, H, d)	PL S-1491/11 Art. 2	Ley 1450/2011, Art. 56, 4.	Proyecto de Ley - Marco Civil de Internet	No consta en norma específica de neutralidad	No hay
				Art. 7, IV.		
				Reglamento Anatel, Art. 59, §2º		

* Ver *infra* nota.

** El hecho de que esta libertad no esté prevista en la norma específica de neutralidad no quiere decir que no lo esté en otra reglamentación.

Cuadro 3 | Cuadro comparativo de otros temas claves de las legislaciones y propuestas legislativas de Chile, la Argentina, Colombia, Brasil, México y Venezuela

	Chile	Argentina	Colombia	Brasil	México	Venezuela
¿Existe excepción al principio de la neutralidad para fines de administración técnica o de seguridad?	Sí, Art. 24, H, a)	PL 1159-D-2011 Sí, Art. 1, c PL S-1491/11 Sí, Art. 3	No	Sí. Proyecto de Ley - Marco Civil de Internet, Art. 9 Sí. Reglamento Anatel, Art. 59, §2º	No	No es aplicable
¿Existe la obligación de oferta de servicio de control parental por los proveedores a pedido de los usuarios?	Sí, Art. 24, H, a)	PL 1159-D-2011 Sí, Art. 1, c*** PL S-1491/11 No	Sí, Art. 56, 3	No No	No	No es aplicable

*** Este artículo no se refiere a la posibilidad de que el usuario solicite al proveedor el bloqueo de contenido por razones de seguridad. Los proveedores podrán bloquear contenido ante una solicitud del usuario de que, por ejemplo, cierto contenido sea prohibido en una escuela o como medida de control parental realizada por el proveedor.

III.B. Regulación de contenido y su impacto en las prácticas de filtrado

Aunque el acceso a la conexión de Internet recién sea objeto de debate en las leyes de los países latinoamericanos bajo estudio, según descubrimos al estudiar concepto de filtrado, las disposiciones legales al respecto no garantizan el libre acceso al contenido que circula en la red. Tampoco lo hacen las disposiciones de neutralidad de la red, dado que todas dejan espacio para restricciones legales. Por esa razón, hay que averiguar cómo son las regulaciones de contenido de esos países. Primero, debemos estudiar cómo son las garantías generales a la libertad de expresión. Después, debemos saber cuáles son las restricciones legales, y si esas restricciones se condicen con las restricciones mínimas aceptables a ese derecho.

El Relator Especial de la ONU para la libertad de expresión, Frank La Rue, en su informe sobre la promoción e protección del derecho a la libertad de expresión en Internet, elaborado después de una serie de consultas y reuniones en el mundo, estipula que una restricción al contenido en línea solo podría establecerse de forma excepcional, siempre que se cumplan tres requisitos:

- a) esté prevista en una ley, que sea clara y accesible para todos;
- b) sea la medida más adecuada para alcanzar tal objetivo (principio de la proporcionalidad y necesidad); y
- c) persiga uno de los objetivos establecidos en el artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por su sigla en inglés)²².

Ese artículo es una de las disposiciones más importantes para tener en mente al tratar el tema de filtrado y su balance con la libertad de expresión. Los párrafos 2 y 3 establecen:

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir

22. Acá también podríamos hacer referencia al artículo 13 de la Convención Americana sobre Derechos Humanos, que trata sobre la libertad de pensamiento y de expresión y que prohíbe, además, en su párrafo 2, cualquier clase de censura previa; a la vez que establece el mismo test tripartito del párrafo 3 del artículo 19 de la Declaración *supra* mencionada.

informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

- a) asegurar el respeto a los derechos o a la reputación de los demás;
- b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

O sea, la libertad de expresión no es un derecho absoluto, y puede estar sujeto a restricciones legales que sean muy puntuales, pero solo de manera de atender a los requisitos mencionados. Además, el Relator de la ONU también establece que cualquier legislación sobre esas restricciones debe aplicarse por una institución que sea independiente de influencias políticas, comerciales, etc., de forma que no se cometan arbitrariedades o discriminación, y que aún así, debe haber vigilancia en caso de aplicación abusiva.

La utilización arbitraria de la ley, por ejemplo criminalizando expresiones legítimas, constituye una restricción grave de derechos. Teniendo en cuenta esos requisitos, a continuación proponemos un examen crítico de las regulaciones de contenido de los países bajo estudio, con el fin de averiguar si en realidad tratan de simplemente asegurar el respeto a la reputación, a los derechos fundamentales de los demás y a la protección de la seguridad nacional, el orden, la salud y la moral públicas de manera balanceada con la libertad de expresión. Para eso, separamos el análisis en 3 clases de contenido que generalmente son objeto de regulación o de prácticas de filtrado:

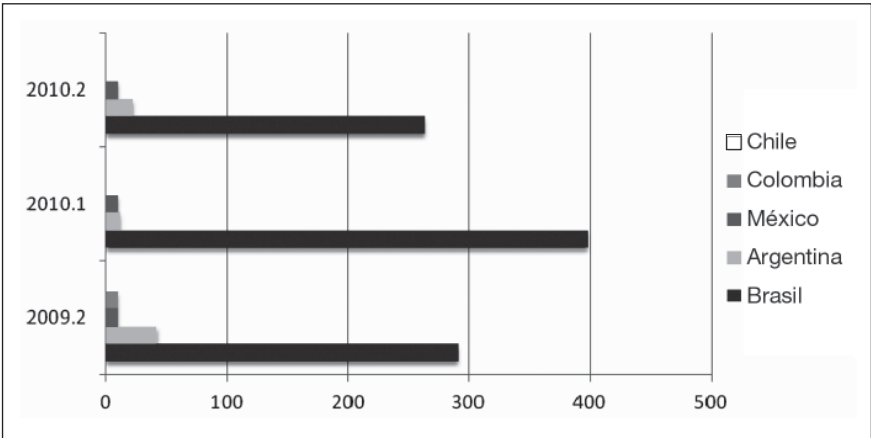
- a) regulaciones de contenido que atenta contra la igualdad y reputación de los demás: contenido racista, xenófobo, de incitación al terrorismo o genocidio, del discurso del odio, la calumnia, injuria y difamación;
- b) regulación de contenido que viole el derecho de autor; y
- c) regulación de contenido de carácter sexual.

Un análisis de esas regulaciones y de cómo han sido utilizadas se hace fundamental porque, como vimos en los capítulos anteriores, los países estudiados aseguran el derecho de acceso y la neutralidad de la red, pero, por otro lado, el poder judicial ha ejercido un papel importante en Latinoamérica respecto a decidir sobre qué debe ser filtrado o bloqueado de la red, como también lo han tenido los propios proveedores de servicios de Internet (ISPs)

que reciben pedidos de remoción de contenido. A veces, como vimos, esto ocurre de manera inadecuada y genera riesgos para la libertad de expresión.

El gráfico a continuación muestra los datos del informe de Transparencia de Google, que indica las solicitudes de remoción de contenido de Brasil, la Argentina, México, Colombia y Chile. Brasil, por ejemplo, de toda Latinoamérica, figura en el lugar más alto de la lista de pedidos de remoción de contenido de Google.

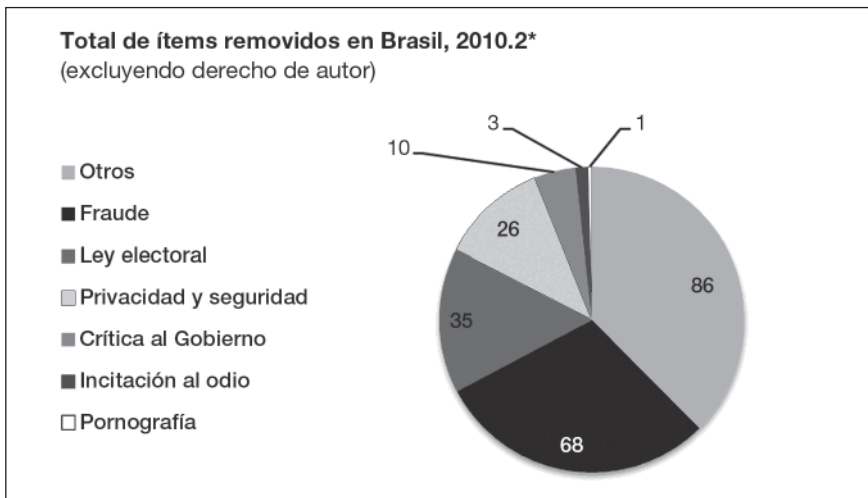
Figura 7 | **Número de solicitudes de remoción de contenido de Google (evaluación semestral, de julio de 2009 a diciembre de 2010)**



Fuente: *Google Transparency Report*, disponible en <http://www.google.com/transparencypreport>.

De acuerdo con las explicaciones de Google, Brasil tiene tantas solicitudes principalmente por la popularidad de Orkut, de donde provenían la mayor parte de los pedidos. Los pedidos eran, en gran parte, reclamos en casos de difamación y suplantación de identidad. En cuanto a los motivos de remoción de contenido en Brasil, el gráfico de abajo muestra los porcentajes de ítems removidos por diversas razones. Según el informe de Google, el 76% de los requerimientos fueron atendidos en el segundo semestre de 2010, resultando en un total de 12.363 ítems removidos de Internet. Entre estos, la mayoría fue por violación al derecho de autor –principalmente en razón de una orden judicial que ordenó la remoción de 18.000 fotos de Picasa–. 546 remociones fueron por difamación, concentradas principalmente en Orkut y YouTube. Los otros casos se muestran en el gráfico a continuación:

Figura 8 | Número total de ítems removidos en Brasil en 2010



Fuente: Datos extraídos de *Google Transparency Report*.

*Estos son datos parciales, pues no están representados los números de casos de derecho de autor. Estos son mucho más grandes y causan distorsiones gráficas, por lo tanto, imposibilitan una comparación visible entre las categorías. Mientras que los casos representados en el gráfico no llegan a más de cien ítems individualmente, en Brasil 11 588 ítems fueron objeto de remociones por derecho de autor.

III.B.I. Remoción de contenido que atenta contra la igualdad y la reputación de los demás

Para los objetivos de esta sección, entendemos como regulación de contenido que atenta contra la igualdad y reputación de los demás a aquella que trata sobre contenido racista, xenófobo, de incitación al terrorismo o genocidio, del discurso del odio, de la calumnia, injuria y difamación. Se va a analizar si los países han emitido regulación sobre esos temas que se aplica a las conductas practicadas en la red, si esa regulación trata sobre prácticas de filtrado, y si esas prácticas respetan los derechos fundamentales. Frente a esas observaciones, se busca analizar si las decisiones de los casos prácticos están de acuerdo con las disposiciones legales y si respetan la libertad de expresión.

III.B.I.a. BRASIL. En Brasil, el crimen de racismo y discriminación racial está previsto en su Constitución Federal. Está descrito como un crimen imprescriptible que no admite fianza. Además, el país tiene en su

ordenamiento una Ley de Crímenes Raciales y en el Código Penal está prevista la injuria por motivo racial, étnico, religioso, de nacionalidad o color de piel. Finalmente, la Ley que criminaliza el Genocidio también trae cuestiones de discriminación en su definición.

Al estudiar pormenorizadamente las previsiones de esas leyes, se entiende fácilmente que ellas también son aplicables a los actos practicados en Internet. Por ejemplo, la Ley de Crímenes Raciales de 1989, trata sobre la incitación al prejuicio y la discriminación en su artículo 20: «*Practicar, inducir o incitar la discriminación o preconcepción racial, color, etnia, religión o procedencia nacional. Pena: reclusión de uno a tres años y multa*». Esta ley establece que se puede aumentar la pena de dos a cinco años y multa si «*cualquiera de los crímenes previstos en el enunciado es cometido por intermedio de los medios de comunicación social o publicación de cualquier naturaleza*». Estas disposiciones configuran una forma de reprimir la difusión de contenido ofensivo en cualquier medio, incluso Internet. Si bien esta no es una disposición de filtrado, esta clase de disposiciones se observa en los párrafos tercero y cuarto del mismo artículo:

- § 3º En los casos del párrafo anterior, el juez podrá determinar, después de previa consulta con el Ministerio Público o por medio de solicitud del mismo, incluso antes de instaurada la investigación policial, bajo pena de desobediencia,
- I - la retirada inmediata o la búsqueda e incautación de las copias del material en cuestión;
 - II - la terminación de su transmisión vía radio o televisión.
 - III - la prohibición de los mensajes o páginas de información en la world wide web.

Aunque sea más evidente en el caso del inciso III del párrafo tercero, con alguna interpretación es posible aplicar las disposiciones de todos esos incisos a los casos de discriminación en Internet, incluso para permitir prácticas de filtrado de contenido.

Los crímenes contra honra, previstos en los artículos 138 a 145 del Código Penal, no regulan la prohibición o retirada de contenido, pero también contemplan prácticas en Internet, pues el artículo 141, que trata de las disposiciones comunes, establece que:

- Artículo 141 - Las penas señaladas en este capítulo se aumentarán en una tercera parte, si alguno de los delitos son cometidos:
- III - en la presencia de varias personas, o por medio que facilite la difusión de calumnias, difamación o injurias.

También existen previsiones sobre la forma de difusión en la Ley de Genocidio (ley 2.889/56, que recrimina la práctica o incitación directa o publica de actos que pretendan destruir grupos nacionales, étnicos, raciales o religiosos). Mientras que la incitación pública ya está enunciada en el artículo 3º, su párrafo 2º dispone un aumento de la pena si hay difusión por medio de la prensa. Esas disposiciones abren un espacio para que queden incluidas las prácticas en Internet. Sin embargo, no hay disposiciones acerca del filtrado de contenido.

Se nota, por lo tanto, que la ley brasileña sobre el tema, aunque tenga solo una disposición legal que se refiere explícitamente a Internet, puede ser interpretada de manera de condenar las prácticas discriminatorias y de discurso intolerante en la red. Cabe resaltar que esa disposición actúa solo en el sentido de disuadir la conducta discriminatoria. Las prácticas de filtrado solo estarían permitidas por la ley de crímenes raciales (§3º incisos I, II y III).

Entretanto, ya existen decisiones sobre la aplicación de esas previsiones legales para punir conductas en el Internet que van más allá de considerar esas prácticas como crimen, al incluir la posibilidad de bloquear el acto calumnioso, difamatorio o injuria.

De hecho, hubo algunas condenas por el crimen de racismo propagado en Internet. El caso de Marcelo Valle Silveira Mello²³, instaurado en 2009, inauguró la práctica en la aplicación de la Ley de Crímenes Raciales en los casos relacionados con la red. Este es un caso de un crimen de racismo que se llevó a cabo a través de la red social Orkut. En este caso, se protestó contra el sistema de cuotas para minorías étnicas y raciales en la Universidad, y las protestas se manifestaron a través de declaraciones altamente perjudiciales contra la raza negra. El proceso llegó hasta la segunda instancia (TJDF), donde el reo fue condenado por unanimidad de votos.

Otro ejemplo paradigmático, más reciente, ocurrió en 2011 a raíz de los comentarios discriminatorios de Mayara Petruso²⁴ en Twitter sobre las

23. «Turma condena acusado de crime de racismo pela Internet», en *JusBrasil*, del 3 de septiembre de 2009, disponible [en línea]: <<http://www.jusbrasil.com.br/noticias/1845390/turma-condena-acusado-de-crime-de-racismo-pela-internet>>. [Nota del editor: consultada el 6/11/11.]

24. «OAB-PE ingressa diretamente com ação penal contra Mayara Petruso», en *JusBrasil*, del 2 de junio de 2011, disponible [en línea] en: <<http://www.jusbrasil.com.br/noticias/2716755/oab-pe-ingressa-diretamente-com-acao-penal-contra-mayara-petruso>>. [Nota del editor: consultada el 6/11/11.]

personas que vienen de la región noreste del país. Como se sabe, Brasil presenta grandes desigualdades regionales, y es común que habitantes de otras regiones vengan al Sudeste, región más rica, para buscar oportunidades. Los comentarios de Mayara despertaron una ola de manifestaciones *prejuiciosas* contra los nordestinos, después de la victoria de la Presidente Dilma Roussef (que también viene de aquella región). Mayara está siendo acusada de racismo e incitación a la práctica delictuosa.

Esos casos tuvieron repercusión en los medios de comunicación, pero hubo otros, así que existe jurisprudencia sobre maneras de proceder frente a esos crímenes. Por ejemplo, de manera interesante el Superior Tribunal de Justicia determinó que los crímenes de racismo practicados en una misma comunidad de Internet deben ser procesados solo en un Estado de la federación.

Además de estas disposiciones del Código Penal, los crímenes contra la honra también están previstos en el Código Electoral. El Código Electoral también ha sido base para procesos por injuria, calumnia y difamación a través de Internet. El texto de los artículos del Código Electoral que tipifican esos delitos (artículos 324 a 327) es similar al Código Penal, pero se limita a la publicidad electoral. Como en las normas penales, en este caso también se prevén aumentos de penas por la utilización de «medios que faciliten la divulgación de la ofensa» (artículo 327, III). Se incluye, por lo tanto, a Internet. Esas previsiones han resultado en el bloqueo de material de manera peligrosa y muy cercana a la censura por razones políticas, como fue el caso del bloqueo de blogs políticos durante las elecciones de 2006 a petición del candidato José Sarney, lo que causó gran polémica en los medios de comunicación tradicionales y en la blogosfera nacional e internacional²⁵.

En el caso específico de Brasil, cuando se trata de la remoción de contenido en razón de quejas por atentar contra la reputación de los demás, es importante considerar que hay registros significativos de filtrado o bloqueo por orden judicial, aunque ese tipo de práctica esté prevista explícitamente solo en la ley de Crímenes Raciales.

25. «Election and Censorship Dialectics in the Brazilian Blogosphere», en *English Global Voices*, del 1º de septiembre de 2006, disponible [en línea] en: <<http://globalvoicesonline.org/2006/09/01/election-and-censorship-dialectics-in-the-brazilian-blogosphere/>>. [Nota del editor: consultada el 6/11/11.]

Conforme datos del informe de Transparencia de Google, entre todos los países analizados en ese informe, Brasil presenta el mayor número de solicitudes de remoción de contenido (263 solicitudes), quedando al frente de Corea del Sur (139) y Alemania (118).

Según el informe, la razón principal de los números considerablemente más altos de Brasil con respecto a los de otros países es la popularidad de Orkut en el país. Según el informe de Google, esta plataforma fue objeto de solicitudes de remoción de contenido por las causas más diversas. Cabe anotar que el país se ha destacado por el uso masivo de las redes sociales. Según comScore, el país es el segundo del mundo en número de visitas a páginas de redes sociales, perdiendo únicamente frente a los Estados Unidos. El último *webinar* de comScore reportó que 99 de cada 100 brasileños acceden a redes sociales al menos una vez al mes. Mientras que Orkut lidera la preferencia entre los brasileños con un 71,9% de alcance, el uso de Facebook está en ascenso, con un 40,8%. El país también es el sexto en mayor número de accesos a Google⁺²⁶.

Si consideramos solamente los casos de difamación en todas las plataformas de Google, 546 ítems fueron objeto de solicitudes. En razón de la ley Electoral, fueron 35, mientras que 3 fueron denunciados por discurso de odio.

Otra razón destacada por Google fue el aumento de solicitudes expedidas por la justicia electoral durante las elecciones presidenciales, que requirió la remoción de contenido relacionado con campañas políticas. Desafortunadamente, no hay datos más completos y precisos que los de Google, que tienen algunas restricciones metodológicas considerables.

III.B.I.b. CHILE. En Chile no hay tipificación penal específica para las cuestiones raciales u otras formas de discriminación. Sin embargo, existen leyes que tratan específicamente el genocidio –la Ley N ° 20.357– y el antiterrorismo –Ley 18.314/84–. Esta última causa una gran conmoción en el país, por ser considerada remanente del periodo dictatorial y por

26. «Quase todo usuário da web no Brasil também entra em redes sociais, diz estudo», *Uol Notícias*, del 28 de abril del 2011, disponible [en línea] en <<http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/04/28/quase-todo-internauta-brasileiro-tambem-acessa-redes-sociais-diz-estudo.jhtm>>. [Nota del editor: consultada el 6/11/11.]

ser actualmente utilizada en contra de los líderes políticos Mapuches²⁷, vedándoles la libertad de expresión. En esas leyes, no se encontraron disposiciones legales que podrían aplicarse a Internet, en especial porque tratan sobre la represión física directa.

Por otro lado, dos crímenes contra el honor, la calumnia y la injuria, están previstos en el Código Penal de manera que permiten aplicaciones para Internet. Mientras que sus definiciones están respectivamente en los artículos 412 y 416, el artículo 422 dispone:

Art. 422. La calumnia y la injuria se reputan hechas por escrito y con publicidad cuando se propagaren por medio de carteles o pasquines fijados en los sitios públicos; por papeles impresos, no sujetos a la ley de imprenta, litografías, grabados o manuscritos comunicados a más de cinco personas, o por alegorías, caricaturas, emblemas o alusiones reproducidos por medio de la litografía, el grabado, la fotografía u otro procedimiento cualquiera.

Aunque no se considere explícitamente el Internet, es posible interpretar que las conductas ahí practicadas son punibles por la frase «otro procedimiento cualquiera». Aún no se tiene conocimiento de jurisprudencia que trate de ese tipo de casos, o sea, aun no se puede decir que haya plena aplicación de esa ley para la plataforma virtual. Para todos esos crímenes, como la aplicación para Internet está sujeta a interpretación, no hay ninguna disposición de filtrado en esos casos.

III.B.I.c. MÉXICO. El genocidio y el terrorismo son delitos tipificados en el Código Penal mexicano. El artículo 149 bis, sobre el genocidio, solo prevé penas para la realización del delito, y no por la incitación al mismo. Por otro lado, en cuanto al delito de terrorismo, el artículo 142 determina que el delito de incitación también se castiga, y es plenamente aplicable a los casos en que se utilice Internet como plataforma de comunicación.

27. «Chile: el peso de la ley antiterrorista sigue cayendo sobre los presos políticos mapuche», en *Uniao Campo Cidade e Floresta*, del 27 de enero de 2011, disponible [en línea] en: <<https://uniaocampocidadeefloresta.wordpress.com/2011/01/27/chile-el-peso-de-la-ley-antiterrorista-sigue-cayendo-sobre-los-presos-politicos-mapuche>>. [Nota del editor: consultada el 6/11/11.]

Los crímenes de discriminación están previstos en la Ley Federal para Prevenir y Eliminar la Discriminación. El artículo 9 de esa ley establece condiciones para la libertad de expresión frente a conductas discriminatorias:

Artículo 9. [...] A efecto de lo anterior, se consideran como conductas discriminatorias:

xv. Ofender, ridiculizar o promover la violencia en los supuestos a que se refiere el artículo 4 de esta Ley a través de mensajes e imágenes en los medios de comunicación.

xvi. Limitar la libre expresión de las ideas, impedir la libertad de pensamiento, conciencia o religión, o de prácticas o costumbres religiosas, siempre que estas no atenten contra el orden público.

xviii. Restringir el acceso a la información, salvo en aquellos supuestos que sean establecidos por las leyes nacionales e instrumentos jurídicos internacionales aplicables.

xxvii. Incitar al odio, violencia, rechazo, burla, difamación, injuria, persecución o la exclusión.

La ley mexicana tiene, por lo tanto, disposiciones que tratan explícitamente sobre crímenes cometidos en la red.

En cuanto a los crímenes contra el honor, México presenta un ejemplo interesante. El país llevó a cabo un proceso de despenalización de esas conductas, que pasaron a estar sujetas solo a multas y están previstas en el artículo 1916 del Código Civil, bajo las disposiciones de daño moral. En los casos en que el daño derive de un acto que haya tenido difusión en los medios informativos, la solución es aún más creativa. Para esos casos, la ley dispone que el juez ordene que los mismos den publicidad al extracto de la sentencia, o la rectificación o respuesta de la información difundida en el mismo medio donde fue publicada, con la misma relevancia que hubiera tenido la difusión original. Esto torna dispensable cualquier disposición de práctica de filtrado.

III.B.I.d. VENEZUELA. En Venezuela existen disposiciones más agresivas en términos de filtrado de contenido de Internet. La Ley de Responsabilidad Social en los Medios de Comunicación de Radio, Televisión y Electrónicos es la principal regulación sobre el tema. En su artículo 28 establece las directrices para varias limitaciones al contenido de los medios de comunicación, incluyendo la difusión de mensajes que:

1. Inciten o promuevan el odio y la intolerancia por razones religiosas, políticas, por diferencia de género, por racismo o xenofobia.

2. Inciten o promuevan y/o hagan apología al delito.
3. Constituyan propaganda de guerra.
4. Fomenten zozobra en la ciudadanía o alteren el orden público.
5. Desconozcan a las autoridades legítimamente constituidas.
6. Induzcan al homicidio.
7. Inciten o promuevan el incumplimiento del ordenamiento jurídico vigente.

Una descripción legal tan amplia de contenido que deberá ser limitado es un ejemplo de una disposición legal que abre un espacio claro para prácticas de filtrado.

También es bastante específica la manera en la que el Código Penal de Venezuela describe los crímenes de calumnia, injuria y difamación, pues además de los casos generales, practicados contra cualquier ciudadano, existe una disposición más específica para aquellos que vengán a «ofender de alguna manera el honor, la reputación o el decoro» del presidente, del vicepresidente y/o de miembros del judicial (arts. 147 a 151) o legislativo (arts. 222 a 228). Para estos casos específicos, la pena es de restricción de libertad, mientras que en los casos generales (arts. 442 a 450) también hay una pena de multa. Para todos los casos, las penas se amplían «si la ofensa se hubiere hecho públicamente», lo que puede incluir también casos de divulgación de ofensas en Internet.

Además, con respecto a las prácticas de filtrado, importa notar que el artículo 448 dispone:

En caso de condenación por alguno de los delitos especificados en el presente capítulo, el juez declarará la confiscación y supresión de los impresos, dibujos y demás objetos que hayan servido para cometer el delito; y si se trata de escritos, respecto de los cuales no pudiere acordarse la supresión, dispondrá que al margen de ellos se haga referencia de la sentencia que se dicte relativamente al caso.

Con base en este artículo, es posible en Venezuela realizar el bloqueo de contenido en Internet que sea considerado calumnioso, injurioso o difamatorio, a partir de que haya una condena y declaración del juez para que se tomen medidas de filtrado.

Sin embargo, la separación de los casos generales y aquellos centrados en las autoridades puede ser una amenaza velada, una forma de desalentar la crítica política y ciudadana. Los acontecimientos recientes confirman el clima de tensión en relación a la crítica política en Venezuela. Por ejemplo,

un caso de referencia en 2010 fue la represión sufrida por el *twittero* Cristian Fuentes por tomar fotos de situaciones de mal funcionamiento del metro de Caracas²⁸ y publicarlas bajo la cuenta @Caracasmetrocuando. Mientras Cristian hacía el informe fotográfico por Twitter, los policías lo detuvieron y lo obligaron a borrar sus fotos.

También en 2010, el caso de Noticiero Digital se volvió famoso por la polémica que causó entre un sitio de noticias y el presidente Hugo Chávez. En esa ocasión, el portal *noticierodigital.com*, que funciona como un foro de tendencia opositora, fue acusado por Chávez de haber cometido el delito de calumnia por publicar información falsa sobre el asesinato del ministro de Obras Públicas y Viviendas, Diosdado Cabello. Las noticias fueron publicadas en el foro del sitio. Al defenderse, el noticiero subrayó que: «cada usuario es consciente de que los mensajes en este foro son las opiniones y expresiones de sus autores y no de los administradores y moderadores (con excepción de los mensajes de estas personas), por lo que en ningún caso *Noticierodigital.com* es responsable de las mismas». Aunque los administradores del foro afirmaron que el Gobierno intenta restringir las críticas y la libertad de expresión, dándose cuenta de la polémica generada por los *posts*, procedieron a eliminarlos y a suspender a los usuarios que los habían publicado. Mientras tanto, Chávez exigió a los fiscales que tomaran medidas de inmediato contra el sitio, y fue más allá, al pedir más controles sobre Internet. Son palabras del presidente: «Internet no puede ser una cosa libre, que se haga y se diga lo que sea, ¿verdad? No, cada país tiene que poner sus reglas y sus normas, como los canales que entran a Venezuela por cable, por satélite. Eso no puede ser así, que transmitan lo que les dé la gana, envenenando la mente de mucha gente».

Ese se tornó un caso paradigmático y ejemplo claro de que el usuario no tiene sus derechos aclarados y, por lo tanto, están desprotegidos. Además, ha servido de excusa para discursos amenazadores a la libertad de expresión y a la red. Frente a ese caso, Chávez y sus aliados políticos han expresado críticas cada vez más duras a los sitios de redes sociales como Twitter y

28. «Habla el tuitero del Metro: “Me detuvieron por hacer fotos del caos cotidiano”», en *Noticias24*, del 2 de noviembre de 2010, disponible [en línea] en: <<http://www.noticias24.com/actualidad/noticia/178935/habla-el-tuitero-del-metro-me-detuvieron-por-hacer-fotos-del-caos-cotidiano>>. [Nota del editor: consultada el 6/11/11.]

Facebook. Dijeron que estos sitios son usados por sus rivales para difamar a funcionarios públicos. En el mismo sentido, CANTV, la empresa de telecomunicaciones estatal venezolana, anunció que planea establecer un filtro centralizado y controlado por el Gobierno por donde pasaría todo el tráfico de Internet. Aunque Franco Silva, presidente de CANTV, negó que la medida fuera a ser usada para controlar el acceso a la red, son afirmaciones preocupantes para los defensores de la libertad de prensa y de expresión.

III.B.I.e. COLOMBIA. En la legislación colombiana, los crímenes de preconcepción racial, étnico, xenofobia, etc. se concentran en la categoría de crímenes de racismo y discriminación en general. La Constitución de Colombia prevé en el Capítulo I del Título II «los derechos fundamentales» del ciudadano y establece en su artículo 13 la libertad y la igualdad ante la ley. El artículo 13 enumera como inaceptables las distinciones entre ciudadanos en razón de «sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica». En el Código Penal, estos derechos son resguardados bajo el título «Delitos contra personas y bienes protegidos por el derecho internacional humanitario». El artículo 144 del Código hace referencia a los actos de terrorismo y el artículo 147 a los actos de discriminación racial. Ninguno de ellos contiene disposiciones específicas sobre la Web. Por otro lado, bajo el tema del discurso del odio, el Código Penal colombiano también prevé el crimen de Apología al Genocidio (artículo 102), tratándolo como un delito que se comete «por cualquier medio real», quedando incluido en la definición, por supuesto, Internet.

En Colombia, hemos visto que el artículo que contiene disposiciones sobre la instigación a delinquir ha sido utilizado para tratar los crímenes de odio en la red. El artículo 348 del Código Penal dispone que es infractor «el que pública y directamente incite a otro u otros a la comisión de un determinado delito o género de delitos». Esta disposición podría ser utilizada para tratar con conductas discriminatorias en la red. Aunque no haya mención alguna de filtrado de contenido, la pena acaba por incurrir en prácticas de filtrado, incluso amenazas a usuarios.

El caso más reciente involucró a Nicolás Castro, estudiante de 23 años, creador de un grupo en Facebook en que amenazaba de muerte al hijo del ex presidente Álvaro Uribe, Jerónimo Uribe. Nicolás fue acusado por el delito de instigación a delinquir, por el cual podría quedar sujeto a una pena de entre 6 y 15 años de cárcel. Nicolás fue el primer colombiano castigado por una amenaza virtual. El proceso empezó en 2009. Además de exigirle el cierre de la página, las autoridades encarcelaron a Nicolás. El caso ha causado polémica

en el país. Aunque la mayoría de las voces de las redes sociales reprochan el mensaje de odio atribuido a Nicolás, muchos manifestaron críticas en el sentido de que no sería motivo para una medida criminal. Muchas fueron las respuestas indignadas por el hecho de que una broma, aunque reprochable, deje un joven en la cárcel por más tiempo del que se han encarcelado criminales paramilitares. También se destacó que existen muchos otros grupos en Facebook que siguen existiendo aunque explícitamente inviten a asesinar a: Hugo Chávez, George W. Bush, Armando Maradona, Shakira y a otros personajes de televisión o integrantes de tribus urbanas como los Emos y Punks. Incluso la senadora Piedad Córdoba se sumó al debate desde su cuenta en Twitter, afirmando que al menos 20 grupos en Facebook convocaron a otros para matarla, pero ninguno ha sido procesado²⁹. La abogada de Nicolás defendió a su cliente afirmando el derecho a la libertad expresión en la red social. El caso sigue bajo análisis.

En los artículos 220 a 226 de su Código Penal, Colombia prevé el delito de calumnias e injurias. Ambos delitos conllevan una pena de prisión y multas que se incrementan en el caso de que el delito «se cometiere utilizando cualquier medio de comunicación social u otro de divulgación colectiva o en reunión pública». Además, el artículo 222 prevé la injuria o calumnia indirecta, que establece que «quedará sometido a las mismas penas quien haga publicar, reproducir, repetir la injuria o calumnia imputada por otro, o quien haga la imputación de modo impersonal o con las expresiones: se dice, se asegura u otra semejante».

Esos tipos penales se han utilizado como base para los cargos contra los periodistas de Internet, como Alfredo Molano³⁰ –acusado de injuria y calumnia por publicar la columna «Araújo et al»– en el periódico *El Espectador*, y Claudia López³¹ –acusada por los mismos delitos al divulgar información

29. «Twitteros piden libertad de Nicolás Castro y convocan a marcha en Facebook», en *Semana.com*, del 3 de diciembre de 2009, disponible [en línea] en: <<http://www.semana.com/nacion/twitteros-piden-libertad-nicolas-castro-convocan-marcha-facebook/132196-3.aspx>>. [Nota del editor: consultada el 6/11/11.]

30. «Juez absolvió al periodista Alfredo Molano en caso de calumnia e injuria» en *El tiempo.com*, del 9 de febrero de 2010, disponible [en línea] en: <<http://www.eltiempo.com/archivo/documento/CMS-7158467>>. [Nota del editor: consultada el 6/11/11.]

31. «Colombia: Jueza absuelve a una columnista acusada de injuria y calumnia», en *El economista.es*, del 25 de febrero de 2011, disponible [en línea] en: <<http://www.eleconomista.es/flash/noticias/2857083/02/11/Colombia-Jueza-absuelve-a-una-columnista-acusada-de-injuria-y-calumnia.html>>. [Nota del editor: consultada el 6/11/11.]

sobre el financiamiento de la campaña presidencial de Ernesto Samper Pizano por el cartel de Cali-. Afortunadamente, ambos fueron absueltos.

III.B.I.f. ARGENTINA. La legislación argentina sobre los crímenes de odio está basada, sobre todo, en la ley antidiscriminación, Ley 23.592 de 1988. Para fines de nuestro análisis, se destaca entre sus disposiciones el artículo 3:

Art. 3º.- Serán reprimidos con prisión de un mes a tres años los que participaren en una organización o realizaren propaganda basados en ideas o teorías de superioridad de una raza o de un grupo de personas de determinada religión, origen étnico o color, que tengan por objeto la justificación o promoción de la discriminación racial o religiosa en cualquier forma.

En igual pena incurrirán quienes por cualquier medio alentaren o iniciaren a la persecución o el odio contra una persona o grupos de personas a causa de su raza, religión, nacionalidad o ideas políticas.

Es posible considerar que esa ley prohíbe el discurso racista y de odio también en Internet. Pero la verdad es que las interpretaciones de este tipo han sido polémicas. Eso se verificó justamente en un debate jurisprudencial de 2000, cuando la *Cámara Federal de Apelaciones de San Martín, Buenos Aires, determinó que la venta de literatura u objetos nazis* en el sector de subastas de Yahoo! no era un crimen punible por la ley antidiscriminación. La Cámara afirmó, además, que la venta de ese material en el ámbito *offline* tampoco estaba prohibida. El tribunal determinó, por lo tanto, que «el sitio de subastas no incita a la discriminación ni al odio; ahí únicamente se venden objetos de la simbología nazi, y eso no viola la ley».

Esa decisión tuvo dos aplicaciones prácticas. Mientras que los actos no fueron considerados como un delito bajo ley 23.592, fueron objeto de bloqueo de contenido en la red, porque el juez federal determinó que

se comunicará al Ministerio de Relaciones Exteriores Comercio Internacional y Culto que deberá arbitrar todos los medios a fin de que Yahoo Inc! se abstenga de exhibir ofertas y acercar a las partes, interviniendo en forma directa o indirecta en el proceso de comercialización y/o difusión de objetos y simbología que reavivan el pensamiento y la doctrina nacionalsocialista ofendiendo el orden y la moral pública contraviniendo normas vigentes.

Esa resolución también es criticable, porque los técnicos no encontraron la forma de hacer realidad el pedido del juez. El Ministerio de Relaciones

Exteriores ha informado que hay imposibilidades técnicas y jurídicas para hacer efectiva la disposición. Por un lado, no se puede evitar la emisión de Yahoo! en la Argentina y, por otro, existe el problema de cómo aplicar a una empresa extranjera, que almacena sus datos fuera del país, una decisión de la justicia local.

Más allá de esa ley, en 2005, mediante el Decreto 1086, la Argentina puso en marcha su Plan Nacional contra la Discriminación, que trata sobre discriminación, xenofobia y racismo. En ese plan están previstas acciones para:

Arbitrar los medios para ejercer un seguimiento y control estatal efectivos sobre formas y contenidos de los medios de comunicación estatales, privados, comunitarios e Internet que incluyan cualquier tipo de discriminación, prejuicio, burla, agresión y/o estigmatización a distintos grupos o sectores de la población que por sus características puedan ser víctimas de discriminación.

Se sugiere crear un Observatorio de la Discriminación en los Medios de Comunicación Masiva dependiente del COMFER y crear un área específica dentro del INADI. Se busca

formular una política de contenidos para sitios web orientada a sancionar a proveedores de Internet que alberguen sitios con información discriminatoria y/o xenófoba, como modo de impedir su capacidad de difusión.

Este es un tema polémico, que puede dar lugar a cuestionamientos sobre muchas de las disposiciones legales de los países bajo análisis. El caso nos enseña que podemos estar de acuerdo o no con que sea permitido subastar artículos asociados a la simbología nazi, pero seguramente hay consenso de que es peligroso que se pidan bloqueos contra sitios pornográficos, o de determinadas religiones o posiciones polémicas. La consecuencia sería que grandes empresas como Yahoo! adopten la política de admitir solo los sitios que sean «políticamente correctos». Eso implicaría dar un paso atrás en la diversificación que nos permite Internet, que fue concebida inicialmente como un espacio abierto y de debate democrático para que, a través de procesos dialécticos de análisis de discursos en contra y a favor de un mismo tema, se llegue a decisiones y posiciones razonables. En ese sentido, en 1997 la declaración presidencial sobre Libertad de Expresión en Internet ha asegurado algunas protecciones constitucionales al contenido en Internet, pues como hemos visto, la línea entre censura y prohibición de contenidos ofensivos es tenue.

Para los casos de injuria y calumnia, podemos formular consideraciones interesantes sobre el caso de Argentina. En 2009, el país aprobó varios cambios en su Código Penal, atenuando la punibilidad de esas conductas. De manera que hoy en el Código Penal, para la calumnia (artículo 109) y para la injuria (artículo 110) están previstas simplemente penas de multa, sin cárcel:

Artículo 109: La calumnia o falsa imputación a una persona física determinada de la comisión de un delito concreto y circunstanciado que dé lugar a la acción pública, será reprimida con multa de pesos tres mil (\$ 3.000.-) a pesos treinta mil (\$ 30.000.-). En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas.

Artículo 110: El que intencionalmente deshonrar o desacreditar a una persona física determinada será reprimido con multa de pesos mil quinientos (\$ 1.500.-) a pesos veinte mil (\$ 20.000.-). En ningún caso configurarán delito de injurias las expresiones referidas a asuntos de interés público o las que no sean asertivas. Tampoco configurarán delito de injurias los calificativos lesivos del honor cuando guardasen relación con un asunto de interés público.

Este es un gran paso hacia adelante para garantizar la libertad de prensa, ya que reduce la posibilidad de la imposición de sanciones desproporcionadas o injustas. Eso es lo que Nora César, titular de la comisión de Legislación Penal de la Cámara de Diputados de Argentina, defendió en entrevista a TÉLAM: «La libertad de prensa es un pilar intocable para este Gobierno, de la que todos los periodistas gozan, como tal vez no haya ocurrido en otras administraciones»³². Los medios de comunicación virtuales también quedarían comprendidos en esa protección, pues, debido a la amplitud de las disposiciones del Código Penal argentino, las leyes sobre difamación y calumnia se pueden aplicar a Internet.

III.B.II. Remoción de contenidos que violen el derecho de autor

La protección jurídica de los derechos de autor ha sido invocada con frecuencia para la remoción de contenido de la red y para la implementación

32. «Diputados aprobó el proyecto que despenaliza las calumnias e injurias», en *Télam*; *sine data*, disponible [en línea] en: <<http://www.telam.com.ar/vernota.php?tipo=N&dis=1&sec=1&idPub=165957&id=322148&idnota=322148>>. [Nota del editor: consultada el 6/11/11.]

de mecanismos de filtrado. Hay que entender que la protección de obras intelectuales puede representar una limitación a la libertad de expresión.

La mayoría de las leyes de derechos de autor en América Latina no tratan directamente sobre la protección de obras intelectuales a través de Internet, y tampoco contienen disposiciones sobre procedimientos específicos para la remoción o el filtrado de contenido que infrinja los derechos de autor en la World Wide Web. De esta manera, los titulares de derechos autorales utilizan leyes generales sobre la protección de la creación intelectual en cualquier medio o soporte, y extienden la interpretación de estas disposiciones al ámbito digital.

Por ejemplo, la ley brasileña de derecho de autor (Ley 9610/98), dispone que la distribución no autorizada de contenido está sujeta a la «suspensión de la divulgación» (artículos 102 y 105), la indemnización (art. 103) e incluso a la destrucción de las máquinas utilizadas para realizar el ilícito (art. 106).

La protección de los derechos de autor en Brasil está establecida en la Constitución Federal, que dispone que «pertenece a los autores el derecho exclusivo de utilizar, publicar o reproducir sus obras, transmisible a los herederos por el tiempo que la ley estipule» (art. 5, XXVII). La protección de los derechos de autor en la Constitución ha generado un curioso discurso en el sentido de considerar que la tutela autoral sería un derecho absoluto. Por un lado, es cierto que los derechos de autor deben ser garantizados, pero por otro, la libertad de expresión y otros derechos fundamentales deben ser ponderados junto con la protección de los derechos de autor.

El discurso que solo toma en cuenta la protección de los derechos de autor y la total represión, sin considerar cómo esos derechos deben convivir con otros derechos fundamentales, es fuente de la mayoría de los casos de contenido de Internet que fue llevado *offline* a pesar de haber existido buenos argumentos legales a favor de su mantenimiento.

Varias comunidades de la red social Orkut, operada por Google, han sido bloqueadas o removidas sobre la base de denuncias extrajudiciales que determinaban que las comunidades incurrieran en una violación a los derechos de autor. Uno de los casos más notorios fue la eliminación de la comunidad Discografía, que recomendaba enlaces a través de los cuales se podía descargar canciones y álbumes en MP3³³.

33. «Orkut perde sua maior comunidade para troca de músicas», en *Folha.com*, del 16 de marzo de 2009, disponible [en línea] en: <<http://www1.folha.uol.com.br/folha/informatica/ult124u535222.shtml>>. [Nota del editor: consultada el 6/11/11.]

Aún basándose en la legislación autoral, los sitios que reproducen leyendas de series televisivas y películas han sido objeto de notificaciones extrajudiciales. El caso de la página web *legendas.tv* es un buen ejemplo de cómo el mecanismo de notificaciones extrajudiciales ha servido para restringir la publicación de contenido cuya ilegalidad sería, al menos, fácilmente cuestionada frente al régimen de las limitaciones y excepciones al derecho de autor³⁴.

El sistema de notificaciones ha recibido una especial atención en razón del Proyecto de Ley para la reforma de la Ley de Derecho de Autor en Brasil. En su artículo 105-A, ese proyecto dispone la responsabilidad solidaria del proveedor de hospedaje de contenido si este no impide el acceso al supuesto contenido ilegal luego de haber sido notificado por la víctima del daño. El proyecto de ley está redactado de la siguiente forma:

Art. 105-A. Los responsables por alojar contenidos en Internet pueden ser solidariamente responsables, en conformidad con el artículo 105, por daños y perjuicios derivados por tornar pública obras y fonogramas sin la autorización del titular, si es notificado por el propietario ofendido y no toma las providencias para, en el marco de su servicio y dentro de un plazo razonable, tornar indisponible el nombrado contenido infractor.

De manera distinta de lo que ocurre en Brasil, Venezuela tiene una Ley de Delitos Informáticos que estipula las penas para varias conductas que considera ilícitas en Internet. En relación con los derechos de propiedad intelectual, esta norma dice:

Artículo 25.- Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

34. «APCM pede retirada do site Legendas.TV do ar por infração de copyright», en *IDG Now!**, del 3 de febrero de 2009, disponible [en línea] en: <<http://idgnow.uol.com.br/internet/2009/02/03/apcm-pede-retirada-do-site-legendas-tv-do-ar-por-infracao-de-copyright/>>. [Nota del editor: consultada el 6/11/11.]

Tratar las violaciones de los derechos de autor en el ámbito de la legislación penal se justifica por la especificidad del derecho penal, que, en general, no permite analogías. Por resultar en penas más severas que las del derecho civil e incluir medidas de restricción de la libertad, la legislación penal se ha convertido en un recurso común para prevenir la comisión de violaciones de derechos de autor e, indirectamente, fomentar prácticas de filtrado de contenido.

La Constitución colombiana determina que «el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley» (art. 61). Como miembro de la Comunidad Andina, el país es signatario del Régimen Común sobre Derechos de Autor y Derechos Conexos (la Decisión 351 de 1993) que ofrece amplios derechos a los autores. Su Ley de Derecho de Autor (Ley 44 de 1993) complementa este régimen y añade penas por delitos contra los derechos de autor, incluyendo:

Artículo 55.- Las publicaciones, ejemplares, reproducciones, moldes, planchas, matrices, negativos, cintas, carátulas o etiquetas incautadas serán sometidos a inspección judicial con la ayuda del perito, y una vez demostrada por este medio su ilegitimidad, serán destruidas por las autoridades de policía judicial, en presencia del funcionario judicial y con citación de la defensa y la parte civil.

El Código Penal colombiano trata sobre la protección de los derechos morales y patrimoniales del autor en los artículos 270 e 271, y sobre la protección de los mecanismos de defensa de estos derechos en el artículo 272. El artículo trata sobre mecanismos técnicos y tecnológicos para proteger los datos almacenados en los ordenadores, Internet y televisión vía satélite, lo que implica la posibilidad de aplicar tales disposiciones al ámbito digital.

Frente a eso, la Corte Suprema colombiana, al tratar de copia de música, tiene una decisión paradigmática, de 2008, sobre la difusión por medio de Internet de material protegido por el derecho de autor. Acerca de esta decisión, aclara Carolina Botero:

El precedente que sienta esta sentencia no es despreciable, afirma que la copia cuando no hay ánimo de lucro no es delito y le da un alcance restringido al concepto de «ánimo de lucro» al vincularlo con una escala económica, reconoce la importancia de las excepciones y su aplicabilidad en el entorno penal como un elemento subjetivo del delito que el juez debe considerar, dice

que solamente «usar» un software sin poder exhibir su licencia no es delito y, aunque solo sea a título de ejemplo, involucra el tema de las descargas en Internet con lo cual el análisis al menos deberá ser considerado por otros jueces cuando se enfrenten a un caso de estos³⁵.

En Chile, hubo una reforma significativa de la Ley de Derecho de Autor. Por un lado, las multas y penalidades para crímenes contra los derechos de autor fueron aumentadas; y por otro, también se desarrollaron mecanismos para evitar la arbitrariedad y la censura previa. Hoy día, en Chile, los proveedores de servicios de Internet no tienen responsabilidad total por los contenidos que sus usuarios hacen disponibles en Internet y el filtrado de contenidos solo puede ocurrir por decisión judicial.

La importación por parte de los países latinoamericanos de soluciones adoptadas por países europeos o norteamericanos para el combate a las infracciones a los derechos autorales ha caracterizado los últimos años de la evolución legal del tema en la región. En ese sentido, prácticas como el corte de la conexión de Internet después de recibir notificaciones por violar derecho de autor, como la de la Ley Hadopi, de Francia³⁶, empezaron a aparecer como proyectos de ley en Latinoamérica.

En Brasil, por ejemplo, el proyecto de ley de autoría del Diputado Federal Bispo Gê Tenuta propuso el corte de la conexión a la red después de la cuarta notificación de una supuesta violación de derecho autoral. Después de mucha controversia, el Proyecto de Ley 5361/2009 fue descartado. Según el diputado, los debates apuntaron que «sería imposible diferenciar aquellos que sacan provecho de la piratería como un negocio y los jóvenes que utilizan Internet para escuchar música, como era en el pasado, cuando gravábamos la radio en cinta casete»³⁷.

35. «equinoxio: La Corte Suprema de Justicia sienta precedente sobre “ánimo de lucro”, “uso personal”, etc.», en *carobotero-co*, del 9 de mayo de 2008, disponible [en línea] en: <<http://www.karisma.org.co/carobotero/index.php/2008/05/09/equinoxio-la-corte-suprema-de-justicia-sienta-precedente-sobre-animo-de-lucro-uso-personal-etc/>>. [Nota del editor: consultada el 6/11/11.]

36. PROJET DE LOI favorisant la diffusion et la protection de la création sur internet, de junio de 2008, disponible [en línea] en: <<http://www.senat.fr/leg/pjl07-405.html>>. [Nota del editor: consultada el 6/11/11.]

37. «Bispo Gê desiste de copiar o modelo francês de perseguição aos compartilhadores», en *trezentos*, del 21 de agosto de 2009, disponible [en línea] en: <<http://www.trezentos.blog.br/?p=2752>>. [Nota del editor: consultada el 6/11/11.]

Afirmaciones como esta muestran cómo el filtrado de contenido basado en la protección de derechos de autor representa una situación evidente de los efectos negativos de los mecanismos de filtrado frente la libertad de expresión y el derecho de acceso, por afectar situaciones legítimas y generar represión imprecisa y contraproducente para la propia.

III.B.III. Remoción de contenidos de carácter sexual

III.B.III.a. BRASIL. La ley brasileña trata sobre crímenes de ultraje público al pudor en el Código Penal. Entre sus disposiciones, el artículo 234 criminaliza la venta y exposición pública de un «objeto obsceno» como un crimen de menor potencial ofensivo. Hay que acordarse de que una conducta común en la convivencia social no puede, al mismo tiempo, ser considerada relevante para el derecho penal. En el caso de esa disposición, la doctrina ha entendido que con la Constitución Federal (CF) post dictadura, está asegurada la garantía a la libertad de expresión, así que no se puede hablar sobre punibilidad en relación con esa previsión legal. De hecho, en razón de los cambios en la costumbre social, la represión a ese delito decrecía aún antes de la Constitución de 1988 con la abolición de la censura por el artículo 5º, IX de la CF. Ese tipo penal es casi ineficiente, caso contrario, no serían permitidas las salas especiales de cine porno, sex shops, revistas o canales de televisión que contienen material pornográfico. Estos son todos materiales y formas de negocios tolerados por la sociedad y autorizadas por el poder público, que incluso pagan impuestos para ello. La mayor parte de la jurisprudencia entiende que las conductas ahí previstas no deben ser penadas, porque el bien jurídico tutelado, o sea, el sentimiento común de pudor público, ha cambiado sustantivamente. Ya no hay aceptación social para esa disposición, dado que existe una causa supra legal de exclusión aceptada por la doctrina moderna y por la jurisprudencia. Ese razonamiento se extiende a la publicación de contenidos pornográficos en Internet.

Pero, obviamente, hay otra cuestión con relación a los contenidos pornográficos que, definitivamente, debe ser rechazada por la sociedad: la pornografía infantil. Ese tema es abordado en la redacción del Estatuto del Niño y del Adolescente-ECA (Ley 8069/90). Ese estatuto fue enmendado por la Ley 11829/08, específicamente para abordar casos en la red, de manera que los artículos 241 a 241-C, definen las penas por diversos delitos relacionados con pornografía infantil en Internet y otros medios de comunicación.

La ley establece un sistema de responsabilidad de toda la cadena de la pornografía, pues además de penar a aquellos que producen, registran o dirigen el contenido ilegal, pena también a aquellos que agencian, facilitan, reclutan, coaccionan, o de cualquier manera actúan como intermediarios para la participación del niño o adolescente en las escenas pornográficas (artículo 240, § 1º). También están sujetos a penas aquellos que venden, exponen, publican, distribuyen, adquieren o almacenan esa clase de imágenes.

Específicamente sobre responsabilidad de los proveedores, el párrafo §2º del artículo 241-A responsabiliza a aquellos que viabilizan el acceso o almacenamiento del contenido ilícito desde que «el responsable para la prestación de servicio, oficialmente notificado, deje de deshabilitar el acceso al contenido ilícito del que trata el enunciado del artículo».

Es importante notar que esa ley tiene, por lo tanto, una disposición sobre filtrado bastante equilibrada con el derecho a la libertad de expresión, porque no establece que el proveedor debe ser notificado para que sea responsabilizado. No crea, por lo tanto, ninguna clase de restricción a priori que obligue a los proveedores a vigilar toda clase de contenido que se transmita en su red, lo que sería una grave violación a la privacidad del usuario. Sin embargo, de hecho los responsabiliza para que retiren el contenido.

La ley también establece un mecanismo de denuncia. No está penada la conducta de quienes almacenan el contenido con el objetivo de informar sobre el mismo a las autoridades competentes. Además de la iniciativa pública, por medio del Ministerio Público, esa clase de delitos también podían ser denunciados vía Safernet, que es una organización civil de derecho privado que coopera con las instituciones públicas.

Aunque esa ley ya tenga disposiciones precisas y adecuadas, también existe la intención de ampliar la responsabilidad de los proveedores. Fruto de una Comisión Parlamentaria de Investigación (CPI) sobre la Pedofilia, el Proyecto de Ley 494/08 pretende responsabilizar los proveedores de acceso aunque no sean notificados. Consideramos que un reglamento así es oneroso para los proveedores y puede poner en riesgo la innovación en la red. Además, el tema ya se encuentra bastante protegido por la legislación vigente. Aunque el tema sea de la máxima importancia, y extremadamente sensible, hay que hacer un balance entre todos los derechos que deben ser protegidos. En Brasil, el combate a la pornografía infantil en Internet ya está apoyado por una legislación que trata sobre los usos en Internet. Han existido operaciones exitosas basadas en el ECA. Como ejemplo, podemos mencionar

las operaciones Carrossel I³⁸ y Carrossel II³⁹, en las cuales la Policía Federal dio cumplimiento con varias órdenes de búsqueda y cumplió varias de búsqueda y aprehensión basadas en el artículo 241 y siguientes.

Es importante notar que Safernet, la misma organización que ha presionado por un nuevo marco legal, recientemente perdió su contrato de cooperación técnica con el Ministerio Público Federal de San Pablo. El Ministerio comunicó, en noviembre de 2010, que la organización no presenta condiciones satisfactorias para atender a la demanda de procesamiento y análisis de las notificaciones que recibe de los usuarios de Internet a través de su «central nacional de denuncias». Ahora, con el fin de la asociación, los usuarios deben realizar sus denuncias a través del sistema Digi-denúncia. El acuerdo anterior establecía que las denuncias fueran recibidas por Safernet. Safernet, luego de investigar los enlaces, debía transmitirlos a las autoridades. Según el MPF, las denuncias acumuladas llegaron a 40 mil, entre ellas, los técnicos del MPF encontraron 27 pruebas de delitos graves que no fueron pasadas por Safernet. Estos son indicios de que más allá de que haya cambios en la ley, son necesarios arreglos institucionales para investigar denuncias.

III.B.III.b. VENEZUELA. En Venezuela se estableció un sistema de control legal sobre las actividades de material pornográfico en Internet. El país tiene tres leyes que tratan sobre el tema: la Ley Especial contra los delitos informáticos, la *Ley Orgánica de Protección al Niño, Niña y del Adolescente* (LOPNA) y la Ley para la Protección del Niño y del Adolescente en Salas de Uso de Internet, Videojuegos y otros Multimedia.

La primera establece las reglas básicas para la actividad pornográfica en Internet. Según el artículo 23, toda la difusión de material pornográfico debe estar precedida por una advertencia sobre el contenido. La disposición siguiente, el artículo 24, rechaza específicamente la pornografía infantil al penar la exhibición pornográfica de niños o adolescentes en la red.

38. «MPF/BA: economista é denunciado por disponibilizar via internet materiais de pornografia infantil», en *Ministério Público Federal*, del 29 de abril de 2011, disponible [en línea] en: <http://noticias.pgr.mpf.gov.br/noticias/noticias-do-site/copy_of_criminal/economista-e-denunciado-por-disponibilizar-via-internet-materiais-de-pornografia-infantil>. [Nota del editor: consultada el 6/11/11.]

39. «Operação Carrossel II combate pornografia infantil pela Internet», en *SaferNet Brasil*, del 3 de septiembre de 2008, disponible [en línea] en: <<http://www.safernet.org.br/site/noticias/oper%C3%A7%C3%A3o-carrossel-ii-combate-pornografia-infantil-pela-internet>>. [Nota del editor: consultada el 6/11/11.]

En la LOPNA, se establecen los derechos y deberes básicos de los niños. Entre ellos, el artículo 33 regula el derecho a ser protegidos contra abuso y explotación sexual. Junto con el artículo 24 de la ley anterior, esas son las únicas disposiciones legales que tratan sobre la pornografía infantil en el país, ya que las otras disposiciones tratan principalmente sobre la clase de contenidos que pueden ser accesibles a los niños. Así son los artículos 74 y 79 de la LOPNA, que prohíben el acceso de los niños a cierto contenido indebido. Por otra parte, la ley de salas de Internet regula el uso adecuado de los servicios de Internet con fines educativos. Entre sus disposiciones, esta ley establece prácticas de filtrado necesarias en salas de acceso a Internet. El artículo 10 de la ley establece que todas las salas de juegos computarizados, electrónicos o multimedios y de Internet están obligadas a implementar controles, mecanismos de seguridad y programas en las computadoras y equipos destinados a niños, niñas y adolescentes para hacer cumplir las disposiciones de la ley. Asimismo, establece que los proveedores de servicios de Internet deberán suministrar estos controles, programas, y mecanismos de seguridad a todos sus usuarios de manera gratuita.

III.B.III.c. COLOMBIA. En 2009 Colombia aprobó, por medio de la ley 1336/09, una serie de enmiendas a la legislación (Ley 679 de 2001 y Ley 599 de 2000) para combatir la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes, incluso en la red. Así, la reformulación del artículo 218 de la Ley 599/2000 define que practica pornografía con personas menores de 18 años quien «fotografie, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, transmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad».

Frente a esa definición, la ley 1336/09 establece un párrafo para el artículo 10 de la Ley 679/01. Este artículo prevé la actuación del Ministerio de Comunicaciones por medio de denuncias y con poder de aplicar multas y bloquear sitios web. El nuevo párrafo otorga competencia al Ministerio de Comunicaciones para exigir toda la información que considere necesaria a los proveedores de servicios de Internet para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. El párrafo se refiere específicamente a reglas de filtrado al definir que se podrá:

1. Requerir a los proveedores de servicios de Internet a fin de que informen en el plazo y forma que se les indique, qué mecanismos o filtros de control están utilizando para el bloqueo de páginas con contenido de pornografía con menores de edad en Internet.

2. Ordenar a los proveedores de servicios de Internet incorporar cláusulas obligatorias en los contratos de portales de Internet relativas a la prohibición y bloqueo consiguiente de páginas con contenido de pornografía con menores de edad.

Los proveedores de servicios de Internet otorgarán acceso a sus redes a las autoridades judiciales y de policía cuando se adelante el seguimiento a un número IP desde el cual se produzcan violaciones a la presente ley.

Además, así como ocurre en Venezuela, también trata de los café de Internet, estableciendo la obligación de que esos sitios tengan un reglamento de uso público adecuado, cuya violación genere la suspensión del servicio al usuario o visitante.

III.B.III.d. ARGENTINA. La Argentina todavía no tiene una legislación específica sobre pornografía infantil en la red o sobre pornografía en general. Existen, sin embargo, iniciativas locales para regular este tema. Este es el caso, por ejemplo, de la ciudad de Buenos Aires que optó por incorporar en la Ley 451 del municipio:

Artículo 1°.- Los establecimientos comerciales que, en el ámbito de la Ciudad Autónoma de Buenos Aires, brinden acceso a Internet, deben instalar y activar en todas las computadoras que se encuentren a disposición del público, filtros de contenido sobre páginas pornográficas.

Artículo 2°.- El/la titular o responsable del establecimiento comercial puede desactivar los filtros de contenido en sus equipos de computación, cuando los usuarios de los mismos sean mayores de 18 años. (Conforme texto Art. 1° de la Ley N° 943, BOCBA N° 1604 del 08/01/2003)

O sea que, como en otros países, la Argentina trata la protección de niños por medio del establecimiento de mecanismos de filtrado. Es importante destacar que esa ley trata sobre cibercafés, mientras que la Ley Federal 25.690 establece que los proveedores deberán proveer a los usuarios filtros que sean fácilmente configurables por los usuarios para decidir por ellos mismos qué contenidos no desean acceder. Esta es una solución interesante, y menos restrictiva, que respecta tanto la estructura de la red como la protección de los niños por medio de la autodeterminación de los usuarios.

III.B.III.e. CHILE. El principal marco legal chileno que regula la pornografía en la red es la Ley 19.927 de 2004 que altera los Códigos Penal, de Procedimiento Penal y el Procesal Penal en materia de Delitos de Pornografía Infantil. Dentro del paquete de alteraciones realizadas por la ley, está el cambio del artículo 366: «El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años será sancionado con presidio menor en su grado máximo».

La terminología «cualquiera que sea su soporte» claramente incluye en el ámbito de la ley la pornografía infantil en Internet. Además de esta ley, existen algunos proyectos en trámite, como el proyecto que pretende introducir en el Código Penal previsiones para casos de *grooming* y *morphing*, formas de seducción y abuso de menores que tienen soporte necesariamente en Internet.

Por otro lado, aunque Chile tiene una unidad contra crímenes sexuales que monitorea sitios webs de pornografía infantil y procesa a los individuos que vendan, guarden, o intercambien pornografía infantil en Internet, no hay informes de que el Gobierno monitoree los e-mails o salas de chat con otros propósitos.

III.B.III.f. MÉXICO. México también trata específicamente la pornografía infantil en Internet en su Código Penal. El artículo 202 describe el delito como «quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos». Está incluida, por lo tanto, Internet como herramienta para la realización del delito. No solo la difusión, sino también el almacenamiento están prohibidos:

Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

No hay, todavía, ninguna disposición sobre filtrado de contenido; solo hay una sanción por tornar disponible contenido y/o almacenarlo.

IV. Actuación de los proveedores de servicios⁴⁰

El debate sobre los efectos de los mecanismos de filtrado no puede ignorar el papel de los proveedores de servicios y los problemas que su implementación genera en la práctica, especialmente cuando el filtro es requerido por orden judicial. Para finalizar nuestro análisis, en esta sección se dará especial énfasis a los proveedores que operan sitios de contenido cooperativo, porque esos sitios ilustran claramente los desafíos de la preservación de la libertad de expresión y la preservación de otros derechos en Internet.

El filtrado de contenido realizado por proveedores de servicios, cuando es ordenado judicialmente, a menudo resulta de acciones indemnizatorias que traen acumulativamente un pedido de compensación financiera y otro de la prohibición de que el contenido continúe disponible en la web.

En el caso de los sitios de colaboración, el contenido que aparece en la página web no es generado por una central de edición, sino por sus propios usuarios, que incorporan fotos, videos, archivos de música o texto. Ese contenido puede ser de autoría o propiedad del usuario y deberá adecuarse a los términos de licencia de contenido del sitio en cuestión.

Sin embargo, cuando las imágenes, textos y videos musicales son de autoría de otros o cuando la propiedad de los derechos es de un tercero –y su uso no se ajusta a las hipótesis de excepciones y limitaciones a la protección autoral–, se debe solicitar una autorización. En casos en que no haya un permiso para mostrar u otros usos de la obra, más allá de los usuarios que expusieron contenido no autorizado, las empresas o personas que explotan esos sitios colaborativos, o sea, los proveedores de servicios de Internet, podrían ser procesados por uso indebido del contenido.

Lo mismo se aplica a los casos ya comentados sobre contenidos fuera de la esfera del derecho de autor que causan daño a los demás, cuando

40. Es importante aclarar que en la categoría de ISPs incluimos tanto a los proveedores de conexión como a los proveedores de servicios o contenidos. Esa diferencia es bastante clara, por ejemplo, en el texto legal del Marco Civil de Internet de Brasil, que impone diferentes responsabilidades, de acuerdo con la clase de ISP de que se trate. En esa sección, trataremos solo sobre proveedores de servicios y no sobre los proveedores de conexión, por el hecho de que para estos últimos entendemos que no se debe aplicar ningún mecanismo de filtrado que no sea por requisitos técnicos de gestión de la red.

se analiza la posibilidad de responsabilizar los proveedores de servicios por manifestaciones de sus usuarios, sea a través de los comentarios que expresan prejuicios de género, origen étnico, opción sexual, etc.

En esas acciones judiciales, es común que el autor, además de una indemnización por los daños ocasionados, le pida al juez que prohíba la utilización del material objeto de la acción. Esta prohibición, impuesta al proveedor que opera el sitio web, por lo general determina que la multa se aplicará a cada nueva violación de los derechos de los demás.

El problema con estos fallos de los tribunales se encuentra en el mecanismo de filtrado que los proveedores deben tener de manera de impedir que los derechos de otros no sean violados por sus usuarios. Ese filtro puede ser cuestionado en términos de eficacia y por los efectos adversos que puede causar al desarrollo tecnológico, creativo e innovador de los usos de la red. Principalmente, el efecto adverso sería la posibilidad de que el filtrado interfiera con contenido que no es el objeto de las acciones, o que interfiera sobre la neutralidad de red.

En primer lugar, es necesario hacer algunas críticas a la elección de los mecanismos de filtrado de contenido como forma de proteger a los derechos de los demás. Hay varias demandas que han solicitado la retirada de contenidos por supuestas violaciones de derechos, lo que implica no solo una infracción al derecho de autor, sino, también, violaciones al derecho a la imagen y a la privacidad. Por otra parte, esas informaciones pueden ser consideradas importantes para el desarrollo y por tanto, estar protegidas por las leyes de libertad de expresión.

Entonces, una dificultad preliminar en el debate sobre el filtrado consiste en determinar cuáles serían los criterios para determinar qué mecanismos de filtrado deben adoptarse. El mecanismo utilizado determinará lo que puede o no aparecer en un sitio web. La mayoría de las decisiones judiciales que ordenan la eliminación de algún material de una página web solo requiere al demandado que se cumpla con la decisión. Sin embargo, no se especifican los términos a utilizar para establecer el filtro, qué expresiones estarían prohibidas, etc. La consecuencia de esta incertidumbre acerca de los métodos a adoptar para poner en práctica el filtrado resulta en que los proveedores utilicen su propio criterio.

Es curioso darse cuenta de que, en ese punto, la incertidumbre presentada por las decisiones judiciales puede actuar tanto a favor como en contra del reo. Esto es así porque, por un lado, se otorga libertad para decidir la forma de filtrar el contenido que se encuentra protegido por alguna regulación, y, por otro, permite volver a demandar si el filtrado no está funcionando

como se planteaba con la decisión imprecisa –o sea, si el video, texto, foto o música vuelvan a ser mostrados en Internet–. En esta segunda etapa, es probable que se intente aplicar las sanciones más graves, al tratarse de un caso de incumplimiento de una decisión judicial. Lo que no parece estar claro en las decisiones judiciales es que muchas veces el incumplimiento de lo establecido deriva precisamente de la dificultad técnica de excluir algunos contenidos, especialmente de los sitios web colaborativos. Este problema se agrava por el silencio de la propia decisión acerca de cómo debería realizarse el filtrado.

Es cierto que el acusado siempre debe adoptar la postura de colaborar para la eliminación del daño. Dejar al demandado decidir sobre cómo filtrar el contenido acaba por imponer una carga excesiva para la empresa o persona que opera el sitio, ya que deben tomar decisiones complejas acerca de la visualización de contenido en línea, optando por determinado mecanismo de filtrado y aún corriendo el riesgo de ser cuestionado otra vez en los tribunales si su decisión sobre la forma de eliminar el daño resulta ineficaz. Este es precisamente el escenario de total desincentivo a la innovación que además puede ser explotado por prácticas abusivas contra el derecho de libertad de expresión y acceso a la información y ni siquiera responder al objetivo por el cual se realizó.

Se puede afirmar que la indefinición sobre los criterios de filtrado es un problema inicial en el análisis de este mecanismo como potencial generador de efectos negativos para el desarrollo tecnológico. Pero hay al menos otras tres consideraciones que pueden hacerse sobre el manejo de los filtros que pueden contribuir a comprender las consecuencias de las demandas de indemnización. Es posible afirmar que el filtrado por decisión judicial es (i) ineficaz; (ii) va más allá de los límites específicos para los que fue requerido y (iii) afecta la neutralidad de la red⁴¹.

Se dice que el filtrado es ineficaz porque en el estado actual de desarrollo tecnológico no hay cómo garantizar con precisión que determinado contenido no esté disponible en sitios web de naturaleza colaborativa. Esto es así porque los medios para burlar el filtrado son simples y están

41. Estos tres efectos negativos del filtrado ya fueron explotados, desde otra perspectiva, por Affonso Pereira de Souza, Carlos, Pedro de Paranaguá Moniz y Sérgio Branco Vieira Júnior, «Neutralidade da rede, filtragem de conteúdo e interesse público: reflexões sobre o bloqueio do site Youtube no Brasil», en *Revista de Direito Administrativo* 246 (septiembre/diciembre de 2007); p. 67 y ss.

en constante actualización, tornando el bloqueo de determinado contenido una verdadera persecución hacia los nuevos modelos de burla de las reglas y técnicas de control.

En el caso de tribunales que determinan que el bloqueo sea realizado en sitios web colaborativos sin indicar ninguna metodología para hacerlo, la empresa o persona que opera el sitio web pasan a tener la obligación de crear las condiciones para evitar que el contenido objeto de la demanda vuelva a ser reincorporado por sus usuarios. Aunque la prohibición pueda estar incluida en las normas sobre el uso de la página, como los términos y condiciones de uso, de hecho, tornarlas eficientes es una cuestión de código fuente, o sea, de tecnología, que pasa a tener fuerte un impacto en los efectos de la regulación⁴². Aunque se determine que todo el sitio sea removido, como ocurrió en Brasil cuando todo YouTube fue prohibido por algunas horas frente a una demanda por derecho a la imagen, existen medios tecnológicos por los cuales los usuarios pueden acceder al contenido, como por ejemplo, utilizando un servidor proxy⁴³ y evitando así las reglas de filtrado.

Además, es importante destacar que la prohibición de que determinados sitios web muestren determinado contenido no impide que otros sitios, incluso fuera de la jurisdicción nacional, lo hagan, lo que perpetúa el daño por la red. Esta es exactamente la tercera prueba sugerida por Lawrence Lessig en el dictamen emitido en el caso de Napster: ¿cuál sería la eficacia de una demanda por daños y perjuicios con intención de suspender las actividades de una red de intercambio de archivos si no hay un mecanismo de filtrado perfecto? La respuesta a esa clase de pregunta sería simplemente la migración de sus usuarios a otros sitios web, donde el daño puede continuar.

En este punto, la afortunada ausencia de un centro de control de la red es una característica que impide la adopción de mecanismos de filtrado que abarcarían todas las formas de visualización de contenidos en Internet, lo que dificulta que se pueda llevar a cabo la responsabilidad y su función compensatoria. Vale la pena mencionar que esta descentralización ha asegurado un pluralismo cultural y una libertad de expresión nunca antes experimentada en los medios de comunicación.

42. Véase Lessig, *supra* nota 9.

43. Cfr. «Sites estrangeiros ridicularizam bloqueio do YouTube no Brasil», disponible [en línea] en: <<http://tecnologia.terra.com.br/noticias/0,,OI1337230-EI12884,00-Sites+estrangeiros+ridicularizam+bloqueio+do+YouTube+no+Brasil.html>>. [Nota del editor: consultada el 6/11/11.]

Tim Berners-Lee, considerado uno de los «padres» de Internet, al detallar las perspectivas que se podrían adoptar para la construcción de su arquitectura ha señalado que

entre las inspiraciones de carácter mercadológico e ideales humanistas, nos dimos cuenta de que la adopción de una perspectiva de control sería una decisión equivocada. La red ha sido diseñada de manera que no haya un centro en donde los usuarios necesiten registrar un nuevo servidor u obtener la aprobación para la inclusión de nuevos contenidos. Cualquier persona puede crear un nuevo servidor o insertar nuevos contenidos. Hablando filosóficamente, si la Internet debe ser un bien universal, debería crecer sin limitaciones. Hablando tecnológicamente, si hubiera un punto de control, rápidamente se convertiría en un cuello de botella para el crecimiento de la Internet, que nunca ganaría la escala deseada. Su falta de control era lo importante⁴⁴.

Por lo tanto, se puede concluir que los reclamos de indemnización que son decididos en favor de mecanismos filtrado de contenido, en general, son soluciones poco eficientes que contribuyen a generar impactos negativos en la innovación y en el desarrollo tecnológico a través de Internet.

Esos efectos se hacen aún más claros cuando nos damos cuenta de que el filtrado va más allá de los límites específicos para los cuales se ordenó, ya que no son raras las veces en que los mecanismo de filtrado, implementados para atender al orden judicial, terminan restringiendo el acceso a otros contenidos y no solo a aquellos cuyas opiniones se solicitó que se prohibieran⁴⁵. Por

44. Bernes-Lee, Tim, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor*, Nueva York, HarperCollins, 1999, p. 99. En el mismo sentido, haciendo hincapié en que el propósito es crear un canal de difusión de información en Internet cada vez más amplia, sin ningún tipo de control de la calidad de lo que se transmite de esta manera, véase Rossi, Giuseppe, «Il cyberlaw tra metafore e regole», en *Rivista di Diritto Civile*, año XLVIII, N° 06 (noviembre/diciembre de 2002), p. 798.

45. Se hizo famoso en Internet por bloquear sitios web que informaban sobre la exploración espacial de Marte mediante un vehículo robot de la NASA (National Aeronautics and Space Administration), ya que la mayoría de los filtros colocados en las computadoras de su casa para controlar la navegación de los niños, solo restringe el acceso a sitios web que contienen la palabra 'sexo'. En inglés, uniendo las palabras 'Mars' (Marte) y 'exploration' (exploración), el resultado es la palabra *vie*, la que desbloquea los sistemas de filtrado. Véase Callahan, Tom, «Only 2 Libraries Adopt Filters for the Internet», en *The New York Times*, del 14 de mayo de 2000, disponible [en línea], <<http://query.nytimes.com/gst/fullpage.html?res=9D00E2D8163BF937A25756C0A9669C8B63>>. [Nota del editor: consultada el 6/11/11.]

ejemplo, si se implementa un filtrado por palabras clave, es posible que otros materiales, lícitamente insertados en determinado sitio web colaborativo, también sufran restricciones por las mismas terminologías, obras con títulos idénticos, o muy parecidos. Eso evidencia que los mecanismos de filtrado necesitan ser mejorados constantemente para que su adopción sea mínimamente segura sin que terceros, que no tengan nada que ver con la acción indemnizatoria, sufran sus efectos.

Como refuerzo de la incómoda posición de los proveedores de contenido de Internet, está el hecho de que la persona que se sienta afectada por la remoción o filtrado indebido de contenido puede tomar medidas judiciales para que su obra vuelva a estar disponible en la red. Los proveedores pueden intentar evitar acciones como esas incluyendo en sus términos y condiciones de uso explicaciones de que las obras expuestas pueden verse afectadas por demandas judiciales. Aun así, no se puede descartar la posibilidad de que los mecanismos de filtrado generaren nuevos problemas para el negocio del proveedor.

O sea, nuestro escenario hipotético se inició con una situación en la que había solo una víctima (el autor de la obra disponible sin autorización), y pasó a un segundo momento en el que hay una nueva víctima, que comenzó a tener problemas justamente por la solución que se trató de tomar para remediar el daño de la primera víctima, o sea, por el mecanismo de filtrado.

Ese escenario reduce de manera significativa el espacio para la innovación en Internet, porque los nuevos proveedores podrán simplemente optar por no adoptar nuevos modelos de negocios por temor de que sean responsabilizados por los actos de sus usuarios. En el caso de las infracciones al derecho de autor, la responsabilidad de las empresas que operan redes *peer-to-peer* podría conducir a desalentar el desarrollo de esa tecnología, que seguramente no se destina solo a la producción de actos ilícitos, como se estableció en el precedente del caso Betamax.

Sobre estos problemas, Casimiro de Vasconcelos Sofia señala que estas tecnologías «sin embargo, presentan algunos problemas que parecen insuperables y que se relacionan con el hecho de que bloquean más contenido de lo previsto, lo que puede dar lugar a una censura encubierta»⁴⁶.

En Brasil, el Tribunal de Justicia del Estado de Sao Paulo tuvo la oportunidad de decidir un caso en el que la empresa Anima Producciones Audiovisuales Ltda., titular de los derechos de autor de la película *Pelé*

46. Vasconcelos Casimiro, Sofia de, *A Responsabilidade Civil pelo Conteúdo da Informação Transmitida pela Internet*, Coimbra, Almedina, 2000; p. 39.

Eterno, que retrata la vida y la carrera del jugador de fútbol, presentó una demanda para remoción de los clips de la película que estaban en YouTube. De acuerdo con los datos del proceso, más de cien video clips han sido creados por los usuarios, algunos incluyendo comentarios, nuevas imágenes, prácticas de remix o *mash ups*, etc. Esas prácticas fueron considerados usos indebidos de la obra⁴⁷. De la decisión del Agravo de Instrumento, se destaca:

3. Independientemente del derecho de la autora obtener cualquier beneficio efectivo derivado del uso de su obra, insistiendo en la remoción del contenido de la web, por falta de autorización o transferencia de derechos, considerando que hay un delito de reproducción no autorizada, en que los demandados se aprovechan de las imágenes de terceros, aunque otros elementos fueron incorporados, todavía se nota la unidad artística de la demandante, razón por la cual es imprescindible acoger el recurso, frente a la presencia de los requisitos mencionados en el artículo 273 del Código de Proceso Civil, una vez comprobada la verdad entre las alegaciones y la pruebas presentadas, así como el temor fundado de daños irreparables o de difícil reparación.

[...]

5. Con base en lo anterior, se anticipa la tutela, para que las requeridas eliminen el contenido de sus sitios web, bajo pena de multa diaria de \$1,000.00, con condición de que la sanción pecuniaria no se aplicará en el caso de compartir videos que ya están circulando en la red, cuyo bloqueo sería técnicamente imposible, de manera que se excluye la responsabilidad por eventual propagación de dicho contenido a través de «links» alternativos en sitios o portales diferentes, incluso por el reemplazo del video en los propios sitios de las requeridas que sea hecho por terceros, todo ello sin perjuicio de la indemnización por daños que les cabe como criadoras y mantenedores de los servicios, en caso de que sea procedente la acción por indemnización.

La decisión señala claramente las dificultades del mecanismo de filtrado y adopta una postura cautelosa sobre la imposición de responsabilidades

47. TJSJP, Agravo de Instrumento n° 497 958 4/7-00; rel. Des. Testa Marchi; j. em 13.03.2007.

por los videos que se pueden encontrar en Internet⁴⁸ por medio de links alternativos⁴⁹ cuyo bloqueo es imposible.

Finalmente, y en refuerzo a los efectos negativos de la adopción de mecanismos de filtrado como resultado de demandas judiciales, es preciso señalar que esas prácticas afectan la neutralidad de la red.

En el caso paradigmático de la modelo brasileña Daniela Cicarelli, mencionado anteriormente, más allá de la decisión de la remoción del video en cuestión de YouTube, la decisión emitida por el Tribunal de Justicia de San Pablo determinó que, al no ser capaz de evitar la presentación del video, el acceso a los sitios web demandados debería ser cancelado en el territorio nacional⁵⁰.

Esta decisión alcanzó a millones de usuarios de Internet en Brasil al determinar el bloqueo total al sitio web. Aunque la nueva decisión, publicada un día más tarde, aclaró que la determinación judicial no tenía ese sentido, dos empresas que operan los *backbones* de la red brasileña llegaron a bloquear el acceso al sitio web, atendiendo al que parecía, por los términos de la decisión, ser objeto del orden judicial.

El bloqueo de todo un sitio por la exhibición de un único video que supuestamente lesionaba, en el caso en cuestión, los derechos de imagen y intimidad de dos personas, demuestra cómo la adopción de filtrado es una solución negativa para el ejercicio de una serie de derechos fundamentales, y no resuelve los intereses de los autores. La adopción de los mecanismos de

48. Debido a que la acción se ha introducido en contra de la empresa Google Brasil Internet Ltda, la solicitud incluye no solo la eliminación de partes de la página web YouTube, sino, también, la eliminación de la página web Google Videos, ambos operados por la parte demandada.

49. Parece estar sentado en la doctrina nacional e internacional que la persona que establece un vínculo a una página no puede ser responsable por el contenido que encontrará allí. Este entendimiento se basa, principalmente, en el hecho de que el contenido de la página en cuestión se puede cambiar sin que esto sea notado por el autor del enlace. La dinámica de la rendición de cuentas como un simple comportamiento podría generar no solo una baja en el incentivo para que sean hechas las conexiones entre las páginas electrónicas, que es una de las principales características atractivas de la World Wide Web, pero no requieren de un monitor compatible con la mayoría de las actividades realizadas en línea. En este sentido, véase Petillion, Flip y Sophie Huart, «La responsabilité des intermédiaires dans la violation des droits d'auteurs», en *Droits Intellectuels: à la reconquête d'une stratégie pour l'entreprise*, Bruselas, Bruylant, 2002, pp. 577-579.

50. «Leia a íntegra da medida que manda desbloquear o YouTube no Brasil», en *IDG Now!**, del 9 de enero de 2007, disponible [en línea] en: <http://idgnow.uol.com.br/internet/2007/01/09/idgnoticia.2007-01-09.7954769479/IDGNoticia_view>. [Nota del editor: consultada el 6/11/11.]

filtrado está lejos de lograr un equilibrio entre las funciones de responsabilidad civil y la preservación de los derechos fundamentales de la red mundial⁵¹.

En la práctica, en las acciones de indemnización en América Latina, y especialmente en Brasil, se nota que a menudo el titular del derecho ofendido demanda al proveedor de servicios que aloja el contenido. Esa práctica hace que el proveedor que opera un sitio web colaborativo viva en constante amenaza de acciones judiciales. Como medida para evitar nuevas acciones, es de suponerse que se amplíe la práctica de supervisión por parte del proveedor frente al contenido incorporado a su sitio web por los usuarios.

Sin embargo, esta percepción encuentra dos grandes obstáculos. Inicialmente, el monitoreo perfecto de todo el contenido publicado en un sitio web colaborativo requeriría, dependiendo del tamaño de la página web, de la contratación de un equipo para analizar toda la gama de materiales alojados. La inclusión de mecanismos de filtrado automático, como se ha visto, tiene una serie de imperfecciones que solo la observación humana puede corregir, pero la supervisión humana puede fallar en relación a la licitud de la obra en cuestión.

La contratación de personal y de grupos especializados para la lectura y la eliminación previa de los contenidos del sitio web no es suficiente para aplacar el riesgo de posibles demandas judiciales. Esto se debe al hecho de que los criterios para la evaluación de un contenido nocivo y de los derechos de los demás no están claros. En ausencia de un criterio uniforme, seguramente el proveedor optará por el bloqueo y no por el mantenimiento del contenido polémico. Esta clase de decisiones no solo empobrece el mundo de los contenidos relacionados con su sitio web, sino que termina por imponer una especie de censura que discrimina entre lo que se puede y lo que no se puede mostrar en la Internet World Wide Web.

Se da una situación inusual en la que el proveedor, como intermediario entre los usuarios y el público en general, puede resultar una posible víctima. A continuación se presenta un resumen de Ronaldo Lemos:

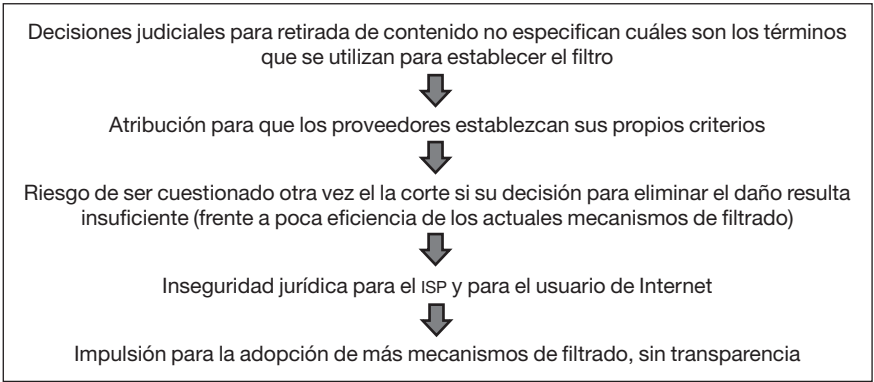
51. Solo como curiosidad, cabe destacar que el mismo día 09 de enero de 2007, cuando TJ / SP aclaró que no requerían el bloqueo de la totalidad de YouTube, senadores de los Estados Unidos trajeron de vuelta a la agenda la discusión sobre la neutralidad de la red, a través de la Ley de Libertad de Expresión en Internet, confrontese Gross, Grant, «Senadores dos EUA recolocam projeto sobre neutralidade na web em pauta», en *IDG Now!**, del 10 de enero de 2007, disponible [en línea] en: <http://idgnow.uol.com.br/internet/2007/01/10/idgnoticia.2007-01-10.8286737443/IDGNoticia_view>. [Nota del editor: consultada el 6/11/11.]

Lo que es sorprendente acerca de la responsabilidad del intermediario en Brasil es que, a diferencia de otros países, no hay criterios legales establecidos para la exención o asignación de responsabilidad a los intermediarios frente a la recepción de una notificación. Por lo tanto, el proveedor de acceso a Internet trabaja en incertidumbre y miedo acerca del resultado de las decisiones judiciales, en ese contexto, es más probable que eliminen el contenido, sin verificación de la legitimidad de la solicitud, una vez que no tienen incentivos para hacerlo de otra manera. Tenga en cuenta que no existe un sistema de predicción de «refugio seguro» en el país, específicamente de eximir al proveedor de su responsabilidad si cumple con determinados requisitos⁵².

La amenaza que ese escenario representa para la innovación en Internet implica necesariamente la reducción deliberada de contenido por parte de los proveedores que, temerosos de recibir sanciones, optan por filtrar contenidos que eventualmente puedan causarles daño. Como ha señalado Ronaldo Lemos, «una gran parte del contenido en la red, aunque legítimo, no tiene ninguna clase de protección legal... con la amenaza a los intermediarios, se puede retirar sin un mayor escrutinio el contenido que podría ser legítimo de la red»⁵³.

Frente a esa tendencia, se observa la creación de un peligroso ciclo vicioso, contrario a los requisitos básicos de la libertad de expresión:

Figura 9 | **Ciclo vicioso, contrario a los requisitos básicos de la libertad de expresión**



Fuente: Elaboración propia.

52. Lemos, Ronaldo, *Direito, Tecnologia e Cultura*, Río de Janeiro, FGV, 2005, p. 125.

53. *Ídem*.

No sería impreciso afirmar que el futuro de la innovación en Internet parece estar amenazado por la adopción de algunas técnicas de filtrado y acciones por daños y perjuicios. Este escenario no es favorable a la creación de nuevos modelos de negocios, ni a la innovación. El equilibrio entre la preservación de los derechos legítimos (como la honra, el derecho de autor, etc.) y la libertad para llevar a cabo actividades innovadoras que utilizan la tecnología, incluso para garantizar otros derechos, como el de la ciudadanía y de la libertad de expresión se encuentra en riesgo y es imprescindible que esas cuestiones se tomen en cuenta en ese momento particular de reglamentación de Internet por el cual pasan los países de América Latina, de manera que el futuro de Internet en la región se garantice y esté fundamentado en los principios de libertad, apertura y neutralidad de red.

V. Conclusiones

El tema del filtrado de contenido de Internet tiene difícil delimitación. Por un lado, es cierto que la aplicación de esos mecanismos implica en una restricción a la libertad de expresión. Por otro, existen algunas excusas legales para hacer lugar al filtrado, como por ejemplo, los casos de pornografía infantil. Esas excusas han sido utilizadas para realizar prácticas de filtrado que se han ampliado a cada nuevo caso denunciado y a cada nueva tecnología desarrollada. Así, frente a excusas de protección de derecho de autor y protección al honor, inadvertidamente, pasan a ser aceptables verdaderos mecanismos de censura previa, algo ampliamente rechazado por los principales tratados de derecho internacional firmados por los países bajo estudio, pero que, sin embargo, han sido asimilado por los Gobiernos y las empresas en la intención de restringir el libre flujo de la comunicación en la red global.

Aunque la mayor parte de los países analizados aún no figure con destaque en los informes internacionales sobre los países «enemigos» de la libertad de expresión en la red, la región tiene una historia de prácticas efectivas de censura a la prensa tradicional, lo que denota una tendencia también hacia los contenidos de la red. Este potencial debe tornarse el centro de nuestras preocupaciones a medida que la región supera el problema de la brecha digital y empieza a regular las prácticas en la red.

De hecho, la región se encuentra en un momento particular porque todos los países viven un momento de regulación de Internet. Se están debatiendo políticas de acceso, leyes de neutralidad de la red y de responsabilidad de

intermediarios. Acerca de regulaciones de contenido, los países analizados tienen disposiciones específicas para prácticas de filtrado solo en sus leyes sobre pornografía infantil. Pero en la mayoría de ellos, aunque las demás regulaciones de contenido no sean específicas para Internet, estas han sido aplicadas en el ambiente de la red. Así es que, de manera preocupante, tipos penales de delitos contra la honra han sido utilizados para el filtrado de contenido político (en México, Venezuela y Colombia, principalmente, pero también en Brasil). Otras razones de filtrado indebido generalmente están vinculadas a la violencia o a la represión de las infracciones al derecho de autor.

Este es el caso, por ejemplo, de las acciones por daños contra los proveedores de servicios que han sido destacadas en nuestro análisis, especialmente contra aquellos que ofrecen redes sociales y mecanismos de búsqueda. Brasil y la Argentina⁵⁴ son ejemplos fuertes de la tendencia de la víctima del daño a iniciar una demanda directamente contra el proveedor (por lo general en casos contra el honor) para solicitar la eliminación de contenidos, la implementación de un mecanismo de filtrado y una indemnización. En Brasil, el amplio reconocimiento judicial de la aplicabilidad del Código de Defensa del Consumidor (Ley 8078/90) favorece ese escenario, porque los tribunales han identificado a la víctima de esa clase de daño con los consumidores perjudicados por un producto defectuoso o un servicio.

Es importante destacar que este estudio trató, en su mayor parte, sobre casos de filtrado provenientes de acciones judiciales, dado que no se tiene acceso a datos de filtrado «voluntario» llevado a cabo por el Gobierno o entidades privadas antes de que el contenido sea objeto de un reclamo. La ausencia de esa clase de información es aún más preocupante si el objetivo es garantizar que la Internet a la que accedemos sea ofrecida de manera de respetar los principios de libertad de expresión, apertura y neutralidad de la red.

Por esa razón, independientemente del motivo para que se establezca algún mecanismo de filtrado, siempre es importante que haya transparencia en cuanto a la utilización de esos mecanismos –y por transparencia se quiere decir que el usuario sea informado de que se realizó un filtrado y por qué–. O sea, si un proveedor de servicio utiliza mecanismos de filtrado voluntario,

54. *Transparency Report*, disponible [en línea] en: <<http://www.google.com/transparencyreport/governmentrequests/AR/?p=2010-12>>. [Nota del editor: consultada el 6/11/11.]

es importante que el usuario sea informado de esos mecanismos en los términos de servicio. Se destaca acá que cuando se trata de los proveedores de conexión no se les debe otorgar ningún espacio para el filtrado de contenido específico. Ellos deben seguir el principio de neutralidad de la red en la administración del tráfico, en relación con cualquier clase de contenido.

Por otro lado, si hubo una orden judicial para la remoción de contenido, es importante que el usuario, al intentar acceder al sitio en donde estaba el contenido removido, sea informado de que el contenido fue bloqueado y por qué. Al menos parte de las órdenes judiciales que, por falta de conocimiento tecnológico de los jueces, han derivado en remociones excesivas podría hacer ese tipo de determinación. El juez debe estar consciente de que si es inevitable el bloqueo de determinado contenido, este debe ser claro y estar delimitado por razones objetivas, proporcionando una definición de estándares adecuados que minimicen la discreción de quien aplique el filtrado y requiriendo transparencia en esas prácticas. Eso es para que la implementación de esas órdenes no vaya más allá del bloqueo o filtrado del contenido específico que se solicita.

En última instancia, debatir si se debe filtrar algunos contenidos que circulan en la red es uno de los temas clave para el futuro de la red y para pensar en una reglamentación que sea capaz de mantener su naturaleza y arquitectura libre y abierta. El análisis sobre las elecciones que son hechas y sobre cómo se da su aplicación nos lleva a darnos cuenta de la complejidad del tema y sirve como un vector para entender y criticar esas mismas opciones que de manera peligrosa han progresado en sentido del control de la conducta y la prevención o reparación de los daños que ocurren a través de Internet. Los delitos en Internet, la privacidad, el comercio electrónico y la libertad de expresión son solo algunas de las cuestiones relacionadas con el debate sobre el filtrado de contenidos en la red. Esta pluralidad de temas señala cómo la discusión acerca de los mecanismos de filtrado pasa por diversas áreas del conocimiento y afecta la manera en que tratamos distintas cuestiones vinculadas a la aplicación de la ley frente a los avances tecnológicos.

Anexo: Cuadros comparativos de la legislación y jurisprudencia de los países analizados

Acceso al servicio de Internet

Derecho de acceso a Internet

Brasil	Venezuela				Colombia	Argentina	Chile	México
Legislación								
Marco Civil de Internet	Decreto N° 825/2000	Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos	Constitución de la República Bolivariana de Venezuela	Ley Orgánica de Telecomunicaciones	Ley 1341/09	Decreto N° 554/97	Proyecto de Reforma Constitucional consagra el derecho al acceso a Internet	Proyecto de ley acerca de los derechos del usuario de Internet
PEC 6/11 - Acceso a Internet como derecho constitucional								
Plan Nacional de Banda Larga					Proyecto de Ley 149/Senado		Más acerca del proyecto	
Casos y Jurisprudencia								

Neutralidad de la red

Brasil	Venezuela	Colombia	Argentina		Chile	México
Legislación						
Ley General de Telecomunicaciones (Lei Geral de Telecomunicações)	La neutralidad de la red en Venezuela	Plan Nacional de Desarrollo: art. 56	Proyecto de Ley S-1491/11	Proyecto de Ley 1159-D-2011	Ley 20453	Reglamento de la neutralidad de la red
Marco Civil de Internet, artículos 2, IV; 9 y 12						
						Ley de Telecomunicaciones, artículo 44
Casos y Jurisprudencia						

Regulación de contenido

Crímenes de odio

Brasil	Venezuela	Colombia	Argentina	Chile	México
Legislación					
Ley de crímenes raciales, artículos 1º y 2º	Ley de responsabilidad social en radio, televisión y medios electrónicos, artículo 28	Constitución política, artículos 11 y siguientes	Convenión internacional sobre la eliminación de todas las formas de discriminación racial	Ley Anti-terrorismo	Ley federal para prevenir y eliminar la discriminación
Código Penal, artículos 140 y 141		Código penal, artículos 102, 144, 147, 201 y ss.	Decreto 1086/05	Ley de Genocidio	
Ley 8.072/90, artículo 2º			Ley N° 23592		
Constitución de Brasil, artículos 5º, XLII; 3º, IV.					
Ley 2.889/56, artículos 1º y 3º					Código penal
Casos y Jurisprudencia					
Caso Marcelo Valle Silveira Mello	Gobierno investiga a blog	Caso Nicolás Castro			
Caso Mayara Petruso	Fiscalía investiga a sitio web	Caso Piedad Córdoba			

Pornografía infantil; contenido obsceno y sexualmente explícito

Brasil		Venezuela		Colombia			Argentina	Chile	México	
Legislación										
Estatuto de la Niñez, artículos 227, 228, 240 hasta 241-D	Proyecto de ley 494/08	Ley Orgánica de Protección al Niño, Niña y Adolescente (LOPNA)	La Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimediales	Código Penal, artículo 218	Ley 679 del 3 de agosto de 2001 sobre Abuso y pornografía de menores en Internet, artículos 7, 8 y 10	Ley 1336 de 2009	Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía	Proyecto de Ley s-0256/11	Ley N° 19927 Proyecto de ley que modifica el Código Penal y criminaliza la pornografía infantil en medios virtuales	Código Penal, artículo 202
Casos y Jurisprudencia										
Operación Carrusel	Hace un par de años hubo una investigación por videos pornográficos de adolescentes colocados en YouTube. La información del caso se acalló al descubrirse que los videos eran publicados por las propias adolescentes involucradas.	Caso Paul Anthony Brailsford	El Juzgado Penal 23 del Circuito de Medellín condenó el pasado enero de 2011 a diez años de prisión a Wilson Hernando Daza Duque por el delito de pornografía con menores de edad. Según se desprende de la investigación, Daza Duque, profesor de música de 34 años de edad, creó un correo en redes sociales para contactar a menores. Luego fotografiaba y amenazaba a los menores con la publicación de las fotos. Tras la denuncia del hecho, el Cuerpo Técnico de Investigaciones de la Fiscalía de Colombia allanó la casa del profesor y lo capturó. Aunque Daza Duque aceptó los cargos, no obtuvo rebaja de pena porque las víctimas eran menores de edad.							

(Continúa)

(Continuación: Pornografía infantil; contenido obsceno y sexualmente explícito)

Brasil	Venezuela	Colombia	Argentina	Chile	México
Casos y Jurisprudencia		<p>No tenemos conocimiento sobre leyes específicas que prohíban contenido obsceno y sexualmente explícito en Internet. Tampoco conocemos de normas generales sobre el tema que se apliquen a Internet. En sentencia T-391/07 de la Corte Constitucional, se hizo un análisis sobre expresiones sexualmente explícitas y soeces en una emisora radial y se estableció que: «Las autoridades gozan de un margen constitucional para establecer limitaciones razonables y proporcionadas sobre la difusión social de este tipo de expresiones, a los efectos de proteger simultáneamente los derechos de los demás, pero sin que ello implique que están facultadas para suprimir estas expresiones o impedir su transmisión a través de los medios de comunicación mediante censura». Creemos que si la Corte Constitucional mantiene su línea jurisprudencial, este criterio puede aplicarse para contenido obsceno y sexualmente explícito en Internet.</p>			

Propiedad intelectual											
Brasil			Venezuela			Colombia			Argentina	Chile	México
Legislación											
Ley de derechos autorales, artículos 7º, xlii; 33; 41; 101 hasta 109	Ley del Software	Decreto 1355/94	Constitución de Brasil, artículo 5º, xxviii	Ley Especial contra Delitos Informáticos	Convenio de Berna	Ley 23 de 1982	Tratado de la OMPI sobre derecho de autor	Tratado de la OMPI sobre interpretación o ejecución y fonogramas	Reforma de la Ley de Propiedad Intelectual	Ley de Derechos Autorales Mexicana	
					Constitución Política, artículos 6 y siguientes	Código Penal, título VIII	Régimen Común sobre Derecho de Autor y Derechos Conexos	Ley 44 de 1993			
Casos y Jurisprudencia											
										Caso Guillermo Vélez	

Calumnias e injurias (difamación)

Brasil	Venezuela	Colombia	Argentina	Chile	México
Legislación					
Código Penal, artículos 138 hasta 145	Podrían aplicarse las disposiciones con respecto a delitos contra la reputación incluidas en el Código Penal	Código Penal, artículos 220 y siguientes	Ley 26551	Código Penal Ley 26551	Código Civil
Código electoral, artículos 324, 325 y 326					
Casos y Jurisprudencia					
	Caso <i>Noticiero Digital</i>	Caso Claudia López	Caso Alfredo Molano		
	Caso Jesus Majano				
	Caso Cristian Fuentes				

Prohibiciones generales

Brasil	Venezuela	Colombia	Argentina	Chile	México
Legislación					
Proyecto de ley 84/99 - PL Cibercrímenes	Ley General de Bancos	Ley de <i>habeas data</i>	Proyecto de ley s-0209/09		
	Newsletter Nº 1 legal TIC				
Casos y Jurisprudencia					
	Caso <i>dólar paralelo</i>	Caso <i>El Liberal venezolano</i>			Leyes generales sobre telecomunicaciones en México

Bloqueo de contenido, remoción de contenido, filtrado

Bloqueo de servicios basados en la web 2.0

	Venezuela					Chile	México
Brasil							
Legislación							
Casos y Jurisprudencia							
Caso Cicarelli	Detienen a ingeniero por sus comentarios en Twitter.	Ciudadanos detenidos por opinar en Twitter.	Comisión de medios solicita a la fiscalía investigar redes sociales en Internet				

Bloqueo de páginas web

Brasil		Venezuela		Colombia		Argentina	Chile	México
Legislación								
Proyecto de Ley 7439/2010	Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos	La Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimediales	El cierre, bloqueo o limitación al acceso de páginas de Internet se puede dar por dos razones: a) por razones preventivas: para evitar el acceso por parte de menores de edad a páginas web que puedan afectar su desarrollo y su educación, así como por petición de los suscriptores o usuarios; b) en casos de pornografía infantil y hechos relacionados: al tratarse de una conducta punible, el bloqueo de acceso es un deber de los proveedores de servicios de Internet, además de ser una sanción aplicable por las autoridades respectivas.	Ley 25690/02				
	Ley para Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimediales		Resolución 1732 de 2007 de la Comisión de Regulación de Comunicaciones, artículos 113 y 114 Decreto 1524/2002, artículo 6-5 Ley 679/2001, artículo 4					
Casos y Jurisprudencia								
Generalmente, los casos de bloqueo involucran la protección de la privacidad o daños morales o materiales causados por contenido en Internet. No tenemos conocimiento de casos específicos.	Frecuentemente (al menos un viernes por mes), los usuarios del servicio de ABA-CANTV (empresa de telecomunicaciones propiedad del estado venezolano) se quejan de la imposibilidad de acceso a sitios web. Los sitios con frecuencia más afectados son blogs alojados como Blogger o WordPress, así como las páginas <i>Noticiero Digital</i> (www.noticierodigital.com) y <i>Chiguire Bipolar</i> (www.elchiguirebipolar.net). El Gobierno no reconoce la existencia de ningún mecanismo de bloqueo.		Un ejemplo de cierre de páginas web por parte de la policía judicial se presentó el pasado mes de noviembre de 2010. En esta ocasión, se reportó que una operación colombiana investigativa contra la pornografía infantil permitió el cierre de 5 000 páginas web, luego de detectar la descarga digital de fotografías y videos desde conexiones a Internet. También se reportó el bloqueo por parte de Telefónica-Telecom de una página de Internet denominada <i>rapidshare</i> , con un tráfico de 60 000 personas, por «políticas de ética y requerimientos del Ministerio de Tecnologías de la Información y las Comunicaciones». Finalmente, en 2010, la Corte Constitucional solicitó a De justicia que descolgara de su página web la identificación y referencias a una niña cuya adopción por parte de la pareja homosexual de su madre biológica estaba siendo analizada gracias a una acción de tutela, en la que nuestra organización presentó una intervención ciudadana.					

Notice and Take Down

Brasil		Venezuela	Colombia	Argentina	Chile	México
Legislación						
Ley de derechos autorales, artículos 102 a 110	Proyecto de ley 84/99-PL Cibercrímenes	Ley de responsabilidad social en radio, televisión y medios electrónicos				
Casos y Jurisprudencia						
			No existen en Colombia disposiciones legales específicas basadas en el principio de «notificación y retirada». Existe, sin embargo, una aplicación general del principio de <i>notice and take down</i> entre técnicos, basada en la práctica general de EEUU y en caso de que se llegara a firmar el tratado de libre comercio con dicho país (TLC).			

Bibliotecas y cybercafés

Brasil		Venezuela	Colombia	Argentina	Chile	México
Legislación						
Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedia, artículos 8 y 10	Ley para la Prohibición de Videojuegos y Juguetes Bélicos	Ley 1336 de 2009, artículo 4				
Casos y Jurisprudencia						
						Datos sobre cybercafés en México

Mecanismos de denuncia

Brasil		Venezuela	Colombia	Argentina	Chile	México
Legislación						
Privados:	Públicos:	Público: la Ley de responsabilidad social en radio, televisión y medios electrónicos y el CONATEL	Existe una ruta para la denuncia, control y seguimiento de páginas de internet con contenidos de pornografía infantil que parte del reporte de las denuncias a las unidades especializadas de delitos sexuales de la Fiscalía. Si la denuncia es pertinente, sigue el trámite en el Cuerpo Técnico de Investigación (CTI), la Oficina de Asignación de la Fiscalía, para asignar fiscal responsable, y la comisión al cuerpo técnico de investigación judicial, para realizar la investigación penal.			
Safernet	Ministerio Público Federal-Grupo de Combate a los Crímenes Cibernéticos					
Campaña Nacional de Combate a la Pedofilia en la internet	El Ministerio Público Federal es reglamentado por la Ley N° 75/93					
Casos y Jurisprudencia						
En Safernet, es posible denunciar los siguientes temas: pornografía infantil, racismo, apología o incitación a crímenes contra la vida, xenofobia, neonazismo, malos tratos en contra de los animales, intolerancia religiosa, homofobia y tráfico de personas. Es posible denunciar cualquier contenido ofensivo al Ministerio Público Federal.			Proyecto Internet Sano, del Gobierno, pero hay participación del sector privado.			

Licencias y responsabilidad

Responsabilidad de los ISPs

Brasil		Venezuela	Colombia	Argentina	Chile	México
Legislación						
La empresa ISP puede constituirse como cualquier otra persona jurídica. Debe dejar en claro que entre las actividades que componen su objeto social están la prestación de servicios de acceso o de información en la red. Si el servicio de acceso a Internet se ofrece vía radio o por tecnología ADSL, se necesita una licencia de Agencia Nacional de Telecomunicaciones.	Marco Civil de Internet	Ley de responsabilidad social en radio, televisión y medios electrónicos	Ley 1341/2009, artículos 10 y 15			Ley Federal de Telecomunicaciones
Casos y Jurisprudencia						

Responsabilidad de los buscadores y proveedores de contenido

Brasil		Venezuela	Colombia	Argentina	Chile	México
Legislación						
Marco Civil de Internet	Ley de derechos autorales	Ley de responsabilidad social en radio, televisión y medios electrónicos				
Casos y Jurisprudencia						

La determinación de la jurisdicción en litigios por difamación por contenidos en Internet: algunas observaciones para América Latina

Eduardo Bertoni¹

Introducción

El derecho penal incluye en su catálogo de conductas prohibidas los delitos por difamación. Los *nomen juris* que se le han dado a los diversos tipos penales en América Latina van desde las injurias hasta las calumnias, la contumelia y otras descripciones que, en general, tienden a proteger el bien jurídico «honor», entendido tanto desde su aspecto objetivo (reputación) como subjetivo (autovaloración). Sin perjuicio de las distintas teorías que fundamentan el derecho penal, podría decirse que la inclusión del bien jurídico honor como un bien tutelado por el aparato punitivo estatal responde o bien a disuadir que se produzcan daños o puestas en peligro al bien jurídico, o bien a reforzar –mediante la amenaza penal– el valor que una sociedad le otorga en un momento dado al bien jurídico del que se trate mediante la punición de las conductas que lo dañan o ponen en peligro².

1. Agradezco a Andrea de la Fuente –investigadora del CELE– y a Mario Moreno –pasante durante 2010-2011– por su colaboración en la investigación para este trabajo.

2. Al respecto, véase Bertoni, Eduardo, «El bien jurídico tutelado en los delitos contra el honor: ¿sigue siendo el mismo aun después de la sanción de la ley de “*habeas data*”?», en el *Suplemento de Jurisprudencia Penal de la Revista La Ley*, Buenos Aires, marzo de 2001.

Por su lado, el derecho civil también da respuesta a los ataques al honor. Al iniciar una demanda civil por difamación, el presunto damnificado busca obtener una compensación económica por el daño a su imagen, honor, integridad moral o reputación. Sin perjuicio de que distintas jurisdicciones admitan distintas variantes y limitaciones a lo que es accionable en concepto de difamación, lo cierto es que en América Latina se ha incluido como concepto compensable el daño moral producido por la difamación. Ese concepto es de difícil cuantificación.

La base que fundamenta ambas acciones (la penal y la civil) es siempre una expresión. La forma de esa expresión –escrita, verbal, artística– no es determinante de la consecuencia jurídica que se busca, pero la potencia de su diseminación puede ser una de las razones a la hora de determinar, por ejemplo, la cuantía del daño. Sin embargo, el derecho a expresarse es uno de los derechos fundamentales en una democracia³, con lo cual, dependiendo del contenido de la expresión (por ejemplo, una expresión de interés público), puede argumentarse con éxito que las responsabilidades ulteriores (civiles o penales) de una determinada expresión no sean necesarias en una sociedad democrática⁴, y con ello, que no corresponda ningún tipo de consecuencia por la expresión supuestamente dañina.

Consecuentemente con lo expuesto, los jueces deben analizar distintas cuestiones que hacen a la expresión emanada por quienes son llevados a los estrados judiciales, ya sean estos de índole penal o civil. Pero ¿cuáles son los jueces a los que corresponde hacer ese análisis? Esta pregunta, si bien no es nueva, adquiere una relevancia importante cuando la expresión que se imputa como difamatoria ha sido conocida a través de Internet. Sintéticamente, ¿corresponde iniciar la acción judicial ante el juez del domicilio de la víctima, del victimario o hay que tener en cuenta otros criterios? El objeto de este trabajo consiste en tratar de describir cómo se

3. La Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos han apoyado la relación de la libertad de expresión con la democracia en cada uno de los casos en los que han tratado violaciones al artículo 13 de la Convención Americana sobre Derechos Humanos. Al respecto, véase Bertoni, Eduardo, *Libertad de Expresión en el Estado de derecho*, 2ª edic. actualiz., Buenos Aires, Del Puerto, 2007, p. 111.

4. He argumentado que los efectos que se pueden producir por la implementación de responsabilidades posteriores a la expresión pueden equipararse con los efectos que provoca la implementación de los mecanismos de censura previa, y que el efecto inhibitorio de «sanciones» civiles puede ser igual o mayor que el de las sanciones penales. *Íd.*, pp. 95 y ss.

ha respondido a esa pregunta tanto en América Latina como fuera de esa región⁵. Es fundamental destacar que la respuesta que se dé es importante ya que los estándares legales que dan lugar a una determinación judicial de la configuración de un delito o de la existencia de una causa válida para accionar en el ámbito civil varían según la jurisdicción que los regula.

En general, puede decirse que en los Estados Unidos, lo más extendido es accionar por difamación civil, y los tribunales exigen a los litigantes que son figuras públicas que prueben la existencia de «real malicia», que es un estándar difícil de cumplir por los demandantes⁶. El sistema inglés es más amigable para con el demandante que el estadounidense. En América Latina, además de la posibilidad de acceder al reclamo de daños por la vía civil, la mayoría de los países prevén penas de prisión por delitos de difamación.

Como puede advertirse, el juez que resulte competente y la ley que resulte aplicable son fundamentales a la hora de determinar las consecuencias jurídicas de ciertas expresiones: en algunas jurisdicciones, la reparación por medio de una acción civil será más difícil de obtener que en otras jurisdicciones, mientras que en otras jurisdicciones, hasta puede llegarse a la amenaza de cárcel cuando la vía penal esté habilitada.

Como veremos en el presente análisis, en América Latina, tradicionalmente, el tribunal competente ha sido el del lugar en donde se publicó o se tomó conocimiento del contenido considerado difamatorio. En los casos de los medios impresos, ha sido relativamente sencillo determinar el sitio de publicación o el de exteriorización de los dichos presuntamente difamatorios. Los contenidos en Internet que incluyen ediciones electrónicas de publicaciones impresas y blogs e involucran nuevos actores, como los proveedores de servicios de Internet, los buscadores, etcétera, complejizan la determinación del lugar de publicación y el de donde provienen los dichos. Por otra parte, dado que los delitos y acciones por difamación protegen el valor del honor o la reputación, y que estos valores pueden en teoría verse afectados por el grado de extensión de la distribución que permite Internet,

5. Aclaremos que no es el fin de este artículo concentrarnos en cuándo un contenido puede o no ser «difamatorio», o en qué momento, o no, la expresión es parte del derecho a expresarse libremente. Daremos por comprendidas esas circunstancias y pretendemos concentrar nuestros esfuerzos en el estudio de los argumentos que se han dado para otorgar jurisdicción territorial a determinados jueces y no a otros.

6. Véase un estudio sobre el estándar legal de la «real malicia» en Bertoni, *supra* nota 2, p. 141 y ss.

es posible que las publicaciones en Internet influyan sobre la determinación de la existencia de un daño a los bienes jurídicos tutelados. Teniendo en cuenta que conceptos como los de ‘publicación’, ‘edición’ y ‘daño’ han sido factores relevantes en la determinación de la competencia, vale la pena estudiar cómo los tribunales los han valorado en casos de contenidos en Internet al resolver sobre su propia competencia.

En el sistema interamericano de protección de los derechos humanos, los delitos penales de difamación han sido considerados hasta ahora contrarios a la Convención Americana de Derechos Humanos, y varios países han adoptado leyes que despenalizan estos delitos⁷. Los organismos de protección del derecho a la libertad de expresión han destacado durante años el efecto de disuasión respecto a la libertad de expresión que genera la mera posibilidad de ser enjuiciado penalmente por difamación. Este efecto disuasorio ha sido también extendido recientemente a las acciones civiles⁸. Pero particularmente en la órbita penal, si los contenidos de las publicaciones que se encuentran en Internet influyen sobre la determinación de la jurisdicción de modo de extender la potestad jurisdiccional en juicios

7. La idea del efecto intimidatorio que genera la sanción penal para quienes desean expresarse críticamente en cuestiones de interés público germinó en el sistema interamericano con el informe de la Comisión Interamericana de Derechos Humanos sobre la incompatibilidad entre las leyes de desacato y la Convención Americana sobre Derechos Humanos (CIDH, *Informe anual de la Comisión Interamericana de Derechos Humanos*, 1994 e *Informe sobre la compatibilidad entre las leyes de desacato y la Convención Americana sobre Derechos Humanos*, OEA/Ser.L/V/II.88, doc. 9 rev., 17 de febrero de 1995, respectivamente). Esta idea dio frutos en las recomendaciones de la Comisión Interamericana de Derechos Humanos y en las decisiones de la Corte Interamericana de Derechos Humanos, véase, a los efectos, Bertoni, *supra* nota 2, pp. 109 y 110.

8. En los alegatos y reflexiones presentados ante la Corte Interamericana de Derechos Humanos entre el 24 y 25 de agosto de 2011 en Bogotá, Colombia, en el caso iniciado por la revista *Noticias* contra el ex presidente argentino Carlos Menem, el perito experto Roberto Saba sostuvo que un sistema de responsabilidad civil puede afectar o inhibir la libertad de expresión. El perito Julio Cesar Rivera (+), sostuvo, en el mismo sentido, que el artículo 1071 bis constituye una norma vaga y excesivamente amplia, tanto respecto de las conductas prohibidas como en materia de cuantificación del daño moral. Ello resulta particularmente problemático en materia de libertad de expresión, ya que esta clase de normas generan un efecto disuasivo o intimidatorio y además posibilitan una aplicación selectiva y discriminatoria.

Fuente: *Perfil* - Corte Interamericana de Derechos Humanos, «Suplemento Especial: El Juicio Revista ‘Noticias’ vs. Menem», 28 de agosto de 2009, disponible [en línea] en: <http://www.perfil.com/export/sites/diarioperfil/docs/0829_suplemento_CIDDHH.pdf>. [Nota del editor: consultada el 12/11/11.]

por difamación sobre periodistas, bloggers y comunicadores, se estaría verificando una tendencia que va en sentido opuesto a la de disminuir la posibilidad de ser enjuiciado penalmente por difamación. En otras palabras, quienes pretendan impedir expresiones críticas sobre asuntos de interés público, buscarán las jurisdicciones que sean las más «agresivas» contra ese tipo de expresiones.

Las publicaciones en Internet han fomentado la práctica llamada «*turismo de difamación*» («*libel tourism*»). Esto es una forma de elección deliberada de la jurisdicción en la cual se interpone una demanda judicial (*forum shopping*). Al escoger la jurisdicción en la cual litigar, la parte accionante pretende obtener una ventaja sobre la otra parte o partes en el litigio. Un peligro inherente a esta práctica es que los autores incurren en la autocensura al evitar que se reporten situaciones que pudieran dar lugar al inicio de una querrela o demanda por difamación.

Para enfrentar los dilemas que plantea la jurisdicción, pueden intentarse dos caminos. El primero, intentar una solución general para los países por medio de un tratado que se aplique a los casos de Internet. La otra posibilidad es trabajar para lograr la mayor armonización de las reglas de difamación entre los países que lleve a la consecuencia de que no importe el lugar ni la ley que se aplique, porque esta última será pareja e igualitaria en todos los casos. Una tercera solución la ofrece la tecnología: quien se expresa por Internet podría decidir que lo que manifiesta no sea accesible en jurisdicciones que le pudieran traer problemas.

Todas estas propuestas de soluciones no aparecen en el horizonte dentro de nuestra región. Es importante resaltar que la idea de la armonización, en verdad, podría responder a los criterios que fundan la soberanía de los Estados, aunque reinterpretada: en materias vinculadas con Internet, lo que hace un Estado internamente afecta a otros Estados y viceversa, por lo que siempre podría hablarse de un interés compartido de los Estados para armonizar sus legislaciones y, así, no afectar su propia soberanía⁹.

9. Bertrand de la Chapelle, se refiere de esta manera al hablar del conflicto de jurisdicción: Las legislaciones nacionales se mantienen como un instrumento clave para el diseño de políticas públicas. Sin embargo, una proliferación descoordinada de leyes que son potencialmente incompatibles, por ejemplo, aquellas referidas a privacidad o libertad de expresión, generan conflictos de jurisdicción. Es difícil para las plataformas globales respetar una diversidad de reglas. Además, las actividades de las personas desarrolladas en Internet, habitualmente ofrecen una naturaleza transfronteriza, que trae particulares

Asimismo, queremos llamar la atención sobre la última solución –la tecnológica–, que si bien puede proteger a quien se expresa, tiene la consecuencia mediata de que muchas personas a las que le podría interesar esa expresión se verán imposibilitadas de recibirla, afectándose, así, su derecho a la información. Hasta donde conocemos, no se ha planteado la posibilidad de discutir un tratado en nuestra región, aunque la armonización de las leyes de difamación debería venir –aunque está lejos de ser una realidad– de la mano del impulso del sistema interamericano de derechos humanos.

Como ya adelantáramos, en este artículo se examinarán algunas decisiones judiciales en distintos países en litigios por difamación, que han sido iniciados por contenidos originados en Internet, en los que se ha presentado alguna cuestión vinculada a la jurisdicción, con el fin de exponer cómo se ha establecido esta última en esos casos¹⁰. En la sección I, se presentarán algunos casos y soluciones adoptadas en Australia, Canadá, Inglaterra y los Estados Unidos, donde este tema ha tenido un tratamiento especial. En la sección II, se examinarán los criterios adoptados en algunos casos iniciados en América Latina. Finalmente, en la sección III, se formularán algunas observaciones para América Latina a partir de los casos analizados.

Los casos han sido resumidos a partir de fuentes abiertas en Internet y también de compilaciones de casos sobre el problema de jurisdicción en juicios por expresiones en Internet en estudios académicos sobre el tema¹¹.

problemas de *enforcement*. Finalmente, las decisiones domésticas que toma un Gobierno determinado pueden tener efectos directos o indirectos en el territorio de otro. Si la soberanía es la capacidad de ejercer la autoridad suprema sobre el territorio, Internet es un desafío directo al principio de territorialidad de la ley, uno de los componentes del modelo surgido de Westfalia.

Véase en Multistake Holder Governance, «Principles and Challenges of an Innivative Political Paradigm», en *MIND, CO:LLABORATY DISCUSSION PAPER SERIES* No1, #2 Internet Policy Making, una publicación de Internet & Society Co:laboraty, Editor Wolfgang Kleinwächter, 2011 IGF Nairobi Special Issue, 1ª edic., *sine data*.

10. No es objeto de este trabajo llevar adelante una recopilación exhaustiva de decisiones judiciales, sino, antes bien, exponer una suerte de «muestreo» de algunas que consideramos relevantes y que aportan argumentos para reflexionar sobre el tema que tratamos de resolver.

11. Se han recogido casos de las publicaciones de Packard, Ashley, «Wired but Mired: Legal System Inconsistencies Puzzle International Internet Publishers», en *J. INTL MEDIA & ENTERTAINMENT LAW*, 1, 1 (2001), y del *Media Law Resource Center New Developments Bulletin*, de diciembre de 2010.

I. Criterios adoptados en el derecho comparado

I.A. Australia

I.A.I. *Dow Jones c/ Gutnick* (2002)

El caso *Dow Jones v. Gutnick*¹² es emblemático sobre el tema de jurisdicción en casos de difamación en Internet en Australia. La compañía Dow Jones & Company Inc. imprime y publica el *Wall Street Journal* y la revista *Barron's*. A la vez, Dow Jones también opera el sitio web *WSJ.com*, que incluye contenidos de ambos medios antes mencionados.

La edición online de *Barron's* del 28 de octubre de 2000 contenía un artículo titulado «Unholy Gains», en el que se hacía referencia al señor Joseph Gutnick. Al considerar que el artículo lo difamó, inició una acción civil por daños en la Corte Suprema de Victoria—lugar donde residía Joseph Gutnick— contra Dow Jones¹³.

La Corte Suprema de Victoria rechazó la solicitud de Dow Jones de suspender permanentemente el procedimiento. La compañía había alegado que Victoria era una jurisdicción inapropiada para iniciar la acción. En su apelación a la Corte Superior australiana (*High Court*), Dow Jones argumentó que la publicación del artículo había ocurrido en Nueva Jersey, en los Estados Unidos, lugar donde alojaba sus servidores, y argumentó que era preferible que quien publica material en la web pueda gobernar su conducta según el lugar donde se encuentran alojados los contenidos en los servidores—a menos que esa decisión fuese arbitraria—. De lo contrario, argumentó, quien publica no podría evitar que cualquiera descargue el contenido y sea demandado en cualquier lugar. Gutnick pretendía un resarcimiento por el daño a su reputación, que habría sufrido en Victoria.

La Corte Superior australiana (*High Court*) determinó que los contenidos fueron publicados en Victoria cuando los suscriptores de *WSJ.com* descargaron el contenido de la página. La Corte aplicó un estándar de «*jurisdicción claramente inapropiada*», según el cual la Corte se abstendría de ejercer jurisdicción con fundamento en el principio de *forum non conveniens* solo en el caso de que la jurisdicción invocada por el accionante

12. *Dow Jones & Company Inc. v. Gutnick* [2002] HCA 56 (10 December 2002).

13. *Dow Jones v. Gutnick* [2002], *supra* nota 10, párr. 2.

sea claramente inapropiada. Otro principio relevante que aplicó la Corte y que no fue cuestionado por las partes es el principio de que en una acción por daños en la cual existe una conexión con otra jurisdicción fuera de Australia la regla de derecho aplicable para ser utilizada es que las cuestiones de derecho sustantivo son gobernadas por el derecho del lugar de la comisión del hecho que da lugar al daño (*place of commission of tort*)¹⁴.

La Corte determinó que Victoria no era una jurisdicción claramente inapropiada en virtud de que la presunta difamación habría ocurrido allí. La Corte destacó que la causa de acción civil por difamación en Australia se rige por el principio de responsabilidad objetiva y está enfocada en resarcir un daño a la reputación, y que este se configura cuando una publicación es comprendida por un lector u observador. Por ello, la Corte consideró que la publicación debe entenderse como un acto bilateral y no unilateral, y que, ordinariamente, la difamación se habrá producido en el lugar en donde el material se hizo disponible –que generalmente sería donde el contenido es descargado, siempre que el accionante goce allí de reputación susceptible de ser dañada. La Corte agregó que esta bilateralidad de la publicación es la base de la regla según la cual cada comunicación difamatoria da lugar a una causa de acción independiente¹⁵. La Corte destacó que en Australia las reglas sobre el derecho aplicable no requieren de que el lugar de la publicación de material difamatorio sea solo el lugar de la conducta de quien publica. Dado que el daño a la reputación se habría producido en Victoria y que el accionante reclamaba la reparación del daño solamente en ese estado, la Corte consideró que el derecho sustantivo aplicable era el de Victoria¹⁶.

I.B. Canadá

I.B.I. *Black c/ Breeden* (2010)

En el caso *Black c/ Breeden*¹⁷, Conrad Black inició seis acciones por difamación entre 2004 y 2005 ante la Corte Superior de Ontario (*Ontario Superior Court*) contra empleados de la empresa Hollinger International.

14. *Dow Jones v. Gutnick* [2002], *supra* nota 10, párr. 9.

15. *Dow Jones v. Gutnick* [2002], *supra* nota 10, párrs. 25, 26, 27.

16. *Dow Jones v. Gutnick* [2002], *supra* nota 10, párrs. 42, 48.

17. *Black v. Breeden*, 2010 ONCA 547, August 13, 2010, Docket c50380.

Conrad Black es un empresario que ganó su reputación primero en Canadá y luego internacionalmente como dueño y editor de periódicos. Se desempeñó hasta el 2004 como director de Hollinger International, una compañía registrada en Delaware y que ha tenido sedes en Nueva York y Chicago. Black y sus asociados controlaban Hollinger International por medio de dos compañías de Ontario, Hollinger Inc. y The Ravelston Corporation Limited¹⁸.

En 2003, un accionista mayoritario de Hollinger International denunció la ilegitimidad de algunos pagos que habían sido hechos a Black, sus asociados y a las entidades bajo su control. Esto dio lugar a una investigación. El comité especial conformado para este fin concluyó que existieron pagos que no habían sido autorizados debidamente¹⁹.

Al interponer las acciones por difamación, Black alegó que los contenidos en la página de Hollinger International –disponible en Canadá–, que se referían a lo que resolvió el comité y a las disputas legales que le siguieron, eran difamatorios. Arguyó que los contenidos fueron leídos y republicados en Ontario por *The Globe and Mail*, el *Toronto Star* y el *National Post* y que dañaron su reputación en Ontario²⁰.

Los demandados interpusieron una solicitud de suspender la acción con el fundamento de que la Corte de Ontario no tenía jurisdicción y plantearon alternativamente que no era la jurisdicción conveniente. Argumentaron que no existía una conexión real y sustancial entre Ontario y las acciones, y que las jurisdicciones más apropiadas eran los estados de Nueva York o Illinois, en los Estados Unidos²¹. Este planteo fue rechazado.

La Corte de Apelaciones de Ontario (*Court of Appeal for Ontario*) confirmó esta decisión, aplicando el test de jurisdicción (*assumed jurisdiction*) tal como había sido reformulado en *Van Breda c/ Village Resorts Limited* 22(2010)²². Consideró que si bien el juez que había resuelto

18. *Black v. Breeden* [2010], *supra* nota 16, párrs. 8, 9.

19. *Black v. Breeden* [2010], *supra* nota 16, párrs. 10, 11.

20. *Black v. Breeden* [2010], *supra* nota 16, párr. 3.

21. *Black v. Breeden* [2010], *supra* nota 16, párr. 29.

22. 98 O.R. (3d) 721 (C.A.). En *Van Breda*, Sharpe J.A. identificó como la base del test de «conexión real y sustancial» a la conexión que la acción tiene con el tribunal competente y la conexión del demandado con el tribunal competente. El juez consideró que los demás principios del test de *Muscutt v. Courcelles* (2002 CanLII 44957 (ON C.A.)) debían analizarse, no como elementos independientes, sino como herramientas analíticas para determinar estos dos factores principales.

el planteo de suspensión no había realizado el análisis requerido por Van Breda, este había concluido que el objeto de la acción civil (*tort*) había sido cometido en Ontario. La Corte citó al juez que había resuelto el planteo de suspensión cuando expresó que la jurisprudencia era clara en que el corazón de una acción por difamación (*libel*) era la publicación. El juez que había resuelto sobre el pedido de suspensión dijo que

la acción civil por difamación se configura en el lugar donde ocurre la publicación. La publicación tiene lugar cuando las palabras son oídas, leídas o descargadas. Las palabras en cuestión pudieron haber sido formuladas en los Estados Unidos por los directores o asesores de una compañía estadounidense, pero fueron publicados o republicados en Ontario, y se alega que causaron daño en Ontario. La conexión entre el objeto de las acciones y Ontario es significativa²³.

En cuanto a la conexión entre la acción y el tribunal competente, la Corte de Apelaciones de Ontario (*Court of Appeal for Ontario*) consideró que si bien existe un vínculo entre la acción y los Estados Unidos, y que es posible que exista una jurisdicción con más conexión con la acción que Ontario, Van Breda deja claro que el test para asumir jurisdicción no depende de comparar la fuerza de la conexión con otra jurisdicción potencialmente disponible. La Corte consideró que existen daños que claramente se materializaron en Ontario. La Corte de Apelaciones de Ontario (*Court of Appeal for Ontario*) concluyó que los hechos relevantes relacionados con lo que alega Black sobre la publicación en Ontario y el daño por él sufrido respecto de su reputación en Ontario determinan que existe una conexión sustancial entre su demanda y el sitio.

En cuanto a la conexión entre el demandado y el tribunal competente, la Corte de Apelaciones de Ontario (*Court of Appeal for Ontario*) estuvo de acuerdo con el juez que había resuelto sobre el pedido de suspensión en

23. *Black v. Breeden* [2010], *supra* nota 16, párr. 33. A continuación, citamos el texto original:

The case law is clear that the heart of a libel action is publication. The tort of defamation is committed where the publication takes place. Publication occurs when the words are heard, read or downloaded. The statements in question may well have been made in the u.s. by the directors or advisors of a u.s. company, but they were published or republished in Ontario and they are alleged to have caused injury in Ontario. The connection between the subject matter of the actions and Ontario is thus significant. [Footnotes omitted.]

que existió una conexión entre los demandados y el tribunal competente. El juez que había resuelto sobre el pedido de suspensión consideró que los demandados debieron haber tenido conciencia de algunos de los muchos lazos de Black con Ontario o de que este había establecido una reputación significativa en Ontario, utilizando una analogía con la responsabilidad objetiva del productor en casos de productos defectuosos.

I.B.II. *Burke c/ NYP Holdings, Inc. (2005)*

Larry Brooks es un columnista del *New York Post*. Brooks escribió un artículo que se publicó en la edición del 27 de febrero de 2005 del *Post*. La nota se refería a actividades del señor Burke relacionados con un incidente que ocurrió en Vancouver en un partido de hockey y al contenido del testimonio anticipado de Burke en un juicio. Este último inició una demanda civil por difamación en Ontario contra NYP Holdings, Inc, que es la compañía que se encuentra detrás del *New York Post*, al considerar que el artículo lo difamaba. El artículo del señor Brooks estaba disponible en una página web administrada por el *Post*²⁴. El periódico solicitó que la acción en Ontario fuera suspendida y rechazó la jurisdicción de Ontario en el caso. La Corte Suprema de Columbia Británica (*Supreme Court of British Columbia*) decidió que existía *jurisdiction simpliciter*, ya que existía una conexión «real y sustancial» con el demandado o el objeto del litigio. Para llegar a esta conclusión, G.D. Burnyeat, J. sostuvo que

La difamación es una acción por daños (*tort*). El acto dañoso tuvo lugar en Columbia Británica cuando el señor Russell accedió al artículo en la página mientras se encontraba en Columbia Británica. La publicación dentro de Columbia Británica se dio en ese momento, ya que la acción por daños por difamación ocurre cuando las palabras son oídas o leídas: *Berezovsky v. Michaels* et él. [2000] 2 All E.R. 986 (H.L.); *Dow Jones & Co. v. Gutnick*, [2002] H.C.A. 56 y *Wiebe v. Bouchard* [2005] B.C.J. (Q.L.) N° 73 (B.C.S.C.). Al escribir en su página sobre un tema que era de interés a las personas en Columbia Británica, fuesen o no fanáticos del hockey, estoy satisfecho de que fuera previsible que el artículo fuera levantado por los medios en Columbia Británica dada la publicidad que rodeó el incidente en el

24. *Burke v. NYP Holdings, Inc.*, 2005 BCSC 1287, párrs. 2, 4.

partido del 8 de marzo de 2004 y de la reputación del señor Burke en la Columbia Británica. Todos los testigos de lo que el señor Burke pudo haber dicho antes y durante el juego residen en Columbia Británica. Estoy convencido de que el señor Burke ha satisfecho la carga de probar hechos jurisdiccionales suficientes para establecer una conexión real y sustancial con la acción judicial en Columbia Británica. Por lo tanto, encuentro que ha quedado establecida la *jurisdiction simpliciter*²⁵.

En cuanto a la determinación de si existía *forum conveniens*, que en el caso significaba determinar si Nueva York u Ontario era la jurisdicción más apropiada, la Corte aplicó el test de *Muscutt v. Courcelles*, y tuvo en cuenta que el señor Burke era residente en Columbia Británica; que sufrió daños a su reputación principalmente en ese sitio; que el incidente al que se refería el artículo ocurrió en Columbia Británica y que los testigos de lo que el señor Burke dijo o no dijo se encontraban en Columbia Británica para determinar que esta era la jurisdicción más conveniente. Agregó que requerir al señor Burke litigar este caso en el estado de Nueva York lo privaría de una ventaja jurídica significativa, teniendo en cuenta las diferencias entre el derecho de difamación en Columbia Británica y en Nueva York²⁶.

25. *Burke v. NYP Holdings, Inc.*, 2005 BCSC 1287, *supra* nota 23, párr. 29. A continuación citamos el texto original:

Defamation is a tort. The tortious act took place in British Columbia when Mr. Russell accessed the Column on the website while he was within British Columbia. Publication within British Columbia took place at that time as the tort of defamation occurs where the words are heard or read: *Berezovsky v. Michaels et al* [2000] 2 All E.R. 986 (H.L.); *Dow Jones & Co. v. Gutnick*, [2002] H.C.A. 56; and *Wiebe v. Bouchard* [2005] B.C.J. (Q.L.) No. 73 (B.C.S.C.). By publishing on its website a matter which was of interest to people in British Columbia whether or not they were hockey fans, I am satisfied that it was foreseeable that the Column would be picked up by the media in British Columbia given the publicity surrounding the incident at the March 8, 2004 game and the prominence of Mr. Burke within British Columbia. The incident took place in British Columbia. The witnesses to what might have been said by Mr. Burke prior to and during the game all reside in British Columbia. I am satisfied that Mr. Burke has met the onus of establishing jurisdictional facts sufficient to establish a real and substantial connection within British Columbia to the cause of action. Accordingly, I find that jurisdiction simpliciter has been established.

26. *Burke v. NYP Holdings, Inc.*, 2005 BCSC 1287, *supra* nota 23, párrs. 30, 32, 37.

I.B.III. *Bangoura c/ Washington Post* (2005)

En el caso de *Bangoura c/Washington Post*,²⁷ Cheickh Bangoura demandó en 2003 al *Washington Post* y a tres de sus periodistas por considerar que dos artículos que publicó el periódico eran difamatorios. El primer artículo, titulado «Cloud of Scandal Follows UN Drug Control Official: Boutros-Ghali Ties Allegedly Gave Protection», fue publicado el 5 de enero de 1997 y relataba que los colegas del señor Bangoura, de las Naciones Unidas, lo habían acusado de acoso sexual, manejos financieros indebidos y nepotismo durante el ejercicio de su posición como director asistente regional para África del Sur y África del Este sobre el control de drogas en un programa de las Naciones Unidas. Cheickh Bangoura fue suspendido de su puesto, que expiraría a fin de enero de 1997, el 9 de enero de 1997. El 10 de enero de 1997, el *Washington Post* publicó un segundo artículo que relataba la suspensión de Cheickh Bangoura y reiteraba los dichos del primer artículo. Cheickh Bangoura se mudó en 1997 a Montreal, donde vivió hasta junio de 2000, momento en el que se mudó a Ontario²⁸.

El *Washington Post* solicitó la suspensión de la acción judicial, alegando que no existía una conexión real y sustancial entre esta acción y Ontario y entre el *Washington Post* y Ontario. El 5 de enero, solo siete copias del periódico habían sido distribuidas a suscriptores en Ontario, mientras que aproximadamente 1 106 968 copias habían sido distribuidas en el Distrito de Columbia. Los dos artículos también fueron publicados en la página web del *Washington Post*, donde estuvieron disponibles gratuitamente durante los catorce días posteriores a la publicación impresa. Luego, continuó disponible online a través de un servicio pago. Solo una persona accedió a los artículos a través del servicio pago, que fue el abogado del señor Bangoura²⁹.

La Corte Superior de Ontario (*Ontario Superior Court of Justice*) determinó que era apropiado que los tribunales de Ontario asumieran jurisdicción en el caso, al considerar que el señor Bangoura era un servidor público que había hallado un hogar y un trabajo en Ontario, y que Ontario era el lugar en donde los daños a su reputación serían mayores. El *Washington Post* y los periodistas apelaron esa decisión³⁰.

27. Court of Appeal for Ontario c41379 (Unreported, Armstrong JA, Lang JA, McMurty CJO, 16, September 2005).

28. *Bangoura v. Washington Post* [2005], *supra*, párrs. 1, 5, 6, 7, 8.

29. *Bangoura v. Washington Post* [2005], *supra*, párrs. 2, 10, 11, 12.

30. *Bangoura v. Washington Post* [2005], *supra*, párrs. 3, 21.

La Corte de Apelaciones de Ontario (*Court of Appeal for Ontario*) revirtió la decisión de la Corte Superior de Ontario (*Ontario Superior Court of Justice*) al entender que la conexión entre la acción del señor Bangoura y Ontario era mínima y que no existía tal conexión hasta tres años luego de la publicación de los artículos, por lo que concluyó que no constaron daños significativos en Ontario. Rechazó el argumento de la Corte Superior de que el periódico y los periodistas debieron haber previsto que el artículo iba a «seguir» al señor Bangoura –cualquiera fuese su residencia–, y sostuvo que no era razonablemente previsible en 1997 que el señor Bangoura iba a ser un residente de Ontario. Agregó que sostener lo contrario significaría que un demandado podría ser enjuiciado en cualquier lugar del mundo donde el accionante decidiera residir mucho después de la publicación del artículo difamatorio³¹.

I.C. Inglaterra

I.C.I. Bin Mahfouz c/ Ehrenfeld (2005)

En el caso *Bin Mahfouz c/ Ehrenfeld*³², los demandantes, empresarios de Arabia Saudita, iniciaron el procedimiento sumario previsto en la ley de difamación de 1996 (*Defamation Act 1996*) por considerar que los dichos publicados en el libro de la doctora Rachel Ehrenfeld eran difamatorios. La acción judicial estuvo dirigida contra la Rachel Ehrenfeld, consultora en temas de narcoterrorismo, y la empresa estadounidense que publicó el libro, Bonus Books Incorporated³³. El libro, titulado *Funding Evil, How Terrorism is Financed-And How to Stop it*, se vendía en Inglaterra por intermedio de algunos vendedores en Internet como *Amazon.co.uk*, *Blackwells.co.uk* y *Amazon.com*. El primer capítulo del libro también estaba disponible en la página web del *ABC News*³⁴. Aparentemente, desde el 1º de julio de 2003, unas veintitrés copias físicas del libro se habían vendido en Inglaterra y en marzo de 2004, unas 211 000 personas habrían visitado la página web de *ABC News*³⁵. La acción por difamación se fundó en que el libro sostenía que la familia de Bin Mahfouz financiaba a Al Qaeda y a otras organizaciones

31. *Bangoura v. Washington Post* [2005], *supra*, párr. 25.

32. *Bin Mahfouz v. Ehrenfeld*, [2005] EWHC 1156 (QB).

33. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párrs. 1, 6, 7, 12, 13.

34. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párrs. 14, 16.

35. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párrs. 22, 23.

terroristas³⁶. Los demandados fueron notificados en los Estados Unidos sobre la acción en octubre de 2004³⁷. Luego de que estos no presentaran una defensa, se dictó una sentencia y una medida cautelar contra los demandados en diciembre de 2004³⁸.

La Corte que intervino en el caso en Inglaterra (*High Court of Justice Queen's Bench Division*) emitió la declaración de falsedad solicitada por los demandantes, confirmó la medida cautelar otorgada y ordenó el máximo nivel de daños, en favor de cada demandante, permitido por el procedimiento sumario de la ley de difamación de 1996 (*Defamation Act 1996*)³⁹.

I.C.II. *Dow Jones & Co., Inc. c/ Jameel* (2005)

Dow Jones publica el *The Wall Street Journal* y *The Wall Street Journal On-line*. Esta última es una publicación en una página web, a la que tienen acceso sus suscriptores. Yousef Abdul Latif Jameel, un empresario de Arabia Saudita, consideró que los dichos en un artículo de la publicación online que insinuaba que los demandantes eran sospechosos de financiar a Al Qaeda eran difamatorios. El artículo no hacía referencia al señor Jameel directamente, sino que contenía un enlace a otro documento que identificaba a Jameel como uno de los donantes que había financiado a Osama Bin Laden⁴⁰.

Al resolver en las apelaciones iniciadas contra cuatro decisiones recaídas en contra de Dow Jones, la Corte (*Supreme Court of Judicature Court of Appeal, Civil Appeals Division*) decidió no ejercer jurisdicción sobre el caso con fundamento en que solo cinco individuos dentro de la jurisdicción habían accedido al link, y que tres de ellos eran miembros del equipo legal del señor Jameel. La Corte consideró que sería un abuso del proceso utilizar los recursos económicos de la corte en ese litigio⁴¹.

I.C.III. *Don King c/ Lennox Lewis* (2004)

Don King, un famoso promotor de boxeo, inició un juicio en Inglaterra contra Lennox Lewis, ciudadano británico⁴². Este último solicitó a la Corte que deje sin efecto el permiso que había otorgado para notificar a las partes

36. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párr. 18.

37. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párr. 19.

38. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párr. 21.

39. *Bin Mahfouz v. Ehrenfeld*, [2005], *supra*, párrs. 74, 75.

40. *Dow Jones & Co., Inc. v. Jameel* [2005] EWCA Civ 75.

41. *Dow Jones & Co., Inc. v. Jameel* [2005] EWCA Civ 75, para 70, 71.

42. *Don King v. Lennox Lewis* [2004] EWHC 168 (QB)

en los Estados Unidos, donde ambos residían. El señor Lewis tenía un litigio pendiente en Nueva York, en los Estados Unidos, contra Don King y Mike Tyson por interferencia con un acuerdo comercial entre el señor Lewis y Mike Tyson. Don King –en dos artículos publicados en páginas web– sostuvo que el abogado del señor Lewis había insinuado que Don King era antisemita.

Al evaluar si las cortes inglesas eran el foro apropiado para resolver la cuestión, la Corte (*High Court of Justice Queen's Bench Division*) sostuvo que la evidencia revelaba que el señor King gozaba de una reputación sustancial en Inglaterra, donde había realizado apariciones en televisión, radio y otros medios. También consideró que el señor King tenía una conexión financiera y de negocios sustancial en Inglaterra, como resultado de haber promovido algunos concursos en Inglaterra que involucraron a boxeadores británicos. También consideró que el señor King tenía amigos y conocidos dentro de la comunidad judía en Inglaterra. Además tuvo en cuenta que varios testigos dieron evidencia de que las páginas web eran populares y visitadas frecuentemente por fanáticos del boxeo en Inglaterra. La Corte destacó que la ley británica considera que las publicaciones se llevaron a cabo en Inglaterra, ya que las palabras fueron descargadas en computadoras de ese país. Por estos motivos, la Corte confirmó la decisión que permitió notificar en los Estados Unidos a las partes del juicio.

I.C.IV. *Berezovsky c/ Michaels* (2000)

Dos empresarios rusos demandaron por difamación a la revista *Forbes*. Esta investigaba la situación en la Rusia postsoviética y su trabajo de investigación se enfocaba, en 1996, en el rol de dos figuras importantes en la nueva Rusia. Uno de ellos era el empresario y político Boris Berezovsky. La edición del 30 de diciembre de 1996 de *Forbes* describió a Boris Berezovsky y al señor Nicolai Glouchkov, otro empresario, como «criminales a gran escala». Mientras que en los Estados Unidos, la edición del 30 de diciembre de 1996 de esa revista contaba con 748 123 suscripciones, en Inglaterra contaba con 566 suscripciones.

Los empresarios iniciaron juicios separadamente por difamación en Inglaterra. El señor Berezovsky alegó que tenía fuertes lazos de negocios con ese país. Solicitaron compensación por daños como consecuencia de la publicación de *Forbes* dentro de la jurisdicción a través de la distribución de copias de la revista y a través de la publicación en Internet. Solicitaron autorización al tribunal para notificar a las partes fuera de la jurisdicción. *Forbes* solicitó una suspensión del caso alegando que Inglaterra no era una jurisdicción apropiada para el caso y que tanto los Estados Unidos como Rusia serían jurisdicciones más apropiadas.

En primera instancia y en la Corte de Apelaciones (*Court of Appeal*), se discutió el grado de conexión de los empresarios con Inglaterra y su reputación dentro de ese país. El 22 de octubre de 1997, la primera decisión consideró las peticiones de *Forbes* y dictó dos decisiones, y concluyó que la conexión de los empresarios con Inglaterra eran débiles. El juez consideró que Rusia era la jurisdicción más apropiada.

Los empresarios apelaron la decisión. Esta concluyó que había una causa de acción civil válida en Inglaterra en el caso de ambos demandantes, y que, en consecuencia, había jurisdicción para llevar el juicio a ese país, y que teniendo en cuenta todas las circunstancias, Inglaterra era la jurisdicción apropiada para llevar el juicio.

Forbes apeló ante la Cámara de los Lores (*House of Lords*), la que entendió que la decisión apelada tuvo razón en concluir que los empresarios tenían una conexión sustancial con Inglaterra y una reputación que proteger en Inglaterra. Consideró que los lazos del señor Nicolai Glouchkov con Inglaterra eran más débiles. La Cámara de los Lores consideró que la distribución en Inglaterra del material difamatorio fue significativa y que los empresarios tenían una reputación que proteger en Inglaterra. Entendió que, en casos como este, no es injusto que la empresa extranjera a cargo de la publicación del material sea llevada a juicio en Inglaterra. Consideró, también, que lo sustancial del daño ocurrió dentro de la jurisdicción. Creyó que Rusia no era la jurisdicción apropiada porque solo diecinueve copias de la revista habían sido distribuidas allí y que una decisión en Rusia no remediaría el daño causado en Inglaterra y que los Estados Unidos tampoco eran una jurisdicción apropiada, porque los empresarios no tenían conexión sustancial con ese país.

I.D. Los Estados Unidos

I.D.I. *Calder c/ Jones* (1984)

Aunque este caso no trate el tema de difamación en Internet, igual ha sido el caso más citado en la jurisprudencia estadounidense sobre quién debe de ejercer jurisdicción en estos casos.

En *Calder c/ Jones*⁴³, Jones había iniciado un juicio en la Corte Superior de California (*California Superior Court*), alegando que había sido difamada (*libeled*) en un artículo que había sido escrito y editado en Florida

43. *Calder v. Jones*, 465 u.s. 783 (1984)

y publicado en el *National Enquirer*, una revista que tenía su circulación principalmente en California. Jones vivía allí y su carrera televisiva estaba basada en California. Los demandados incluían al presidente y editor del *Enquirer*, al *Enquirer* y al periodista que escribió el artículo.

Calder era el presidente y editor del *Enquirer* y residía en Florida. Solo había viajado a California en dos oportunidades, con anterioridad a la publicación del artículo y por motivos no vinculados al artículo. El *Enquirer* es una compañía con base en Florida. El periodista que escribió el artículo estaba empleado por el *Enquirer*, tenía residencia en Florida y viajaba frecuentemente a California por motivos de trabajo. El periodista había realizado la mayor parte de su investigación en Florida.

Los demandados alegaron que la notificación de la demanda había sido inválida por ausencia de jurisdicción sobre los demandados en el caso. La Corte Superior de California (*California Superior Court*) admitió el planteo. La Corte de Apelaciones de California (*California Court of Appeal*) revirtió esa decisión, rechazando la sugerencia de la Corte Superior de que consideraciones de la primera enmienda (*First Amendment considerations*) deben entrar en el análisis de la jurisdicción.

La Corte Suprema de los Estados Unidos confirmó la decisión de la Corte de Apelaciones de California (*California Court of Appeal*) y sostuvo que correspondía ejercer jurisdicción sobre los peticionantes en California. La Corte consideró que el artículo periodístico presuntamente difamatorio se refería a las actividades de un residente de California, que la carrera de Jones estaba centrada en California, que las fuentes del artículo surgieron de California y que el daño, en términos del sufrimiento emocional y su reputación profesional, fue sufrido en California. La Corte Suprema entendió que los peticionantes escribieron y editaron un artículo sabiendo que podría tener un impacto negativo en la reputación de Jones en California, por lo cual debieron razonablemente haber anticipado quedar sujetos a la jurisdicción de California.

I.D.II. *Edias Software International, L.L.C c/ Basis International LTD (1996)*

En *Edias Software International, L.L.C c/. Basis International LTD*,⁴⁴ Basis International LTD (Basis) había contratado con Edias Software International (Edias) que esta última se encargaría de distribuir los productos de software producidos por la primera. Basis decidió terminar la relación y envió correos electrónicos a varios de sus clientes europeos y a sus empleados (que se

44. 946 F. Supp. 413 (D. Arz., Nov. 19, 1996)

encontraban en Nuevo México) y publicó información en su sitio de Internet explicando que la relación con Edias estaba terminada con motivo de que la compañía no se comprometió a vender el producto a un precio justo y a proporcionar apoyo técnico apropiado⁴⁵.

Edias inició una demanda por difamación en Arizona, donde tenía oficinas. Basis planteó que la demanda debía ser desechada por ausencia de jurisdicción sobre Edias en Arizona. El planteo se fundó en que Basis no tenía contactos suficientes en Arizona, por lo cual se les haría demasiado costoso proseguir con su defensa en ese estado. Basis era una compañía basada en Nuevo México, que no tenía oficinas, empleados, ni cuentas bancarias en Arizona. La Corte determinó que la decisión de Basis International de publicar las razones de la terminación del contrato *online*, lo cual significaba que estarían disponibles para residentes de Arizona, era suficiente razón para proceder con el caso por difamación en Arizona. El resultado de las actividades tendría consecuencias negativas para el demandante en Arizona, donde este tenía oficinas.

La Corte señaló que

...se atribuye la competencia en Arizona bajo el marco del «test de los efectos». Cuando hay acciones intencionales que están expresamente dirigidas al tribunal del estado y causan daños previsibles a la parte demandada, se puede ejercer jurisdicción en el estado. El email, pagina web y mensajes de foro utilizados por Basis International estaban dirigidos a Arizona y presuntamente causaban daños previsibles a Edias...No se debe permitir que Basis International pueda aprovecharse de la tecnología moderna a través de un sitio web y foro y, simultáneamente, escapar a nociones tradicionales de justicia⁴⁶.

45. Samson, Martin, «Edias Software International, LLC et al v. Basis International Ltd.», en *Internet Library of Law and Court Decisions*, disponible [en línea] en: <http://www.internetlibrary.com/cases/lib_case168.cfm>. [Nota del editor: consultada el 12/11/11.]
46. Fuente: «Basis»:

[...] CompuServe Web Site which reaches Arizona customers ... confers jurisdiction in Arizona under the «effects test». When intentional actions are expressly aimed at the forum state and cause foreseeable harm to the defendant, jurisdiction in the forum state exists. The e-mail, Web page and forum message were both directed at Arizona and allegedly caused foreseeable harm to *Edias*. «Unlike communication by mail or telephone, messages sent through computers are available to the recipient and anyone else who may be watching. Thus, while modern technology has made nationwide commercial transactions simpler and more feasible, even for small businesses, it must broaden correspondingly the permissible scope of jurisdiction exercisable by the courts». [...] *Basis* should not be permitted to take advantage of modern technology through an Web page and forum and simultaneously escape traditional notions of jurisdiction.

I.D.III. *Telco Communications c/ An Apple a Day* (1997)

En *Telco Communications c/ An Apple a Day*⁴⁷, Telco Communications (Telco), una compañía del estado de Virginia, con la subsidiaria Dial & Save en Missouri, demandó a An Apple a Day (Apple) por violación del derecho de marcas.

En la acción iniciada en Virginia, Telco alegó que los demandados publicaron dos comunicados de prensa que difamaron a Telco y que hicieron llamados a un analista financiero en Maryland, a raíz de lo cual habría bajado el valor de las acciones de Telco. An Apple a Day (Apple) es una compañía de *telemarketing* de Missouri que decía ser dueña de la marca Dial & Save. También fueron demandados Christina Anne Steffen, la dueña de Apple, y su esposo, Myles Lipton.

Los demandados solicitaron el rechazo de la acción, que fue denegado por una Corte de Virginia (*United States District Court for the Eastern District of Virginia*). Esta Corte evaluó si existió jurisdicción sobre los demandados en el caso, a la luz de que la conducta presuntamente indebida de estos habría ocurrido a través de Internet. La Corte estuvo de acuerdo con la interpretación en el caso *Inset Systems Inc. c/ Instruction Set*, 937 F. Supp. 161, 165 (D. Conn. 1996), a partir de lo que sostuvo que la publicación de una publicidad en Internet cumplía con el estándar para la aplicabilidad del estatuto de jurisdicción (*long-arm statute*) de Connecticut. Entendió que el apartado 8.01-328.1(A)(4) del Código de Virginia (*Virginia Code*) contenía un lenguaje similar, y que los demandados desarrollaron conductas de publicidad previstas en ese Código.

La Corte dijo que si bien los demandados sostuvieron que no desarrollaban actividad comercial en Virginia, admitieron que estaban haciendo publicidad de su compañía y que habían requerido la asistencia de analistas financieros en la publicación de los comunicados de prensa. Concluye que estaban desarrollando actividad comercial en Internet. Dado que realizaban actividades de publicidad vía Internet, que podía ser visto por un residente de Virginia las veinticuatro horas del día, desarrollaban la actividad con regularidad en los términos del estatuto de jurisdicción. En consecuencia, la Corte entendió que publicar una publicidad es una conducta persistente, y que dos o tres comunicados de prensa llegan a constituir una conducta habitual de conducción de negocios, quedando satisfechos los requisitos del apartado 8.01-328.1(A)(4) del Código de Virginia.

47. 977 F. Supp. 404 (1997).

La Corte también entendió que había jurisdicción bajo el apartado (A) (3) del estatuto de jurisdicción de Virginia. Este apartado permite el ejercicio de jurisdicción sobre una persona que causa un daño por una acción u omisión. La Corte decía que si bien generalmente para que exista jurisdicción en virtud de este apartado se requería presencia física en Virginia al momento de causar el daño, las Cortes se habían ido apartando de ese requerimiento, y cita al respecto el caso de *Krantz c/ Air Line Pilots Assoc., Int'l*, 25 Va. 202, 427 S.E.2d 326 (1993), en donde la Corte Suprema de Virginia (*Supreme Court of Virginia*) concluyó que el apartado (A) (3) quedó satisfecho por un demandado que, actuando totalmente en Nueva York, accedió a un listado electrónico en Virginia. La Corte interpretó que ese hecho significó que estaba cumplido el requerimiento de que exista una acción (*further act*) que exige el derecho de Virginia para configurarse la interferencia dañosa (*tortious interference*) con el contrato del accionante.

La Corte consideró si este caso podía asimilarse a *Krantz*, y entendió que los demandados debieron, razonablemente, haber sabido que los comunicados de prensa iban a ser recibidos en Virginia. Consideró que, de no ser por los proveedores de servicios de Internet y usuarios presentes en Virginia, el presunto daño de la difamación no habría ocurrido en Virginia. Dijo, además, que numerosos inversores e intermediarios financieros estaban basados en Virginia y que la presencia de oficinas en Virginia era necesaria para que esos individuos pudieran acceder a los comunicados de prensa. También consideró que dado que Telco estaba ubicada en Virginia, la compañía sufrió daño allí.

La Corte agregó que la previsibilidad (*foreseeability*) no era suficiente y que los contactos de los demandados con esa jurisdicción debían ser suficientemente fuertes como para que ellos razonablemente tuviesen la expectativa de ser llevados ante los tribunales en Virginia, lo que entiende que se dio en este caso. La Corte concluyó que los demandados debieron, razonablemente, saber que los comunicados de prensa iban a ser distribuidos en Virginia y que Telco estaba basado en Virginia, por lo que sus actividades eran suficientemente análogas a tener una presencia física en ese estado⁴⁸.

48. Véase *Telco Communications v. An Apple a Day* 977 F. Supp, 404, 407 (E.D. va. 1997), disponible [en línea] en: <<http://lw.bna.com/lw/19971014/97542.htm>>. [Nota del editor: consultada el 12/11/11.]

I.D.IV. *Stanley Young c/ New Haven Advocate* (2002)

En *Stanley Young c/ New Haven Advocate*⁴⁹, el director de una prisión en Virginia demandó a dos periódicos de Connecticut, el *New Haven Advocate* (*Advocate*) y el *Hartford Courant* (*Courant*), disponibles en Virginia a través de Internet, por publicar artículos que él consideraba difamatorios.

Una Corte de Apelaciones de Virginia decidió sobre la cuestión de si los demandados, los periódicos de Connecticut y algunos de sus empleados, estaban sujetos a la jurisdicción del estado de Virginia.

Los periódicos habían publicado artículos que hacían referencia a que Connecticut había trasladado parte de su población carcelaria a una prisión estatal en Virginia. En estos artículos, se habría difamado a Young, el director de este establecimiento en Virginia, alegando que Young era racista y que promovía el abuso por parte de los guardias hacia los prisioneros en la prisión estatal de Virginia.

Siguiendo el criterio en *ALS Scan, Inc. c/ Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Cir. 2002), la Corte de Apelaciones decidió que un tribunal de Virginia no puede, constitucionalmente, ejercer jurisdicción sobre una persona de fuera del estado que coloca información en Internet. Resolvió que un tribunal en Virginia no podía ejercer jurisdicción sobre los periódicos demandados, que estaban basados en Connecticut, porque ellos no manifestaron una intención de dirigir sus páginas de Internet ni los artículos que publicaron a una audiencia en Virginia. Así, la Corte revirtió la decisión que había denegado el pedido de los demandados de rechazar la acción por falta de jurisdicción.

I.D.V. *Northwest Healthcare Alliance, Inc. c/ Healthgrades.com, Inc* (2002)

En este caso⁵⁰, Northwest Healthcare Alliance (Northwest), una empresa que proporciona servicios médicos en el estado de Washington, inició un juicio ante un tribunal de Washington contra Healthgrades.com Inc. (Healthgrades). Healthgrades es una empresa de Delaware que tiene su principal sede de negocios en Colorado. Healthgrades opera una página web que publicaba calificaciones sobre empresas de salud. Northwest inició esta

49. Véase No. 01-2340 (4th Cir., December 13, 2002).

50. Véase No. 01-35648, D.C. No. cv-01-00488-BJR, Memorandum (9th Circuit, October 7, 2002), disponible [en línea] en: <<http://www.techlawjournal.com/courts2001/healthgrades/20021007.asp>>. [Nota del editor: consultada el 12/11/11.]

acción alegando difamación y violación de la ley de defensa del consumidor de Washington, luego de haber recibido una puntuación que consideró desfavorable en la página web de Healthgrades.

La Corte de Apelaciones discutió si podía ejercer jurisdicción sobre Healthgrades. Aplicando el «test de los efectos» (*effects test*), el tribunal encontró que Healthgrades se había involucrado adrede en el mercado de servicios médicos de Washington al proporcionar calificaciones sobre proveedores en Washington. Entendió que este accionar estaba expresamente dirigido a Washington, dado que Healthgrades tenía conocimiento de que sus calificaciones de proveedores de Washington tendrían valor principalmente para los consumidores de Washington. Asimismo, consideró que, si bien Healthgrades obtenía información de varias fuentes públicas, incluyendo el Gobierno Federal, la información había sido obtenida originalmente de fuentes de Washington y que la calificación presuntamente difamatoria que recibió Northwest se refería a las actividades en Washington de un residente de Washington. Además, consideró que el daño presuntamente sufrido por Northwest ocurrió en Washington, donde la compañía está registrada, donde tiene su principal lugar de negocios y donde su reputación podría sufrir un daño. Los efectos de la conducta de Healthgrades ocurrieron en Washington, y Healthgrades podía razonablemente esperar tener que responder por su conducta en la jurisdicción donde entendía que sus acciones tendrían efectos.

Por estos motivos, la Corte concluyó que era constitucionalmente permisible ejercer jurisdicción sobre el demandado en el estado de Washington.

I.D.VI. *Clemens c/ McNamee* (2010)

En *Clemens c/ McNamee*⁵¹, una Corte de Apelaciones evaluó si podía ejercer jurisdicción sobre el demandado.

Clemens es un jugador de *baseball* profesional. A pesar de que residió temporalmente en otras ciudades durante su carrera, tenía su residencia permanente en Houston, Texas. *McNamee* estaba siendo investigado en Nueva York por el presunto desarrollo y venta de drogas a atletas para mejorar la actuación deportiva. Durante los interrogatorios policiales, *McNamee* le dijo a los investigadores que había inyectado a *Clemens* drogas

51. Véase No. 09-20525 (5th Circuit, August 12, 2010).

para mejorar la actuación deportiva en 1998, 2000 y 2001 en Nueva York y Toronto. Estas declaraciones fueron luego incorporadas a un informe que las autoridades federales realizaron en otra investigación conducida por el ex senador estadounidense George Mitchell sobre el uso de drogas para mejorar la actuación deportiva, que derivó en un informe conocido como el *Informe Mitchell (Mitchell Report)*.

Las cadenas de noticias nacionales, así como los periódicos más importantes de Texas, volvieron a publicar los dichos de McNamee. Luego de la publicación del *Informe Mitchell*, McNamee habló con John Hayman, un escritor de la página web *SI.com*. Durante esta entrevista en la residencia de McNamee en Queens, Nueva York, este repitió los dichos que habían sido publicados en el mencionado informe. Heyman publicó un artículo conteniendo estos dichos en la página *SI.com* el 7 de enero de 2008.

Clemens inició el juicio por difamación contra McNamee en un tribunal de Texas, en enero de 2008. McNamee cuestionó la jurisdicción del tribunal. La corte de distrito rechazó la acción de difamación por falta de jurisdicción porque los dichos de McNamee sobre Clemens no estaban enfocados en Texas. Esa decisión fue apelada.

Al resolver sobre la cuestión de jurisdicción, la Corte de Apelaciones preguntó si los dichos presuntamente difamatorios de McNamee estaban dirigidos hacia Texas. La Corte de Apelaciones entendió que los dichos en cuestión se referían a actividades que se habían desarrollado fuera de Texas: la entrega de drogas a Clemens en Nueva York y Canadá. La Corte consideró que los dichos no fueron pronunciados en Texas ni estaban dirigidos a residentes de Texas. Con base en estos factores, la Corte concluyó que Clemens no logró establecer jurisdicción sobre McNamee.

I.D.VI. *Silver c/ Brown* (2010)

En *Silver c/ Brown*⁵², David Silver apeló la decisión de la corte de distrito de rechazar su acción por difamación contra Mathew Brown y Jack McMullen.

El señor Silver, quien es residente de Nuevo México, presentó una acción por difamación el 26 de mayo de 2009. Alegó que los señores Brown y McMullen, ciudadanos de Florida, lo habían difamado al publicar un comentario en Internet que lo desfavorecía. El comentario habría

52. Véase No. 10-2005 (10th Circuit, June 14, 2010).

tenido la intención de afectar negativamente la reputación del señor Silver y de la compañía Santa Fe Capital Group (Santa Fe), de quien este era presidente. Santa Fe había suscripto un acuerdo con Growth Technologies International, Inc (GTI). Mathew Brown era el presidente de GTI, y el señor McMullen era miembro del directorio de GTI. En ese acuerdo, Santa Fe se comprometió a asistir a GTI en recaudar fondos de inversores privados a cambio de una compensación económica. El señor Silver reclamó parte de esta compensación que estaba pendiente de pago a Santa Fe, y el señor Brown reclamó el reembolso de la porción de la compensación que había sido pagada por GTI. El comentario, publicado por el señor Brown alrededor del 5 de mayo de 2009 en el blog *DavidSilverSantaFe.com*, tenía como fin desacreditar la reputación de Silver en relación con su actuación durante la relación contractual de Santa Fe con GTI.

La Corte de distrito rechazó los reclamos de Silver por falta de jurisdicción y decidió que bajo la ley de jurisdicción de Nuevo México ni el señor Brown ni el señor McMullen tenían suficientes contactos con Nuevo México para posibilitar que el tribunal ejerciera jurisdicción sobre ellos.

La Corte de Apelaciones afirmó el rechazo de la acción respecto del señor McMullen al considerar que sabía, o debía saber, que debía defenderse de un juicio en Nuevo México al subir el blog.

La Corte de apelaciones revirtió, sin embargo, el rechazo de la acción respecto del señor Brown.

Respecto del señor Brown, la Corte de Apelaciones examinó si había jurisdicción específica sobre el señor Brown según el test de «contactos mínimos», para lo cual se preguntaba si el demandado no residente dirigió intencionalmente sus actividades al estado del tribunal actuante. La Corte consideró que era claro, a partir de *Calder c/ Jones*, que el señor Brown dirigió intencionalmente su blog a Nuevo México y que los daños presuntamente sufridos por el señor Silver derivan de las actividades del señor Brown relacionadas con Nuevo México.

La Corte de Apelaciones consideró que la publicación del blog era claramente un acto intencional. Consideró que el señor Brown creó el blog en cuestión en respuesta directa al negocio fallido y que había amenazado con publicar el blog como un intento de recuperar dinero que consideraba que se le debía a GTI. La Corte evaluó también que el señor Brown era el moderador del blog y que él había escrito al menos la página introductoria que alegaba que su compañía había sido estafada por el señor Silver y Santa Fe. Esto demostró, según la Corte de Apelaciones, que la intención del blog era dañar la reputación del señor Silver y Santa Fe.

La Corte de Apelaciones también consideró que el señor Brown expresamente dirigió su blog a Nuevo México y que el blog era sobre un residente de Nuevo México y sobre una compañía de Nuevo México, y se refería a una relación empresarial que se dio, mayormente, en Nuevo México. Además, el blog estaba ampliamente disponible en Nuevo México por medio de Internet.

Finalmente, la Corte de Apelaciones consideró que el señor Brown tenía conocimiento de que el daño al señor Silver se produciría en Nuevo México. El señor Brown sabía que Santa Fe estaba ubicada en Nuevo México y que el señor Silver vivía en Nuevo México y conducía sus negocios desde allí.

La Corte de Apelaciones rechazó la argumentación de la Corte de distrito de que el blog no estaba dirigido solamente a los residentes en Nuevo México y de que el blog era accesible a cualquiera en cualquier parte del mundo. La Corte dijo que Internet y el uso de los buscadores permite identificar a la persona a quien va dirigida el blog, e interpretó *Calder* en el sentido de que las acciones llevadas a cabo con el fin de que sus consecuencias se sientan en el estado donde se asienta el tribunal son suficientes para concluir que existe un «direccionamiento intencional».

II. Criterios adoptados en América Latina

La búsqueda de jurisprudencia en América Latina es, con algunas excepciones, complicada para cualquier investigador. Los casos citados seguidamente reflejan solamente algunos que o bien tienen directa relación con situaciones donde el contenido difamatorio de una expresión fluye en Internet o bien, sin una directa relación con Internet, son casos que exponen el razonamiento que los jueces y otros operadores aplican y que luego pretenden ser transportados a los casos de Internet.

II.A. Brasil

En el 2006 ocurrió un accidente aéreo cerca de Brasilia entre un avión de pasajeros de GOL Líneas Aéreas y un jet Embraer Legacy perteneciente a la compañía Excel Air. El accidente tuvo como resultado 154 personas muertas en el avión de GOL.

El periodista estadounidense Joseph Sharkey, que viajaba en el jet Legacy y sobrevivió al accidente, escribió un artículo sobre su experiencia,

que fue publicado en la primera página del *New York Times*⁵³. Luego de la publicación de este artículo, el periodista fue entrevistado por periódicos estadounidenses e internacionales, incluyendo el *NBC Today Show* y *NPR*. Además, a raíz de un comentario que hizo durante entrevistas según el cual pilotos internacionales le habían dicho que había fallas en el sistema de control aéreo brasileño, el entonces ministro de Defensa brasileño Walter Pires criticó al periodista ante los medios. El cronista luego comenzó un blog en el que comentó aspectos del accidente⁵⁴. El último artículo de su blog fue publicado el 6 de enero de 2008, y el blog aún está disponible online⁵⁵. Otro blog del periodista también relata su experiencia y sus visiones sobre lo ocurrido⁵⁶.

A raíz de estos acontecimientos, Joseph Sharkey enfrentó dos procesos judiciales en Brasil, uno civil y uno penal, que fueron iniciados por Rosane Gutjhar, una ciudadana brasileña viuda de una de las víctimas del accidente aéreo. Rosane Gutjhar consideró que los dichos de Sharkey eran ofensivos hacia Brasil.

La demanda civil por indemnización fue iniciada en 2008 y tramitada en un Juzgado Civil de Primera Instancia de Curitiba (Juzgado 18° v Cível)⁵⁷. En la demanda civil, la demandante, Rosane Gutjhar, reclamó una indemnización a Joseph Sharkey por expresiones que el periodista habría utilizado para referirse a los brasileños. Alega que el periodista se refirió a ellos o los comparó con «los tres chiflados», «los más idiotas de los idiotas», «un país arcaico», «Tierra de los Tupiniquins y bananas», entre otros calificativos⁵⁸. Según un análisis de estas acusaciones realizada por un

53. Véase «Colliding With Death at 37,000 Feet, and Living», en *The New York Times*, el 3 de octubre de 2006, disponible [en línea] en: <<http://www.nytimes.com/2006/10/03/business/03road.html?pagewanted=1>>. [Nota del editor: consultada el 12/11/11.]

54. Información que proporcionó el periodista al consultarlo para la elaboración de este trabajo.

55. Véase «Colliding With Death at 37,000 Feet, and Living», en *The New York Times*, el 3 de octubre de 2006, disponible [en línea] en: <<http://sharkeyonbrazil.blogspot.com>>. [Nota del editor: consultada el 12/11/11.]

56. Véase «Aviation Know-It-All Crashes Plane Into a Pole», en *Joe Sharkey: Brazil*, el 6 de enero de 2008, disponible [en línea] en: <<http://www.joesharkey.com>>. [Nota del editor: consultada el 12/11/11.]

57. Véase Expediente N° 13998/2008.

58. Página 3 de la versión en inglés de la demanda civil, disponible en: <<http://www.calunia.com.br/p/blog-page.html>>. [Nota del editor: consultada el 12/11/11.]

allegado al periodista, algunas de las frases no provienen del texto escrito por el periodista en sus artículos del blog, sino de comentarios de usuarios a un artículo en otra revista electrónica, *Brazzil.com*, que había sido reproducido por el periodista en su blog⁵⁹.

En cuanto a la competencia para entender en el caso, la demanda sostuvo que era competente el tribunal del domicilio de la demandante, al considerar que son aplicables al caso los Artículos 93, Sección 3, y el Parágrafo Único del Artículo 100 del Código de Processo Civil brasileño (CPC).

Según el artículo 94 del CPC, las acciones de derechos personales serán iniciadas, como regla general, en el lugar del domicilio del demandado. Una de las excepciones a esta regla estaría dada por la Sección 3 de este artículo, según el cual sería competente el tribunal del lugar de residencia del accionante en los casos en que el demandado no tiene domicilio ni residencia en Brasil. Por otro lado, según el parágrafo único del artículo 100 del mismo Código, sería competente el juez del lugar del domicilio del accionante en los casos de reparación de daños derivados de un delito.

En la demanda se argumentó que Joseph Sharkey no residía en Brasil ni estaba domiciliado en ese país, y que el pedido de reparación fue formulado en razón de la comisión de un delito, por lo cual era competente el tribunal del domicilio de la accionante⁶⁰.

El periodista fue notificado de la acción en su domicilio de entonces, en Nueva Jersey, y decidió no presentarse ni defenderse. El juez declaró

59. Véase «Unsafe Skies? Why, I Oughta.... How DARE They Say These Skies Are Unsafe!», en *Joe Sharkey: Brazil*, el 7 de octubre de 2007, disponible [en línea] en: <http://sharkeyonbrazil.blogspot.com/2007/10/how-dare-they-say-these-skies-are_07.html>. [Nota del editor: consultada el 12/11/11.]. Información proporcionada por Joseph Sharkey.

60. Página 6 de la versión en portugués de la demanda civil, disponible en: <<http://www.calunia.com.br/p/blog-page.html>>. [Nota del editor: consultada el 12/11/11.]. A continuación se transcriben las partes referidas en la demanda de los artículos del Código de Processo Civil.

Art. 94 - A ação fundada em direito pessoal e a ação fundada em direito real sobre bens móveis serão propostas, em regra, no foro do domicílio do réu. (...) § 3º - Quando o réu não tiver domicílio nem residência no Brasil, a ação será proposta no foro do domicílio do autor. Se este também residir fora do Brasil, a ação será proposta em qualquer foro.

Art. 100 - (...) Parágrafo único - Nas ações de reparação do dano sofrido em razão de delito ou acidente de veículos, será competente o foro do domicílio do autor ou do local do fato.

Fuente: <<http://www.iberred.org/sites/default/files/cdigo-procesal-civil-brasil.pdf>>. [Nota del editor: consultada el 12/11/11.]

extinta la acción por entender que la querellante no tenía legitimación activa para demandar por no existir una conexión entre los comentarios de Joseph Sharkey y Rosane Gutjhar. El juez consideró que dicha conexión no existía porque las expresiones del periodista no se referían directamente a la querellante, sino genéricamente a todos los brasileños⁶¹. Por otro lado, consideró que los abusos de los medios de prensa solo pueden comprobarse cuando existe una ofensa realmente intencional, directa y con agresividad incuestionable. Consideró que debía imperar el criterio de razonabilidad en evaluar los dichos del periodista y concluyó que estos dichos debían ser tolerados⁶². Rosane Gutjhar presentó un recurso de apelación contra la decisión, que fue admitido.

El expediente fue enviado al Tribunal de Justicia del Estado de Paraná el 14 de febrero de 2011, y la resolución de este recurso en el caso civil está pendiente⁶³.

Rosane Gutjhar también inició un juicio penal contra el periodista en 2009. El periodista recibió una copia de la intimación de un tribunal con sede en Curitiba, estado de Paraná, en su domicilio en Arizona, en 2010, con la intervención de un estudio de abogados de Nueva York. Esta intimación fue cursada a raíz de la solicitud de Rosane Gutjhar de que el periodista proporcionara explicaciones, en los términos del Artículo 144 del Código Penal⁶⁴, sobre los comentarios en sus blogs en relación con el accidente⁶⁵.

El juez decidió extinguir la acción sin la presencia de Joseph Sharkey, porque entendió que Rosane Gutjhar no estaba legitimada para defender los intereses del Gobierno y sus dirigentes, y que no había una ofensa directa contra ella. Contra esa resolución, Rosane Gutjhar interpuso un Recurso en Sentido Estricto (RESE). En junio de 2010, el Tribunal de Justicia de Paraná resolvió confirmar la sentencia que extinguió la acción y oficiar al

61. Véase p. 191 de la decisión judicial.

62. Véanse pp. 192 y 193 de la decisión judicial.

63. Véase [en línea]: <http://www.assejepar.com.br/cgi-bin/det_processo_direto.asp?processo=70967&cbo_comarca=001&cbo_cartorio=18&txt_pesquisa=1398/2008&cbo_pesquisa=1&rdo_tipo_pesquisa=1&direto=S>. [Nota del editor: consultada el 12/11/11.]

64. El Artículo 144 del Código Penal establece (en idioma original) que: «Se, de referências, alusões ou frases, se infere calúnia, difamação ou injúria, quem se julga ofendido pode pedir explicações em juízo. Aquele que se recusa a dá-las ou, a critério do juiz, não as dá satisfatórias, responde pela ofensa».

65. Información proporcionada por Joseph Sharkey.

ministerio de la Justicia para que, si tuviese interés en procesar a Joseph Sharkey, tomara las medidas adecuadas para ello. No se conocen acciones a la fecha por parte de dicho ministerio⁶⁶.

A pesar de que los jueces no trataron el tema de la jurisdicción, resolvieron en los casos civil y penal. El motivo para rechazar las acciones estuvo relacionado con la falta de legitimación para accionar y no con la incompetencia territorial.

II.B. Argentina

II.B.I. Casos resueltos por tribunales locales

Exponemos algunas decisiones de tribunales locales de distintas instancias. Alguno de ellos, como se verá, fueron resueltos por tribunales de apelaciones.

II.B.I.a. *J., G. R. c/ GOOGLE INC*, CÁMARA FEDERAL DE APELACIONES DE SALTA, 4 DE JULIO DE 2011, LA LEY 19/07/2011. En esta causa, el accionante, Guillermo Jenefes, legislador por la provincia de Jujuy, alegó que Google Inc. alojó en sus sistemas de *Blogger* un espacio injurioso y difundió su existencia, aun cuando existía una orden judicial para eliminarlo.

El Juzgado Federal N°2 de Jujuy desestimó, mediante una resolución del 9 de diciembre de 2010, la excepción de incompetencia planteada por Google Inc. La resolución del 9 de diciembre se fundó en la opinión del fiscal federal, quien entendió que

la competencia no se determina en función del inc. 3° del art. 5 CPCCN, sino del inc. 4°, que dispone que será competente «En las acciones personales derivadas de delitos o cuasidelitos, el del lugar del hecho o el del domicilio del demandado, a elección del actor»; puntualizando que «la información que se transmite por Internet tiene la particularidad de llegar a todas partes del mundo, siendo uno de ellos la provincia de Jujuy, que es el lugar donde el actor tiene su domicilio y, por tanto, donde el hecho dañoso produjo sus efectos»⁶⁷.

66. Información proporcionada por la organización Artículo 19, Brasil.

Google Inc. interpuso un recurso de apelación contra esa decisión. Negó que el lugar del hecho fuera la provincia de Jujuy, argumentando que ninguna de las acciones que se le imputan ocurrieron allí, sino que ocurrieron en el lugar de asiento de los sistemas de Google, esto es en California, en los Estados Unidos⁶⁸. Google Inc. argumentó que el dictamen del fiscal confunde el lugar del hecho con el lugar donde el acto produce sus efectos y sostiene que este último no es determinante de la competencia según el derecho aplicable. Google Inc. agregó que

aun así si se atendiera al lugar donde supuestamente el hecho produjo sus efectos, el dictamen también incurre en un error y se contradice, pues del propio «carácter universal» de Internet, que es de público y notorio, y esta parte no discute, se desprende que los supuestos efectos dañosos – entiéndase «mala imagen» que del actor obtendrían los terceros al leer el blog cuestionado– se leen en todo el mundo⁶⁹.

El demandante, por otro lado, argumentó que el lugar del hecho es la provincia de Jujuy dado que «allí es donde él vive y donde la existencia del blog ha afectado a su familia y llegó a conocimiento de sus colegas, amigos, clientes y potenciales votantes»⁷⁰.

La Cámara Federal de Apelaciones de Salta, que entendió en la apelación, rechazó el recurso interpuesto por Google Inc. Concluyó que se debía tener por juez competente al juez del lugar «donde se verifica el daño, es decir, donde el mismo afecta al sujeto dañado»⁷¹. Para llegar a esta conclusión, la Cámara considera que

El art. 5, inc. 4º del Código Procesal Civil y Comercial de la Nación establece la posibilidad, a ejercer por el actor, de promover su acción en la jurisdicción del lugar donde el hecho ocurriera o en la correspondiente al domicilio del demandado, lo que se traduce como la posibilidad de elegir entre jueces de distinta competencia territorial[...] Al respecto, se ha dicho que una recta interpretación

67. Punto IV del dictamen obrante a fs. 207/208, citado en J., G. R. c/ *Google Inc*, Cámara Federal de Apelaciones de Salta, 4 de julio de 2011, LA LEY 19/07/201, Considerando 1.

68. J., G. R. c/ *Google Inc*, *supra* nota 66.

69. J., G. R. c/ *Google Inc*, *supra* nota 66.

70. J., G. R. c/ *Google Inc*, *supra* nota 66.

71. J., G. R. c/ *Google Inc*, *supra* nota 66, considerando 2.

del precepto en cuestión, donde se tenga en cuenta el ámbito espacial de validez de la ley procesal y se apuntale la congruencia interna de la totalidad del ordenamiento, indica que esta elección habrá de hacerse entre magistrados de distinta competencia dentro del territorio de la provincia, sin que pueda concluirse que también otorga derecho para optar entre las diversas jurisdicciones de la totalidad del país, debiendo regirse estas cuestiones por aplicación de la regla *locus regis actus* (cfr. Corte de Justicia de Buenos Aires, Ac. 80285, 01/09/04, R., D. O. c/ Flores, Gabriel y otro s/daños y perjuicios, del voto del doctor de Lázari). Y este aforismo latino («el lugar rige al acto») remite a un principio de derecho (principio de territorialidad) no romano, expresivo de que rigen las normas del derecho territorial, es decir, las del lugar donde el acto se realiza, en contra del principio de la personalidad de las leyes (cfr. Ossorio, Manuel, *Diccionario de Ciencias Jurídicas, Políticas y Sociales*, Buenos Aires, Argentina, Heliasta, 24^a, página 587/ Cabanellas, Guillermo, *Diccionario Poder Judicial de la Nación Enciclopédico de Derecho Usual*, 24^a, Buenos Aires, Argentina, Heliasta, 1996, tomo v, página 228) [...] Así las cosas, sea por conducto de la libre elección del actor o por aplicación de la doctrina más restrictiva cuando se trata de jueces de distintas jurisdicciones, lo cierto es que en materia de actos ilícitos (esto es, en términos civilísticos, de actos que causan un daño injustificado) ha de estarse al lugar del acto [...] Ahora bien, es claro que esta premisa tiende a desdibujarse cuando se pretende aplicarla al ámbito de los actos y negocios jurídicos celebrados por medio de un elemento relativamente novedoso, como es Internet, pues en estos casos el lugar es, estrictamente, el ciberespacio (ámbito artificial creado por medios informáticos, cfr. *Diccionario de la Real Academia Española* - vigésima segunda edición; www.rae.es) que no coincide con ningún territorio en particular, pero coincide con todos los territorios a la vez [...] De ahí que, interpretando de manera armónica los principios bajo examen a la luz de las nuevas circunstancias existentes, la lógica indica que en el caso de daños generados en este contexto, se tenga por juez competente el del lugar donde se verifica el daño, es decir, donde el mismo afecta al sujeto dañado⁷².

72. *Ídem*.

La Cámara continuó expresando que:

el acto mediante el cual se materializa el daño al actor (que consistiría en la alegada difamación, desprestigio de su imagen pública y daño moral) tiene lugar indudablemente en la provincia de Jujuy, pues es allí donde el mismo tiene fijada su residencia, donde vive su familia y plantea su carrera profesional y política; y no en el resto del planeta ni mucho menos en el domicilio de Google (California, Estados Unidos de Norteamérica) donde difícilmente se conozca al presentante y, por ende, exista *prima facie* interés por acceder al blogspot creado a su respecto. Además, de admitir la postura de la demandada, se llegaría a la situación de que todos los potenciales perjudicados por un acto u omisión a ella imputable deberían trasladarse hasta el citado país del Norte para litigar y hacerlo de acuerdo a las normas procesales allí vigentes, lo cual resulta a todas luces disvalioso atento a la desigualdad que siempre existirá entre un simple particular y esta empresa internacional.

II.B.I.b. *NUÑEZ, SILVIA ADRIANA C/ COMUNICACIONES Y MEDIOS S.A. Y OTRO S/ D. Y P.X RESP. EXTRACONT. DE PART.*, CÁMARA DE APELACIONES EN LO CIVIL, COMERCIAL, LABORAL Y DE MINERÍA DE LA CIRCUNSCRIPCIÓN JUDICIAL DE NEUQUÉN, SALA I, EXPEDIENTE N° 367756/8, 5 DE MARZO DE 2009⁷³. La señora Silvia Adriana Núñez inició una demanda civil en la provincia de Neuquén, en la Argentina, contra la Cámara de Agricultura, Industria y Comercio de General Roca y contra la empresa Comunicaciones y Medios S.A., a raíz de que la Cámara de Agricultura, Industria y Comercio de General Roca había redactado un email en el que se la trataba de «estafadora», y la empresa Comunicaciones y Medios SA publicó el contenido de esos dichos en la sección Policiales del diario *La Mañana de Neuquén*.

Intervino en primera instancia el Juzgado en lo Civil N° 5 de Neuquén. En primera instancia, la Cámara de Agricultura, Industria y Comercio de General Roca planteó que el tribunal interviniente de Neuquén era incompetente para entender en el caso, con el argumento de que la Cámara de Agricultura tenía su domicilio en la Ciudad de General Roca, provincia de Río Negro.

73. Fuente: *elDial.com* - AA55F1, publicado el 09/09/2009.

El juez de primera instancia resolvió que era válida la opción de la actora de iniciar la causa en Neuquén, dado que la codemandada, la empresa Comunicaciones y Medios S.A., tenía su domicilio en la Ciudad de Neuquén. Fundamentó esta decisión en el artículo 5°, inciso 4° del Código Procesal Civil y Comercial de Neuquén, según el cual,

con excepción de los casos de prórroga expresa o tácita, cuando procediere, y sin perjuicio de las reglas contenidas en este Código o en otras leyes, será juez competente: [...] 4° En las acciones personales derivadas de delitos o cuasidelitos, el del lugar del hecho o el del domicilio del demandado, a elección del actor.

La Cámara de Agricultura, Industria y Comercio de General Roca apeló la decisión del juzgado de primera instancia que rechazó el planteo de incompetencia. Solicitó que se revoque lo resuelto por aplicación de lo dispuesto por el artículo 5, inciso 5 del Código Procesal Civil y Comercial de Neuquén, que establece que

con excepción de los casos de prórroga expresa o tácita, cuando procediere, y sin perjuicio de las reglas contenidas en este Código o en otras leyes, será juez competente: (...) 5°. En las acciones personales, cuando sean varios los demandados y se trate de obligaciones indivisibles o solidarias, el del domicilio de cualquiera de ellos, a elección del actor.

La Cámara de Agricultura argumenta que, a su criterio, no se dan los supuestos del inciso 5° del artículo 5° que le permitirían a la señora Núñez la elección del lugar donde iniciar el juicio. Consideró que la obligación que se reclama no es «indivisible» y que no existe, además, «litisconsorcio necesario»⁷⁴.

La Cámara de Apelaciones en lo Civil, Comercial, Laboral y de Minería de la Circunscripción Judicial de Neuquén confirmó el rechazo del planteo de incompetencia.

La Cámara de Apelaciones consideró que era competente en el caso el juez del lugar de la difusión de la noticia y que debía entender en el

74. Nuñez, *Silvia Adriana c/ Comunicaciones y Medios S.A. y otro s/ D. y P.X Resp. Extracont. de Part.*, Cámara de Apelaciones en lo Civil, Comercial, Laboral y de Minería de la Circunscripción Judicial de Neuquén, Sala I, Expediente N° 367756/8, 5 de marzo de 2009. Fuente: *elDial.com* - AA55F1, publicado el 09/09/2009.

caso la Justicia de la Provincia de Neuquén. La Cámara entendió que los argumentos del juzgado de primera instancia para rechazar el planteo de incompetencia indicaban que el rechazo estuvo basado, en realidad, en el artículo 5° inciso 5° del Código Procesal Civil y Comercial de Neuquén, que expresaba que

cuando la jueza de grado la rechaza [la incompetencia], si bien dice que lo hace por [...] art. 5to inc. 4to, del desarrollo de la argumentación –al señalar que siendo dos los demandados, la actora ha hecho uso de la opción de iniciar la causa en esta jurisdicción, surge que lo funda, precisamente, en el inciso 5to⁷⁵–.

La Cámara de Apelaciones argumentó que:

Así entendemos que resulta aplicable al caso lo dicho en PI 2005 N°307 T°III F°529/531 y PI 2004 N° 63 T°I F° 107/111, en donde se receptaron los argumentos del Dr. Luis SILVA ZAMBRANO como juez subrogante en el TSJ, en el caso *Ullman*: «Así, en la presente especie, lo que resulta comprensible en orden a los delitos cometidos por la prensa desde el punto de vista del derecho penal, en cuanto a la atribución de la competencia al juez del lugar de la impresión del medio escrito (o de la emisión radiofónica o televisiva en su caso), al facilitarse tanto la averiguación del presunto ilícito como el derecho de defensa del imputado, no necesariamente guarda estricta equivalencia con el derecho civil, y más precisamente, con el que ha dado en denominarse “derecho de daños” en el que el Ordenamiento asienta su mirada, principalmente, en el damnificado con la finalidad de resarcirlo del daño que se le ha infligido».-

Desde esta perspectiva, pues, es legítimo plantearse, como lo hace la Cámara *a quo*, que el «lugar del hecho» al que hace referencia el art. 5°, inc. 4°, del Código Procesal Civil y Comercial de esta provincia, sea aquel en el que el actor tenga su domicilio o su residencia o negocio habituales, es decir, el lugar en el que la publicación «repercute» en aquellas personas que corrientemente están en contacto más o menos directo con el demandante o tienen conocimiento de él, sea por motivos personales, profesionales o de negocios.-

75. *Ídem*.

Entonces, en mi entender, la óptica del derecho de daños impone esta distinción, pues, en tanto que en la esfera represiva se trata de garantizar la investigación y la defensa del acusado, aquí, en vez, la «Justicia» pasa, sobre todo, por ese «restañar el daño», que importa, principalmente, el «mirar» al perjudicado.-

Ahora bien, dicha «mirada» entraña no solo la motivación implicada por el «principio de inmediación», sino, fundamentalmente, por la posibilidad concreta de acceso a la Justicia. O sea: si he sido perjudicado por un medio impreso, emitido o propalado en una jurisdicción extraña (y aunque no sea este el caso, tal vez lejana), como regla general, no resultaré «perjudicado» en aquella «extraña jurisdicción», sino en el lugar en el que normalmente transcurre mi existencia, mi vida de relación.-

Y así pues, como el «medio contó con recursos económicos y técnicos para “extender” su influencia (y, concretamente, «causar daño») en otro ámbito jurisdiccional, tiene que estar también preparado para asumir su responsabilidad en él, y de hecho, normalmente lo está, al menos con mucha mayor facilidad que lo que la generalidad de los particulares damnificados puede llegar a estarlo para litigar en ámbitos ajenos.-

En resumidas cuentas: el «lugar del hecho» es aquel en el que el daño tuvo «realmente» lugar, lo que es aquí equivalente a decir aquel en el que la persona lleva a cabo su «vida de relación», porque es esta, precisamente, la que se ve afectada por el hecho calificado como ilícito y, si decimos que, para «restablecer» adecuadamente su indemnidad, vamos a observar primordialmente al damnificado, consecuentemente también daremos prioridad al «lugar» en el que él deba litigar porque va en ello, en alguna medida, su posibilidad efectiva de acceder a un tribunal de justicia, es decir, que la solución que a este respecto se establezca, comprometerá en cierta manera la garantía de la defensa en juicio de sus derechos (garantía constitucional del debido proceso) y, en ese orden de ideas, mal se predicaría acerca de los «medios» –de poderío económico normalmente superior al de la generalidad de los particulares– que fuesen a verse realmente perjudicados en la defensa de sus derechos por tener que litigar en un medio extraño, pero, en todo caso, ante el dilema de que a alguien le cupiera soportar algún demérito, es justo que sea a ellos.-

Sé que a todo ello se objetará, tanto una zona de indefinición cuando la «vida de relación» pudiera desarrollarse en más de un lugar, como el que se están «confundiendo» la competencia y la garantía de la defensa en juicio, mas respondo diciendo, a lo primero, que así y todo es preferible asumir dicha ambigüedad que acaso generaría un «derecho de opción» para el actor y, a lo segundo, que en el fondo de todo auténtico conflicto de competencia, hay una pugna por lograr que entienda un tribunal que, estimamos, es el que nos dará la razón, sea por su especialización, sea por su proximidad con motivo del domicilio o lugar de residencia, etc., de suerte tal que, estimamos, podrá comprender más cabalmente el caso y sus argumentos, es decir, que esa contienda alienta siempre la cuestión de lograr una cabal defensa de nuestros derechos. (STJ NEU, Acuerdo N°02 de fecha 24 de junio de 2002, del voto de la minoría)⁷⁶.

Con base en estos fundamentos, la Cámara entendió que era competente el juez de la provincia de Neuquén, de conformidad con lo dispuesto por el artículo 5°, inciso 4° del Código Procesal Civil y Comercial de Neuquén⁷⁷.

II.B.I.c. ALIFANO, ROBERTO FRANCISCO S/RECURSO DE QUEJA, CÁMARA NACIONAL DE CASACIÓN PENAL, EXPEDIENTE N° 9375, 3 DE MARZO DE 2009. El señor Roberto Francisco Alifano inició una querrela por injurias en la Ciudad de Buenos Aires con motivo de frases presuntamente injuriantes, que se habrían vertido el 5 de noviembre de 2006 en el diario *La Gaceta*, de Tucumán, República Argentina.

Mediante resolución de fojas 29/30, el Juzgado Correccional N°14 de la Capital Federal declaró su incompetencia territorial a favor del Juzgado Correccional de la Ciudad de San Miguel de Tucumán, provincia de Tucumán.

El señor Roberto Alifano apeló esta decisión. La Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal resolvió, mediante resolución del 29 de abril de 2008⁷⁸, que

76. *Ídem*.

77. *Ídem*.

78. Véase Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, *Alifano, Roberto Francisco s/ incompetencia*, Causa N° 34.227, 29 de abril de 2008.

es criterio del tribunal que los delitos de calumnias e injurias deben considerarse cometidos en el lugar en el que se exteriorizaron los términos presuntamente agraviantes y, cuando ellos son reproducidos por la prensa, corresponde atribuir la competencia al magistrado del lugar donde se realizó la impresión de las expresiones cuestionadas (*in re causa* nº 29 187 *Rodríguez Saa*, rta. 24/8/2006, entre otras) [...] Tal interpretación coincide con la sustentada por la Corte Suprema de Justicia de la Nación (Fallos 311:2537; 312:987; 323:2210; 310:2263; 303:1231; 323:549; 323:2210; 323:4095) y debe primar en este caso, aun cuando la querellante haya tomado conocimiento de los dichos presuntamente ofensivos vía Internet en esta ciudad, pues la divulgación que posibilita el ciberespacio es *erga omnes* –como señala el apelante– y por tanto difusa e indeterminada, en virtud de lo cual, deberá estarse al lugar de la edición impresa.

Sobre la base de estos argumentos y a lo dispuesto por los artículos 37 y 39 el Código Procesal Penal de la Nación⁷⁹, la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal resolvió confirmar la resolución del Juzgado Correccional N°14 de la Capital Federal que había declarado su incompetencia territorial a favor del Juzgado Correccional de la Ciudad de San Miguel de Tucumán, provincia de Tucumán.

II.B.I.d. *RODRÍGUEZ, DIEGO S/DESESTIMACIÓN, CÁMARA NACIONAL CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, SALA IV, EXPEDIENTE N° 24574, 6 DE OCTUBRE DE 2004*. En primera instancia, se decidió declarar inadmisibile la

79. A continuación, se transcriben los artículos mencionados del Código Procesal Penal de la Nación.

Art. 37. - Será competente el tribunal de la circunscripción judicial donde se ha cometido el delito.

En caso de delito continuado o permanente, lo será el de la circunscripción judicial en que cesó la continuación o la permanencia.

En caso de tentativa, lo será el de la circunscripción judicial donde se cumplió el último acto de ejecución.

[...]

Art. 39. - En cualquier estado del proceso, el tribunal que reconozca su incompetencia territorial deberá remitir la causa al competente, poniendo a su disposición los detenidos que hubiere, sin perjuicio de realizar los actos urgentes de instrucción.

presentación de los querellantes contra Diego Luis Rodríguez por los delitos de calumnias e injurias. Los querellantes apelaron esa decisión. La Sala IV de la Cámara Nacional, Criminal y Correccional de la Capital Federal consideró que correspondía revocar lo decidido en primera instancia, porque el planteo de los querellantes «resulta acorde con las exigencias previstas en el art. 418 del Código Procesal Penal»⁸⁰. La Sala IV de la Cámara Nacional, Criminal y Correccional de la Capital Federal continuó expresando que:

En tal sentido, lleva la razón el recurrente en torno a la cuestión de competencia territorial, pues «... en los llamados delitos a distancia, el hecho punible se estima cometido en todas las jurisdicciones en la cuales (sic) se ha desarrollado la acción y también en el lugar de la verificación del resultado. Dicha regla permite la elección de una de esas jurisdicciones atendiendo a las exigencias planteadas por la economía procesal, la necesidad de favorecer, junto con el buen servicio de justicia, la defensa de los imputados» (C.S.J.N., *Servira* del 23/11/1983, Fallos 305:1993) Este antecedente jurisprudencial, resulta de vital importancia para el caso *sub examine*, toda vez que las presuntas injurias y calumnias han sido propagadas mediante el uso de un sitio de Internet, pudiendo verificarse sus efectos en infinidad de lugares;

80. Véase *Rodríguez, Diego s/desestimación*, Cámara Nacional Criminal y Correccional de la Capital Federal, Sala IV, Expediente N° 24574, 6 de octubre de 2004. Nota: El artículo 418 del Código Procesal Penal establece:

La querrela será presentada por escrito, con tantas copias como querrelados hubiere, personalmente o por mandatario especial, agregándose en este caso el poder, y deberá expresar, bajo pena de inadmisibilidad:

- 1°) El nombre, apellido y domicilio del querellante.
- 2°) El nombre, apellido y domicilio del querrelado o, si se ignoraren, cualquier descripción que sirva para identificarlo.
- 3°) Una relación clara, precisa y circunstanciada del hecho, con indicación del lugar, fecha y hora en que se ejecutó, si se supiere.
- 4°) Las pruebas que se ofrecen, acompañándose en su caso la nómina de los testigos, peritos e intérpretes, con indicación de sus respectivos domicilios y profesiones.
- 5°) Si se ejerciere la acción civil, la concreción de la demanda con arreglo al artículo 93.
- 6°) La firma del querellante, cuando se presentare personalmente, o de otra persona, a su ruego, si no supiere o pudiere firmar, en cuyo caso deberá hacerlo ante el secretario. Deberá acompañarse, bajo pena de inadmisibilidad, la documentación pertinente y de la que se haga mérito; si no fuere posible hacerlo, se indicará el lugar donde se encontrare.

Fuente: <<http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/383/texact.htm#16>>. [Nota del editor: consultado el 12/11/11.]

habrá de estarse al que el imputado considere mejor a fin de poder ejercer su derecho de defensa.

Con estos argumentos, la Sala IV de la Cámara Nacional, Criminal y Correccional de la Capital Federal resolvió revocar la resolución, ya que declaró inadmisibile la presentación efectuada por los querellantes contra Diego Luis Rodríguez por los delitos de calumnias e injurias.

II.B.I.e. *N.N. s/ INJURIAS*. CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, SALA IV, EXPEDIENTE N° 1589/09, 21 DE OCTUBRE DE 2009. En primera instancia se dispuso declarar la incompetencia del Juzgado Nacional en lo Correccional de la Capital Federal N°1. La querrela interpuso recurso de apelación contra esa decisión.

La Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal resolvió revocar la decisión de primera instancia, con base en que:

Los argumentos que expone la querrela logran rebatir los fundamentos de la decisión del magistrado de grado, por lo que el auto impugnado habrá de ser revocada (sic).

En casos como el de autos (injurias a distancia), el criterio que debe prevaler para determinar la consumación [y la competencia del juez] es el de la toma de conocimiento por parte del destinatario a quien se desea ofender (*Código Penal comentado y anotado*, Andrés José D'Alessio-Mauro-Divito, Parte especial, artículos 79 a 306, La Ley, Buenos Aires, 1ª edición, año 2004, pág. 119), pues si el correo electrónico con las frases injuriantes no llegaran a destino, el ataque al honor no se hubiera realizado, y por ende nunca hubiera tenido conocimiento de ello la víctima.

Además, reconocida doctrina ha sostenido que «...cuando se trata de una comunicación escrita no cerrada, de las que son hoy las manifestaciones más frecuentes los telegramas, las postales, los e-mails, los mensajes de texto de la telefonía celular y las páginas de Internet, la injuria se consume al llegar a conocimiento del destinatario si se trata de una versión que tiene únicamente aptitud deshonrosa...» (Fontán Balestra, Carlos, *Tratado de Derecho Penal*, Tomo IV, Ed. Abeledo Perrot, Buenos Aires, 2007, pág. 339). En este sentido, surge de la causa que la denunciante manifestó haber tomado conocimiento del contenido del correo electrónico en su computadora personal ubicada en su domicilio sito en la Avenida

Directorio 151, piso 3° de este medio, por lo que, de momento, deberá estarse a los dichos de quien se considera damnificada.

II.B.II. Casos resueltos por la Corte Suprema de Justicia de la Nación

La jurisprudencia de la Corte Suprema argentina que hemos encontrado es uniforme respecto de la determinación de la competencia en los casos penales. Para evitar repeticiones, citamos solo un caso que expone el criterio del máximo tribunal argentino.

II.B.II.a. *VERAZAY, SANTOS JUSTO S/ QUERELLA POR CALUMNIAS E INJURIAS*, CORTE SUPREMA DE JUSTICIA DE LA NACIÓN, COMPETENCIA N°1085. XLIII. En este caso, se generó una disputa sobre competencia entre los integrantes de la Sala I de la Cámara en lo Penal de San Salvador de Jujuy, provincia de Jujuy, y el Juzgado en lo Correccional y de Garantías N°4 de Salta, provincia de Salta. La Corte Suprema resolvió esa controversia⁸¹ de acuerdo con lo que prescribe el artículo 16 de la Constitución Argentina⁸².

El dictamen del Procurador Fiscal del 28 de marzo de 2008 relata que el gerente de A.D.A.I.C.O.P. SALTA S.R.L. inició una querella por los delitos de calumnias e injurias contra la Sociedad Argentina de Autores y Compositores de Música (S.A.D.A.I.C.). En una conferencia de S.A.D.A.I.C. en Salta, los representantes de esta organización habrían sugerido que A.D.A.I.C.O.P. SALTA tenía como finalidad estafar a sus representados, dado que la organización no ingresaba los aportes de los autores a S.A.D.A.I.C.⁸³. El dictamen explicaba que el querellante tomó conocimiento de las declaraciones por medio del sitio web del diario *El Tribuno* de Salta, mientras se encontraba en su domicilio de

81. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII. Véase [en línea] en: <<http://www.csjn.gov.ar>>. [Nota del editor: consultada el 12/11/11.]

82. Art. 16:

Corresponde a la Corte Suprema y a los tribunales inferiores de la Nación, el conocimiento y decisión de todas las causas que versen sobre puntos regidos por la Constitución, y por las leyes de la Nación, con la reserva hecha en el inciso 12 del artículo 75: y por los tratados con las naciones extranjeras: de las causas concernientes a embajadores, ministros públicos y cónsules extranjeros: de las causas de almirantazgo y jurisdicción marítima: de los asuntos en que la Nación sea parte: de las causas que se susciten entre dos o más provincias; entre una provincia y los vecinos de otra; entre los vecinos de diferentes provincias; y entre una provincia o sus vecinos, contra un Estado o ciudadano extranjero.

83. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

la ciudad de Jujuy⁸⁴. El dictamen también aclara que, con fundamento en que la conferencia de prensa en cuestión tuvo lugar en Salta y que allí habrían sido impresos y reproducidos los dichos por la prensa escrita, los integrantes de la Sala I de la Cámara Penal de Jujuy se inhibieron para conocer en la causa. Según refiere el Procurador Fiscal, «sostuvieron que ello es así, sin perjuicio de que el agraviado hubiese tomado conocimiento de esas expresiones desde la computadora ubicada en su domicilio de Jujuy (fs. 110)»⁸⁵.

Por otra parte, la jueza de Salta entendió que debía continuar conociendo en el caso la Justicia de Jujuy, por tener allí su domicilio el querellante y dado que allí «se habría consumado el delito cuando el damnificado tomó conocimiento por medio de la conexión a un sitio “web” correspondiente a la página que exhibe las publicaciones de un diario salteño» (fs.112/115)⁸⁶. El tribunal de segunda instancia de Salta insistió en su criterio⁸⁷.

El Procurador Fiscal sostuvo, citando la jurisprudencia de la Corte Suprema que

El Tribunal tiene dicho que los delitos como los que aquí se imputan deben considerarse cometidos en el lugar en el que se exteriorizaran los términos presuntamente agraviantes, y cuando ellos son reproducidos por la prensa, corresponde atribuir la competencia al magistrado del lugar donde se realizó la impresión de las expresiones cuestionadas (Fallos: 312:987 y 318:857) [...] Por aplicación de estos principios y habida cuenta que las expresiones presuntamente injuriantes publicadas por el diario *El Tribuno* de Salta –las que luego reprodujeron otros diarios de esa misma provincia– fueron editadas allí –circunstancia no cuestionada por la magistrada salteña– (ver fs. 48/51 y 112/115), opino que corresponde al juzgado de la provincia de Salta, conocer en las presentes actuaciones⁸⁸.

Con base en estos fundamentos, la Corte Suprema declaró el 28 de abril de 2008 que debía entender en la causa en la que se originó el incidente el Juzgado Correccional y de Garantías N° 4 de la 4ª Nominación Judicial de la provincia de Salta⁸⁹.

84. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

85. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

86. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

87. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

88. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

89. Corte Suprema de Justicia de la Nación. Competencia N° 1085. XLIII, *supra* nota 80.

II.C. Situaciones en otros países de la región

Como expresamos al comienzo de este capítulo, la recopilación de jurisprudencia en nuestra región es sumamente difícil por razones que son ajenas a este trabajo. En varios países se consultaron expertos u organizaciones que nos relataron situaciones que, si bien no tenemos decisiones judiciales específicas, demuestran alguna de las líneas de pensamiento que tienen los actores judiciales y otros gubernamentales que actúan en la región.

En **Uruguay**, una sentencia judicial del Tribunal de Apelaciones de Familia estableció que las publicaciones en Internet no son un medio de comunicación en los términos que establece la ley de prensa N° 16099. El caso se originó ante la denuncia de los padres de una alumna de colegio cuya foto había sido publicada en un blog. Ante la denuncia, el fiscal solicitó que esa cuestión fuera juzgada por la ley de prensa. El juez de menores rechazó esa petición. Ante una apelación del fiscal, el Tribunal de Apelaciones de Familia consideró que la pretensión del fiscal debía ser rechazada porque la ley N° 16099 se refiere a los medios que cita el artículo 6°. Este artículo de la ley fija las condiciones para ser redactor responsable de un medio de comunicación, escrito, radial o televisivo. El fallo sostuvo que «sin duda, de acuerdo al encuadre doctrinario y fáctico señalado, una publicación en Internet de la fotografía de una persona, con comentarios más o menos hirientes, no responde al modelo legal de publicación en un medio de comunicación que señala la ley nacional», y aclaró que los autores de esas publicaciones en Internet pueden, sin embargo, ser sometidos a una investigación por la ley de difamación e injurias. Como vemos, los jueces no asemejan una publicación en Internet a una publicación en la prensa. Sin embargo, en los casos argentinos, parece que sí lo hacen⁹⁰.

Un caso de **México** que tuvo amplia repercusión pública internacional merece ser incluido en este trabajo, si bien no se trató de un caso vinculado con Internet.

Luego de publicar su libro *Los Demonios del Edén*, la periodista mexicana Lydia Cacho fue enjuiciada en Puebla por difamación por el empresario Kamel Nacif Borge. En el libro, la periodista habría señalado

90. Agradecemos la información sobre este caso a Edison Lanza, académico y periodista uruguayo y director de la ONG CAINFO.

que el empresario estaba ayudando a un pederasta⁹¹. El juicio de difamación contra la periodista fue iniciado en Puebla. La periodista fue detenida en Cancún, su lugar de residencia, y trasladada a la prisión de Puebla, en donde habría permanecido en el Ministerio Público durante treinta horas⁹². Ella habría denunciado haber sido víctimas de amenazas y humillaciones durante el traslado⁹³. Ante una solicitud de la periodista, el Tribunal Superior de Justicia de Puebla resolvió trasladar el caso a Cancún. La argumentación de la periodista se fundó en que el presunto delito se habría cometido en el Distrito Federal, porque allí se difundió el libro y que ella vivía en Cancún. Alegó que el motivo de que su juicio fuera llevado a Puebla era que Kamel Nacif tendría amistad con el gobernador de ese estado. Si bien no se trata de un caso donde las expresiones fueron vertidas por Internet, el caso es relevante porque se puede suponer que la querrela se inició en Puebla por ser una jurisdicción donde los estándares legales para que se configure un delito de difamación son más fáciles de cumplir que en otras jurisdicciones de México. Si es así, este sería un ejemplo de «turismo de difamación»⁹⁴ tema al que nos referiremos más adelante.

En **Costa Rica**, de conformidad con el artículo 20 del Código Penal, el hecho delictivo se entiende cometido tanto en el lugar en que se produjo en todo o en parte la actividad delictuosa como donde se produjo o pudo haberse producido el resultado. Ahora bien, tratándose de delitos en que es difícil o imposible establecer dónde han tenido efecto, como son los producidos en medios de circulación masivo o numerosos, por lo que el lugar determinable es el de la comisión del ilícito y no el de sus efectos, se impone la aplicación del inciso *a* del artículo 47 del Código Procesal Penal, que otorga la competencia al tribunal en cuya competencia territorial fueron cometidos los hechos. Es decir, donde está el *server* o la imprenta; a menos, claro está, que estos se encuentren en el extranjero y tengan efectos (por ejemplo, ofendiendo los derechos de un costarricense) en la República, en

91. Véase «Trasladan juicio contra Lydia Cacho a Cancún », en *es mas*, el 20 de enero de 2005, disponible [en línea] en: <<http://www.esmas.com/noticierostelevisa/mexico/505582.html>> . [Nota del editor: consultada el 12/11/11.]

92. Véase «Pierde Kamel Nacif juicio contra Lydia Cacho», en *cimac noticias*, el 3 de enero de 2007, disponible [en línea] en: <<http://www.cimacnoticias.com/site/07010312-Pierde-Kamel-Nacif.16091.0.html>> . [Nota del editor: consultada el 12/11/11.]

93. *Ídem*.

cuyo caso la competencia la tienen los tribunales de la capital (inciso *b* de ese mismo artículo 47)⁹⁴.

Una situación interesante que encontramos también en Costa Rica se produjo el 19 de mayo de 2010, cuando abogados del Gobierno panameño dieron a conocer un comunicado oficial de la Secretaría de Comunicación según el cual «demandarán en los próximos días –en Costa Rica– al diario digital costarricense *El País* y a las personas responsables de difamar a Panamá»⁹⁵. El motivo de esta determinación era que el Gobierno panameño consideraba que las publicaciones del diario digital costarricense *El País* atentaban contra la seguridad del Estado y del Canal de Panamá⁹⁶. Asimismo, el comunicado expresaba que el autor de los reportajes del periódico digital es responsable por difamación por afirmar en una radio local que el Canal de Panamá está administrado por israelitas, lo cual, según el Gobierno, puede poner en peligro la seguridad del Estado⁹⁷. En el diario digital, se habría alegado que el Gobierno panameño prestó poca ayuda a los Estados Unidos en su lucha contra el narcotráfico y que personas cercanas a un primo del mandatario panameño estarían vinculadas con el narcotráfico⁹⁸.

Con fecha 10 de mayo de 2011, la Procuraduría General de la República de **Costa Rica** dictó la resolución PGR-057-2011, que estaba dirigida al Procurador General de la Nación Suplente (encargado) de la República de Panamá. En esa resolución, la Procuraduría responde a una misiva del Procurador panameño del 7 de junio de 2010, mediante la cual, el procurador panameño solicita a la Procuraduría costarricense que ordene una investigación en relación con publicaciones del periódico digital de Costa Rica *Nuestro País* (www.elpais.cr). El Procurador panameño considera que los dichos de las publicaciones son falsos y que podrían perjudicar las relaciones amistosas entre los Gobiernos de Costa Rica y Panamá. Según la resolución,

94. Este criterio nos fue proporcionado por Ricardo Salas Porras, Letrado de la Sala Tercera de la Corte Suprema. Agradezco a Paul Rueda, Magistrado de la Corte quien me proporcionó esta información.

95. Véase «El Gobierno de Panamá demandará por difamación a [elpais.cr](http://www.elpais.cr)», en *el país.cr.*, el 19 de mayo de 2010, disponible [en línea] en: <<http://www.elpais.cr/articulos.php?id=24504>>. [Nota del editor: consultada el 12/11/11].

96. *Ídem.*

97. *Ídem.*

98. *Ídem.*

Las citadas publicaciones, según el documento que nos ocupa, han surgido de textos emitidos los días 7, 10 y 13 de mayo, todos del año en curso, así como de una entrevista telefónica sostenida con el Sr. Carlos Salazar Fernández (transmitida en *Radio Emisora kW Continente*, programa radial denominado *Hora 9*), en las que se expresan manifestaciones críticas a decisiones de Gobierno del Presidente de la República de Panamá, Sr. Ricardo Alberto Martinelli⁹⁹.

También según la resolución, el procurador panameño

cita como sustento de su reclamo el artículo 282 del Código Penal costarricense, que refiere el delito de «Actos Hostiles» (Título XI Delitos contra la Seguridad de la Nación, Sección II Delitos que comprometen la paz y la dignidad de la Nación) en conexión con el artículo 16 del Código Procesal Penal de Costa Rica (Capítulo I Acción Penal, Ejercicio), que brinda a la Procuraduría General de la República la posibilidad de ejercer la acción penal sin subordinarse a las actuaciones del Ministerio Público, en delitos contra la seguridad de la Nación, entre otros.

El Procurador General costarricense concluye que debe dar una respuesta negativa a lo solicitado por el Procurador panameño, con fundamento en que por un lado los hechos descritos no encuadran en el delito de “actos hostiles” (ya que las actuaciones llevadas a cabo por el señor Salazar Fernández no encuadran como un acto material que califique como hostil), y por el otro lado, la condición de víctima recae en nuestro país y no se aqueja o perciben consecuencias directas del mismo para Costa Rica¹⁰⁰.

En cuanto a la cuestión del «principio de personalidad activa», la resolución analiza que

de la información contenida en su misiva y que conforma una de las razones por las cuales se solicita nuestra intervención,

99. Resolución de la Procuraduría General de la República de Costa Rica PGR-057-2011, 10 de mayo de 2011.

100. *Ídem*.

se deduce que las publicaciones y manifestaciones referidas lo fueron a través de un medio periodístico cuyo origen –en forma presunta– es costarricense (por el dominio de registro «cr»), mas lo cierto es que las emisiones de referencia pueden perfectamente no haber sido emitidas en suelo nacional –pues los usos informáticos lo permiten–, lo que acarrearía problemas de competencia territorial. Igualmente se podría decir del origen del señor Salazar Fernández, ya que de su libelo no se desprende la nacionalidad de dicha persona, aunque se puede suponer que sea costarricense. Sin embargo, recientemente, a través de la Ley de Fortalecimiento de la Legislación contra el Terrorismo, N° 8719 de 4 de marzo de 2009, se adicionó un inciso 4) al numeral 6° del Código Penal, en el que se incluyó el principio de personalidad activa, consignándose que: «ARTÍCULO 6°.- Podrá incoarse proceso por hechos punibles cometidos en el extranjero y en ese caso aplicarse la ley costarricense, cuando:... 4) Hayan sido cometidos por algún costarricense...». Lo anterior permite proceder sin hacer reparos del lugar de comisión de las actuaciones que se presumen delictivas, aplicándole al señor Salazar Fernández dicho principio que dispone que la ley doméstica seguirá al nacional donde este se encuentre¹⁰¹.

En **Panamá**, no encontramos muchos casos resueltos por tribunales que tuvieran vinculación con difamaciones en Internet y que no hubiera vinculación estrictamente panameña y dentro del territorio. La información que obtuvimos para realizar este trabajo es que los casos judiciales existentes de reparación por daños se resolvieron con la doctrina habitual que dispone la jurisdicción donde se producen los efectos del daño¹⁰².

Un caso que tuvimos conocimiento es el relacionado con Patrick Visser, un ciudadano holandés que dirige un proyecto de reforestación de la empresa Silva Tree, quien inició una querrela penal por calumnias e injurias contra periodistas que escribieron artículos en el periódico *The Christian Science Monitor* y en el blog *Bananama Republic* en los que se cuestionó

101. *Ídem* (sin formato).

102. Agradecemos esta información a Ricardo Lombana, académico y abogado panameño.

la legitimidad de las actividades de la empresa¹⁰³. Otras personas figuran también como querellantes. La empresa Silva Tree está basada en Inglaterra y tiene una subsidiaria en Panamá. La querrela fue presentada en Panamá contra Okke Ornstein, periodista a cargo del blog *Bananama Republic* y Sara Miller Llanas, periodista del periódico estadounidense *The Christian Science Monitor* (CSM).

Okke Ornstein es un ciudadano extranjero que escribe su blog principalmente desde Panamá, pero también desde otras ubicaciones. La página del blog está registrada en los Estados Unidos y el servidor de la página del blog está ubicado en Florida, en los Estados Unidos. Sara Miller Llanas es corresponsal de *The Christian Science Monitor* para América Latina y reside en México.

Con la representación de abogados estadounidenses, Visser escribió una carta a GoDaddy, la empresa que proporciona *hosting* al servicio para *Bananama Republic*, para solicitar que el blog fuera dado de baja. En la carta, Visser amenaza con el inicio de una acción por difamación en Florida y alega daños sufridos por Visser por un monto de 200 000 dólares estadounidenses. A la fecha, no tenemos conocimiento de esos procesos civiles conocidos iniciados a la fecha en ninguna jurisdicción contra los periodistas.

La Fiscalía Séptima de Circuito del Primer Circuito Judicial de Panamá inicialmente solicitó el sobreseimiento de los querellados por entender que no podía accionar en un caso de Internet¹⁰⁴. Ante la apelación de los querellantes, un juez ordenó que el caso prosiguiera al considerar que Internet es un medio de comunicación. Ornstein fue comunicado de esta decisión en febrero de 2011. El próximo paso legal sería que los querellados fueran llamados a prestar declaración indagatoria, y luego la Fiscalía determinaría si el caso iría a juicio. La Fiscalía requirió información sobre *Bananama Republic* y *The Christian Science Monitor* a Google Inc, GoDaddy y al proveedor de *posting* del *Christian Science Monitor*. A la fecha, estas solicitudes de información no han sido respondidas. Según comenta Okke Ornstein, ha sido querellando en varios otros casos en Panamá por artículos publicados en su blog, y ninguno de ellos resultó en una condena.

103. Véanse [en línea] los artículos: <<http://www.csmonitor.com/Environment/2010/0420/Carbon-offsets-Using-the-green-cloak-of-certification-to-sell>>; <<http://www.bananamarepublic.com/2010/04/20/panama-is-open-for-business-3-silva-tree-reforestation-scam>>. [Nota del editor: consultadas el 12/11/11.]

104. La querrela tramita bajo el número de expediente 206-10.

III. Algunas observaciones y propuestas para América Latina

Hasta aquí hemos relatado algunas decisiones judiciales y opiniones de expertos en América Latina y en otras regiones que traen argumentos para determinar la jurisdicción por razón de lugar en casos donde el contenido de una expresión difamatoria sea advertido por Internet por el destinatario de esa expresión. Como mencionamos anteriormente, no ha sido objeto de este trabajo llevar adelante una recopilación exhaustiva de decisiones judiciales, sino, antes bien, exponer una suerte de «muestreo» de algunas que consideramos relevantes y que aportan argumentos para la reflexión sobre el tema que tratamos de resolver.

También expusimos antes que la determinación del juez o tribunal que resulte competente para atender las acciones penales o civiles que se inicien por expresiones difamatorias tiene una consecuencia práctica importante: si se trata de un juez o tribunal que no garantiza su independencia de presiones externas –por ejemplo, del Gobierno–, si no existen reglas claras para determinar la jurisdicción, el demandante o querellante podrá decidir sobre el juez que más le convenga, por ejemplo, aquel que sea más fácil de presionar. Por supuesto que también la selección del juez puede obedecer a la ley que se aplicará: el querellante o demandante podrá decidir su acción judicial en aquel lugar que la decisión le sea más favorable. De esto se ha ocupado recientemente lo que mencionamos al comienzo como el «turismo de difamación» (*libel tourism*).

En América Latina estas dos circunstancias se hacen presentes. No es este el lugar para ahondar sobre los problemas de falta de independencia judicial en varios países¹⁰⁵. Tampoco podemos extendernos sobre las diferentes leyes que podemos encontrar aplicables en distintos lugares. Solo a modo de ejemplo resaltamos que mientras en algunos países, se ha despenalizado parcialmente la difamación cuando la expresión se vincula con asuntos de interés público (por ejemplo, la Argentina) en otros quedan vigentes y se aplican delitos de «desacato», que permiten llevar a juicio penal a quienes formulan críticas a sus funcionarios (Ecuador).

105. Sobre problemas de la falta de independencia judicial en países de la región véanse, por todos, los informes de la organización no gubernamental Due Process of Law Foundation - DPLF, accesibles en www.dplf.org. Sobre el mismo problema, enfocado en Argentina véanse, por todos, informes de la organización no gubernamental ANDHES en www.andhes.org.ar.

Por lo tanto, resulta importante estudiar y formular algunas ideas sobre cómo debería resolverse la cuestión de la jurisdicción territorial que hemos planteado en este artículo para que se impida su manipulación y su consecuente efecto nocivo para el ejercicio de la libertad de expresión.

Los argumentos que hemos visto en la jurisprudencia y en las opiniones relatadas más arriba pueden resumirse de la siguiente manera:

- a) El/la juez/a competente es aquel/la juez/a que se encuentra domiciliado/a en el mismo sitio que quien realizó la expresión difamatoria¹⁰⁶.
- b) El/la juez/a competente es aquel/la juez/a que se encuentra domiciliada/a en el mismo sitio que la víctima de la expresión difamatoria¹⁰⁷.
- c) El/la juez/a competente es aquel/la juez/a que se encuentra domiciliado/a en el mismo sitio que el autor de la expresión o la víctima, dependiendo si se trata de una acción civil o una acción penal¹⁰⁸.
- d) El/la juez/a competente es aquel/la que se encuentra domiciliado/a en el mismo sitio en el que fue «impreso» el contenido difamatorio¹⁰⁹.
- e) El/la juez/a competente es aquel/la que se encuentra domiciliado/a en el mismo sitio que el servidor donde se halla la expresión difamatoria¹¹⁰.

El asunto por resolver es si alguna de estas reglas generales nos satisface plenamente para que pueda ser considerada una propuesta de legislación generalizada en los países y que no afecte el ejercicio de la libertad de expresión. Pasamos entonces a mencionar algunas de las preocupaciones que surgen del análisis de estas reglas generales.

106. Este es el argumento implícito en una sentencia de una Cámara de Apelaciones de la Provincia de Neuquén, en el caso *Nuñez*, *supra* citado.

107. Este es básicamente el argumento de *Calder c/ Jones*, *supra* citado, y que se siguió utilizando en otros casos ya relacionados con Internet. El caso argentino citado más arriba no puede ser pasado por alto: luego de entender que en los casos de difamación por Internet los actos se producen en el «cyberespacio» (sic), concluyeron que debía solucionarse la controversia dando la competencia al juez del domicilio de la víctima. Véase caso resuelto en la jurisdicción de la provincia de Salta, ya citado. Argumentos similares se expusieron en el caso *Sharkey*, en Brasil.

108. Una cámara de apelaciones de la provincia de Neuquén, en la Argentina, en el caso *Nuñez*, antes citado, propuso este argumento.

109. Este argumento es el que ha sostenido, entre otros, la Corte Suprema de Justicia de la Argentina en decisiones citadas más arriba.

110. Este fue uno de los argumentos expuestos en el caso australiano *Dow Jones c/ Gutnick*, *supra* citado. Google hizo un argumento similar en uno de los casos de la Argentina referidos en este trabajo.

La regla que otorga jurisdicción al juez del lugar de la «impresión», puede ser útil para un número muy limitado de casos. Si el contenido de una expresión difamatoria se encuentra en una publicación «impresa», por ejemplo, un periódico, pero que también tiene una versión digital, por ejemplo, un periódico digital, la regla del lugar de la «impresión» podría funcionar aunque el contenido difamatorio hubiera sido advertido solo por Internet. Sin embargo, cada vez más existe difusión de contenidos que no tienen una «impresión» tradicional por lo cual esta regla demuestra su inutilidad.

Quienes se aferran a sostener la aplicación de los criterios tradicionales (regla de la impresión) entendiendo metafóricamente que la situación en Internet es asimilable, se equivocan. Y su error reside en algo que varios autores han explicado y que consiste en el peligro de explicar situaciones vinculadas con Internet por medio de «metáforas» que no son apropiadas. Por ejemplo, pensar en que un blog se «imprime» de la misma manera que se imprime un diario y entonces asimilar un blog a un diario, nos lleva a una solución mediante la utilización de una metáfora que se encuentra equivocada¹¹¹.

Erróneamente podría entenderse asimilable la «impresión» con el alojamiento de los elementos que conforman el contenido de la expresión cuando es advertida en Internet. Pero según hemos visto y aun sin caer en ese error por elección de una metáfora equivocada, se ha propuesto que la jurisdicción sea la del lugar donde se encuentra el servidor en el que se encuentra la expresión. Esta regla, también resulta problemática, dado que en muchos casos, los servidores no se encuentran próximos al domicilio ni del autor de la expresión, ni de la persona a la cual la expresión estuvo dirigida. La consecuencia sería que la posible acción judicial –civil o penal– dejaría inconforme a ambos dado la dificultad de ejercerla¹¹².

111. Sobre el problema de cómo las metáforas o analogías, como mecanismo de argumentación, iluminan o deforman los casos referidos a Internet, véase, por todos, Bellie, Patricia, Paul Berman, Brett Frischmann y David Post, *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age*, 4ª edic., *sine loco*, Thomson Reuters, 2011.

112. El ejemplo paradigmático que se da para sostener que la ubicación de los servidores no resultará aceptable como regla lo brinda el caso del *Principado de Sealand*. Sealand es una plataforma militar abandonada ubicada cerca de la costa de Gran Bretaña. Esta fue reclamada por Roy Bates, que se la disputó al propio Gobierno británico (el escudo de Sealand dice «los mares son libres»). Entendiéndola como una nación independiente, se instaló la empresa Havenco, cuya actividad era la de proveer «el servicio de servidores más seguro del mundo y en el único lugar verdaderamente libre». Aludiendo a este caso, como un caso interesante desde el punto de vista académico, Jonathan Zittrain explica que no se trata del lugar donde los «bits» están alojados, sino donde se encuentran las personas que los crearon y que causaron un daño. Véase Zittrain, Jonathan, «Be Careful What You Ask For: Reconciling a Global Internet and Local Law», en *Harvard Law School Public Law, Research Paper N°60 (sine data)*, p. 5.

Las reglas que quedan nos llevan a la determinación de la jurisdicción teniendo en cuenta los domicilios del autor de la expresión o de la víctima de la expresión.

Hemos visto que una decisión judicial propuso una suerte de combinación, teniendo en cuenta si la acción es civil o penal. A primera vista, esta regla parece atractiva. Podría ser razonable establecer esta separación atendiendo, como lo explica el fallo, a los distintos fines de cada uno de los procesos (el civil o el penal). Empero, una aplicación a rajatabla de esta regla estaría a contravía de lo que están proponiendo muchos ordenamientos procesales penales modernos en América Latina, que impulsan el ejercicio de la acción penal *en conjunto* con la acción civil.

Sin perjuicio de las razones prácticas que no hacen recomendable esta regla como regla general, los fundamentos de esa norma serían cuestionables. Es cierto que una acción penal tiene un objetivo punitivo que requiere que quien es imputado pueda tener las mejores garantías de una defensa adecuada y ello lo puede conseguir en la jurisdicción próxima a su domicilio donde podrá ejercer mejor su derecho de defensa, tanto material como técnica. También es cierto que impedir ese derecho de defensa puede generar, además, un efecto inhibitorio de la expresión. Quien desee manifestar una expresión que puede ser considerada difamatoria en una jurisdicción que desconoce y que no podrá defenderse, posiblemente se autocensure y el efecto para el ejercicio de su libertad de expresión resulta negativo.

Sin embargo, resulta dudoso que una acción civil, sin perjuicio que persigue la reparación de una víctima, no pueda generar similares efectos disuasorios en quien desea expresarse¹¹³ En consecuencia, también podría ser inadecuada la regla que podemos llamar «de los efectos» de la expresión supuestamente difamatoria y que otorgaría la jurisdicción al juez donde se domicilia el destinatario de la expresión. Y si nuestra argumentación es correcta, entonces poco importa que la acción sea civil o penal.

La regla que ha sobrevivido hasta ahora, y que pareciera que ante una situación donde una expresión puede tener efectos en un número inimaginable de lugares, es la regla que determina que la jurisdicción se otorga atendiendo al domicilio de quien es el autor de la expresión. En

113. Al respecto, véanse opiniones de Roberto Saba y Julio Rivera, *supra* citadas.

ese lugar, quien efectúe expresiones podrá defenderse adecuadamente –civil o penalmente– y podrá anticipar el resultado de potenciales acciones –civiles o penales– porque conoce la actuación de los jueces y la ley que aplican. Parecería, entonces, que el efecto inhibitorio, problemático para sostener un adecuado ejercicio de la libertad de expresión, se minimiza.

No se nos escapa que esta regla se encuentra más inclinada a proteger la libertad de expresión que otros derechos que también son fundamentales, como por ejemplo, el honor. En otras palabras, será más complicado reclamar por su derecho quien se sienta «difamado», porque deberá hacerlo, en algunos casos, en jurisdicciones que son extrañas.

Este puede que no sea un problema nuevo y que la regla deba ajustarse atendiendo al tipo de expresiones que se trate, otorgándole una vigencia general a esa regla cuando se trate de expresiones que tengan que ver con cuestiones de interés público.

Empero, si esta regla también es puesta en duda, tal vez debamos abandonar la búsqueda de una regla general en el tema de la jurisdicción por razón de lugar en estos casos y concentrar los esfuerzos en impulsar regulaciones que impidan ejecutar decisiones que resulten a todas luces arbitrarias de acuerdo con los estándares que emanan, por ejemplo, del sistema interamericano de protección de derechos humanos¹¹⁴.

Esta puede ser una solución¹¹⁵ para paliar el efecto inhibitorio del que hemos hablado, dado que, a fin de cuentas, no importará quién ni sobre

114. Roberto Pereira, abogado y académico peruano, al comentar alguna de estas ideas durante el taller que se celebró en Buenos Aires el 12 y 13 de septiembre de 2011, simpatizó con esta idea y ofreció una redacción de una regla que debería ser adoptada por los países de la región para que sea efectiva. La propuesta expresa:

Quando se aleguen afectaciones al honor a través de Internet, será competente el juez del lugar del domicilio del autor del contenido difundido, o del lugar del domicilio del afectado, siempre que su derecho sea susceptible de ser afectado en dichos lugares.

En ambos casos, la competencia judicial estará condicionada a que rijan en el lugar legislaciones y decisiones jurisprudenciales compatibles con los estándares internacionales de protección de la libertad de expresión.

115. La solución adoptada por el estado de Nueva York, en los Estados Unidos de Norteamérica –seguida, por cierto, por muchos otros estados– va en ese sentido. En abril de 2008, se aprobó la *Libel Terrorism Protection Act* para proteger a autores y editores estadounidenses de demandas iniciadas y terminadas en jurisdicción extranjera. Básicamente, la ley determina la no ejecución de sentencias extranjeras cuando ellas no sigan la protección que otorga la primera enmienda de la Constitución de los Estados Unidos.

qué base dicta la sentencia. Lo único que importará es si es ejecutable o no¹¹⁶.

Como conclusión, Jonathan Zittrain nos propone una interesante reflexión:

Lo que se puede ganar implementando reglas que hagan fácil la solución de las tensiones que provoca el tema de jurisdicción, lo podemos perder en la capacidad revolucionaria de Internet. El punto de inflexión donde se asienta hace que nos preguntemos qué valoramos más –una armonía internacional y diversidad que incluya la censura como forma de represión o una insuperable barrera de libertad de expresión que incluya tanto expresiones dañinas como constructivas–¹¹⁷.

116. En este sentido, deberían revisarse las normas existentes en los distintos países sobre ejecución de sentencias extranjeras a fin de determinar si las reglas existentes son suficientes para impedir la ejecución. Le agradezco a Julio Rivera (H) el haberme realizado esta sugerencia.

117. Zittrain, Jonathan, *supra* nota 111, p. 14.

Desarrollando políticas de Internet en Latinoamérica: una perspectiva global

Cynthia M. Wong, James X. Dempsey, y Ellery Roberts Biddle¹

Introducción

Los capítulos de este libro describen algunas de las cuestiones prioritarias acerca de políticas en torno a Internet a las que se están enfrentando en la actualidad algunos países en todo el mundo.

Como reconocen los autores de este libro, la naturaleza abierta y descentralizada de Internet otorga a las personas la posibilidad de buscar, recibir y compartir información e ideas a una escala sin precedentes. Internet puede ser una plataforma poderosa para la innovación, el acceso al conocimiento, la participación ciudadana y el crecimiento económico.

Sin embargo, estas características de apertura y libertad de Internet no están determinadas por la tecnología misma. Internet se ha desarrollado de una manera tan rápida e innovadora como consecuencia de decisiones muy específicas tomadas por personas a cargo de la elaboración de políticas públicas y por la industria de la tecnología, quienes crearon un marco basado en los principios de acceso abierto, competencia, innovación y derechos humanos.

1. Los autores pertenecen al Centro para la Democracia y la Tecnología (Center for Democracy & Technology-CDT), una organización no gubernamental con sede en Washington D.C., que se dedica a mantener una Internet abierta, innovadora y libre. Agradecemos a Eduardo Bertoni por la oportunidad de contribuir a este libro.

Ahora, no obstante, este marco político está siendo desafiado. Los Gobiernos de América Latina, al igual que otros en distintas partes del mundo, están buscando prevenir el crimen, el terrorismo y las violaciones a la *ciberseguridad*. Buscan proteger a los menores de edad, resguardar el honor y la privacidad y promover el cumplimiento de las obligaciones exigidas por el derecho de autor en relación con la actividad en línea. Al trabajar sobre estos desafíos, los legisladores de los países de América Latina se enfrentan a preguntas fundamentales: ¿qué tipo de Internet quieren que tenga su país? ¿cómo puede el Gobierno proteger los derechos humanos y a la vez responder a las preocupaciones legítimas sobre políticas? ¿qué rol deben tener los intermediarios –proveedores de servicios de Internet (ISPs), buscadores y otros intermediarios en lograr estas metas?

En este capítulo, intentaremos contextualizar las políticas de Internet en América Latina dentro del debate global sobre la libertad en Internet y la regulación de Internet en el siglo veintiuno.

I. Construyendo un marco de políticas para Internet basado en los derechos humanos

Internet tiene ciertas características fundamentales que la distinguen de las tecnologías de la comunicación anteriores: a un alcance sin precedentes, es global, abundante y (relativamente) poco costosa. Internet puede ser usada por una cantidad ilimitada de usuarios, y las barreras de entrada son relativamente bajas. La red no necesita ni editores ni guardianes para funcionar. De hecho, el diseño de Internet pone el poder en manos de sus usuarios. Cada usuario puede publicar contenido y controlar el contenido al que accede².

El objetivo de preservar estas características debe guiar el desarrollo de las políticas de Internet. Además, estas características esenciales –apertura, control por parte del usuario y accesibilidad– se vinculan directamente con principios de los derechos humanos. El derecho a la libertad de expresión

2. Dempsey, James X., «The Internet at Risk: The Need for Higher Education Advocacy», en *EDUCAUSE Review*, 42-6 (2007). Disponible [en línea] en: <<http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume42/TheInternetatRiskTheNeedforHig/162066>>. [Nota del editor: consultada el 7/11/11.]

no solo sirve a los intereses democráticos, sino que también promueve la innovación. El derecho a la privacidad no solo es fundamental para la autonomía y el desarrollo personal, sino que también es necesario para el crecimiento del comercio electrónico. Tanto en las esferas nacionales como internacionales, un enfoque hacia las políticas de Internet basada en principios de derechos humanos generará un marco legal y regulatorio que maximizará el potencial social y económico de Internet.

De esta manera, los legisladores y miembros de la sociedad que influyen sobre las políticas públicas deben prestar especial atención a las herramientas internacionales y regionales de derechos humanos –la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos– como guías en este proceso. La Corte Interamericana y otras instituciones regionales e internacionales de derechos humanos pueden ser fuentes importantes en estos esfuerzos, junto con los procesos nacionales.

El artículo 19 de la Declaración Universal dice que todo individuo tiene el derecho «de investigar y recibir informaciones y opiniones y el de difundirlas sin limitación de fronteras». En términos similares, el artículo 13 de la Convención Americana protege el derecho a «buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección».

Estas palabras parecen tener una relevancia particular en el caso de Internet. El concepto del derecho a «difundir» la información y las ideas alcanza un nuevo significado en la era de la web 2.0, donde las entidades en línea, que van desde las redes sociales hasta las plataformas de *blogging*, son el soporte de contenidos que los usuarios generan sin costos y permiten que cualquier persona con una conexión de Internet difunda ideas, opiniones y expresiones culturales. De manera similar, los derechos de «buscar» y «recibir» la información parecen anticipar la existencia de buscadores, servicios de *microblogging* –como Twitter– y otros servicios de Internet. Cuando la censura de Internet en un país afecta los derechos a «difundir» o «recibir» información de personas en otros países, la deferencia que tradicionalmente se da a las leyes y normas nacionales podría tener que ser reconsiderada. La Convención Americana tiene provisiones que van más allá de la Declaración Universal al prohibir las restricciones al derecho a la libre expresión «por vías o medios indirectos, tales como el abuso de controles oficiales... o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones».

Sin embargo, los instrumentos internacionales de derechos humanos también reconocen que es permisible restringir la libertad de expresión para cumplir con otros intereses legítimos, incluyendo el respeto al honor de una persona. Los capítulos de este libro explorarán las tensiones entre la libertad de expresión y otros derechos e intereses.

Las características únicas de Internet son relevantes para reconciliar estas tensiones y desarrollar soluciones equilibradas para los problemas de políticas en el ámbito en línea. Las instituciones de derechos humanos han dejado en claro que, para evaluar cualquier política gubernamental que afecte la libertad de expresión, hace falta considerar el medio de comunicación que esté involucrado. Una regulación que sería adecuada para la televisión *broadcast*, donde el espectro es limitado, quizás no sea adecuada para el servicio de televisión por cable, y tal vez lo sea mucho menos para Internet. Algunos tribunales han decidido que la capacidad que tienen los usuarios de circunvalar ciertas restricciones hace más difícil justificar estas restricciones. De manera parecida, la vasta disponibilidad de herramientas de filtrado controladas por los usuarios –para padres y escuelas– provoca que el filtrado hecho por los proveedores de servicios de Internet (ISPs) por requerimiento gubernamental resulte menos necesario y menos justificable como política para proteger a los niños de contenidos dañinos en línea.

De manera similar, dada la capacidad casi ilimitada de Internet de hospedar puntos de vista opuestos, puede ser que haya menos necesidad de una intervención gubernamental para asegurar la imparcialidad o equilibrio o para proteger la reputación. Los errores pueden ser corregidos y el derecho a réplica puede ser efectuado instantáneamente.

Como muestran los capítulos de este libro, al entender las características únicas de Internet y basar nuestro trabajo en principios de los derechos humanos, podemos abordar las preguntas difíciles sobre el desarrollo de políticas para la era digital.

II. Comentarios sobre los capítulos

II.A. Responsabilidad de los intermediarios

Todos los días, millones de periodistas, profesores, alumnos, gente de negocios, científicos, autoridades gubernamentales, políticos y ciudadanos comunes usan Internet para expresarse, acceder a la información, y participar en una cantidad incontable de aspectos de la vida pública y privada. Toda

esta actividad expresiva, social, política y económica es posible porque los proveedores de servicios de Internet (ISPs), empresas de telecomunicaciones, páginas web, servicios en línea y varios otros intermediarios tecnológicos sirven como conductos y plataformas para la expresión y la comunicación. En los últimos diez años, estos servicios han sido innovados, se han expandido rápidamente y han posibilitado usos nuevos. Un ejemplo de esto es el desarrollo extraordinario de plataformas que alojan contenidos creados por usuarios. Muchos de estos servicios son gratuitos para el usuario, lo que conlleva una expansión masiva de oportunidades para la expresión y el comercio.

Muy temprano en la historia de Internet, surgió una pregunta clave: ¿deben los intermediarios ser responsables por contenidos dañinos o ilegales creados o subidos por sus usuarios? Observando marcos nacionales y regionales, se advierte una tendencia general: aquellos Gobiernos que han buscado maximizar el crecimiento de Internet y los servicios en línea han tendido a limitar la responsabilidad civil y penal de los intermediarios de Internet. En contraste, en los países donde más se restringe Internet, los Gobiernos frecuentemente responsabilizan a los intermediarios por los contenidos ilegales subidos por usuarios o les imponen deberes de vigilar las expresiones de los usuarios. Esta práctica obliga a los intermediarios a actuar como guardianes de la red. La imposición de responsabilidad a intermediarios no solo reduce el espacio para la libre expresión, sino que también obstaculiza la innovación y limita la expansión del acceso a Internet³.

Como explican Claudio Ruiz y Juan Lara, muchos de los países sobre los cuales se concentra su artículo no tienen marcos legislativos claros para la determinación de la responsabilidad de los intermediarios por contenidos ilegales creados o subidos por usuarios, en especial fuera de la esfera de las violaciones de los derechos de autor. Los tribunales han producido una jurisprudencia turbia, que proporciona poca ayuda para las empresas que quieren ofrecer sus servicios en América Latina. Esta jurisprudencia tampoco es efectiva como guía para los ciudadanos sobre cómo sus actos de

3. CDT, «Intermediary Liability: Protecting Internet Platforms for Expression and Innovation», de abril de 2010. Disponible [en línea] en: <http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf>. [Nota del editor: consultada el 7/11/11.]

expresión (y su intimidad personal) serán protegidos en línea. Los principios articulados por Ruiz y Lara pueden ofrecer una guía para el desarrollo de políticas sobre este tema en América Latina.

Las leyes que tratan sobre la responsabilidad de los intermediarios en los Estados Unidos y la Unión Europea (UE) merecen ser destacadas. Dos leyes independientes conforman la política estadounidense sobre la responsabilidad de los intermediarios: la Sección 230 de la Ley de Comunicaciones (*Communications Act*) y la Sección 512 de la Ley de Derechos de Autor (*Copyright Act*)⁴. La Sección 230 de la Ley de Comunicaciones estipula que los intermediarios de Internet no pueden ser responsables por los contenidos creados, transmitidos o subidos por sus usuarios. La protección contra la responsabilidad se aplica sin condiciones a una variedad de acciones (con las excepciones de demandas de derechos de autor y de derecho penal federal).

Con respecto a los derechos de autor, la Sección 512 protege a ciertos proveedores de servicios si quitan los contenidos que constituyen violaciones de derechos de autor en respuesta a una notificación privada hecha por el titular del derecho. Esta práctica se conoce como «notificación y retirada» (*«notice and takedown safe harbor»*).

La UE también proporciona protecciones significativas contra la responsabilidad bajo su Directiva sobre el Comercio Electrónico (*E-Commerce Directive*)⁵. Las reglas de la UE distinguen entre los conductores (como los proveedores de servicios de Internet ISPs), servicios de almacenamiento y los intermediarios que alojan contenidos de terceros. Los intermediarios que ofrecen alojamiento tienen que cumplir con un sistema de *notificación y retirada* para protegerse contra la responsabilidad legal. Este sistema no solo se aplica a las demandas por violaciones de derechos de autor, sino a cualquier tipo de contenido.

En nuestra opinión, estas protecciones legales han sido tan importantes para la libertad de expresión en línea como las protecciones constitucionales y las de derechos humanos. Estas han posibilitado el crecimiento

4. 47 u.s.c. § 230, véase [en línea] en: <<http://www.law.cornell.edu/uscode/47/230.html>> y 17 u.s.c. 512, también disponible [en línea] en: <<http://www.law.cornell.edu/uscode/17/512.html>>. [Nota del editor: ambas fueron consultadas el 7/11/11.]

5. Directiva sobre el comercio electrónico, 2000/31/EC, disponible en inglés [en línea] en: <http://ec.europa.eu/internal_market/e-commerce/index_en.htm> y OpenNet Initiative, Europe-Regional Overview, de 2009, también disponible [en línea] en: <<http://opennet.net/research/regions/europe>>. [Nota del editor: ambas fueron consultadas el 7/11/11.]

extraordinario de los servicios de redes sociales y otros sitios interactivos que alojan contenidos creados por usuarios. Sin estas garantías legales, el costo de desarrollar nuevos servicios y aplicaciones sería mucho más alto, y la innovación y las oportunidades para la expresión individual se verían limitadas.

Para promover la innovación y el crecimiento de las industrias domésticas de Internet y proteger los derechos fundamentales, los Gobiernos de América Latina deben adoptar leyes que eximan a los intermediarios de responsabilidad por el comportamiento ilegal de sus usuarios. Si los intermediarios tuvieran que cumplir con ciertos deberes para acceder a esta protección legal, estos últimos deberían estar bien definidos y tener en cuenta el rol y las funciones técnicas de cada tipo de intermediario.

Ruiz y Lara muestran cómo los sistemas de «*notificación y retirada*» pueden ser vulnerables al abuso, especialmente si la obligación de bajar los contenidos puede activarse por la mera expedición de una notificación y sin una determinación judicial sobre la ilegalidad del contenido. Esto permitiría que un funcionario gubernamental, una empresa o un individuo silenciaran la expresión de otra persona mediante la mera expedición de una notificación de retirada. En Chile, la Ley de Derechos de Autor⁶ exige que la notificación del contenido violatorio tenga la forma de una orden judicial. Esta es una protección importante contra el abuso, ya que coloca la decisión de si el contenido viola los derechos de autor en manos del sistema judicial, en vez de obligar a los intermediarios a hacer determinaciones que no están habilitados para hacer.

Por supuesto que, como notan los autores en el apartado sobre la Argentina, la eficacia de este método para preservar la libertad de expresión depende de la calidad del proceso judicial que genera las órdenes de retirada. Este proceso debe incluir ciertos aspectos claves: el usuario que subió el contenido tiene que recibir una notificación del hecho; el Tribunal debe considerar la demanda de una manera justa, y el tribunal tiene que dar al usuario la oportunidad de recurrir la decisión. Bajo la ley de derechos de autor de los Estados Unidos, los intermediarios que ofrecen servicios de alojamiento y que buscan obtener la protección de responsabilidad eliminan

6. Bajo esta ley, 'notificación' (*notice*) indica cómo el servicio adquiere «conocimiento efectivo», lo que activa la obligación de remover contenido.

contenidos cuando reciben una notificación por parte del titular del derecho de autor. Sin embargo, la ley estipula que la persona que subió el contenido cuestionado puede alegar que la notificación de una violación fue en error, en cuyo caso, el intermediario puede volver a subir el contenido sin correr el riesgo de tener responsabilidad legal⁷. Los países de la UE también pueden incluir protecciones parecidas en sus legislaciones nacionales.

Por otro lado, hace falta que este proceso pueda adecuarse a la velocidad y al volumen de violaciones de *copyright* en línea. Al igual que ocurre en otros contextos, mirar las políticas de la responsabilidad de los intermediarios desde la perspectiva de los derechos humanos puede ayudar al proceso de construcción de políticas coherentes que protejan los derechos fundamentales y promueven el crecimiento de las tecnologías de la información y la comunicación. Como dicen Ruiz y Lara, cualquier ley que imponga responsabilidad de intermediarios tiene que ser evaluada bajo los estándares de necesidad y proporcionalidad, así como por su impacto sobre la libertad de expresión y la innovación.

Para ciertos tipos de expresión y actividades ilegales, el método de *notificación y retirada* puede no ser adecuado, especialmente en los casos en los cuales la notificación se efectúe sin intervención judicial. Por ejemplo, los intermediarios no están bien preparados para determinar si cierto contenido es difamatorio. Imagine un caso en el que un *bloguero* escribe un comentario en el que sostiene que un funcionario del Gobierno local ha malversado dinero de la hacienda pública de la ciudad. Si la imputación es cierta, el *bloguero* está cumpliendo una función pública sumamente importante al llamar la atención sobre un incidente de corrupción local. Pero si la imputación es falsa, el comentario puede ser difamatorio. Sin embargo, cuando la compañía que aloja el blog recibe una notificación de retirada, no tiene forma de determinar la veracidad del comentario. El proceso de determinar si una expresión es difamatoria resulta muy difícil porque los casos de difamación, por su naturaleza, requieren de pruebas y análisis. Los intermediarios no tienen la capacidad de tomar este tipo de decisiones y no se les debe permitir remover contenidos sin una autorización judicial.

7. La notificación de la violación podría ser errónea, porque, por ejemplo, el uso del contenido ocurrió bajo el principio de «uso legítimo» (*fair use*), una doctrina bajo el derecho de los Estados Unidos que permite el uso limitado de obras protegidas por el derecho de autor sin el permiso del titular del derecho.

Queremos hacer una advertencia con respecto a una sugerencia de Ruiz y Lara. Los autores recomiendan que los proveedores de servicios de Internet (ISPs) mantengan registros de sus usuarios con el fin de facilitar el proceso para contactar a un usuario si ocurre una infracción ilegal. El anonimato en línea es un punto controversial, pero la expresión anónima es un aspecto importante de la libertad de expresión. Es especialmente importante en relación con los asuntos de interés público, dado que en estos casos es más probable que las personas eviten expresarse si temen ser identificadas.

En los Estados Unidos, la Corte Suprema ha ratificado el derecho a la expresión anónima⁸. Los instrumentos internacionales de derechos humanos también recomiendan que las leyes nacionales preserven las oportunidades para la expresión anónima⁹. En locutorios, cibercafés y lugares desde donde se puede acceder al wifi, la obligación de identificar al cliente podría desalentar a algunos usuarios a usar Internet. Además, el trabajo de recopilar los nombres de todos los clientes sería costoso y podría encarecer el acceso a Internet. Una obligación de este tipo podría dar incentivos a estos proveedores para dejar de ofrecer el servicio, lo que resultaría en una restricción al acceso a Internet.

Como dicen Ruiz y Lara, obligar a los proveedores a recopilar y retener datos sobre la actividad en línea de sus usuarios merece una mayor discusión.

8. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). «Las protecciones a las expresiones anónimas son fundamentales para el discurso democrático. Permitir a los que disienten mantener el anonimato les da la libertad de expresar opiniones críticas o minoritarias. El anonimato es una protección ante la tiranía de la mayoría. Así, ejemplifica el propósito detrás de la Carta de Derechos, y de la Primera Enmienda en especial: proteger a los individuos impopulares de represalias». [Nota del editor: la traducción es propia.] A continuación, se transcribe la cita en su idioma original:

Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views ... Anonymity is a shield from the tyranny of the majority... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation ... at the hand of an intolerant society.

9. Relatoría para la libertad de expresión - Comisión Interamericana de Derechos Humanos, «Mecanismos internacionales para la Promoción de la Libertad de Expresión», en la Declaración Conjunta del Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, el Representante de la Organización para la Seguridad y Cooperación en Europa para la Libertad de los Medios de Comunicación y el Relator Especial de la OEA para la Libertad de Expresión del 21 de diciembre de 2005, disponible [en línea] en: <<http://www.cidh.org/relatoria/showarticle.asp?artID=650&IID=2>>. [Nota del editor: consultada el 7/11/11.]

En nuestra organización (CDT), creemos que los mandatos de retención de esta naturaleza frecuentemente son desproporcionados, porque tales obligaciones implican interferir en la privacidad de todos los usuarios de un servicio para investigar las actividades ilegales de unos pocos usuarios. Como mencionamos más adelante, una alternativa es requerir la «conservación» (*preservation*) de los datos, un proceso enfocado en los usuarios que han sido demandados o que se encuentran bajo investigación policial.

El derecho estadounidense da otra protección importante a los intermediarios. Bajo la Sección 230, estos últimos no solamente quedan protegidos de responsabilidad cuando alojan contenidos creados por usuarios, sino que también están exentos de responsabilidad cuando remueven contenidos creados por usuarios o cuando deshabilitan actividades de usuarios que consideran inapropiadas. Esta protección incluye, por ejemplo, los esfuerzos de *antispam* y ciberseguridad de los proveedores de servicios de Internet (ISPs). Así, la ley les permite bloquear contenidos que parecen ser *spam* o contener código dañino, siempre y cuando actúen de buena fe. Esta política también autoriza a los servicios de medios de comunicación sociales a remover material sexualmente explícito, violento o dañino y a escribir y hacer cumplir sus propias condiciones de servicio. La libertad de bajar contenidos o excluir a los usuarios es algo que los proveedores tienen que tomar en serio y que tienen que practicar con transparencia y coherencia¹⁰. Además, los proveedores tienen que resistir la presión del Gobierno de convertir estándares voluntarios en políticas obligatorias.

II.B. La privacidad y la protección de datos

La protección de datos es uno de los componentes claves dentro del desarrollo de Internet y del comercio electrónico, porque permite a los usuarios confiar en que sus datos personales serán protegidos cuando hacen transacciones en línea. En su capítulo, Lorenzo Villegas apunta algunas

10. Newland, Erica, Caroline Nolan, Cynthia Wong y Jillian York, «Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users», de septiembre de 2011; disponible [en línea] en: <http://www.cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content Removal.pdf>. [Nota del editor: consultada el 7/11/11.]

de las distinciones necesarias para entender este tema e identifica algunas tensiones contemporáneas en relación con el derecho a la privacidad.

El derecho a la privacidad tiene tres aspectos centrales: en primer lugar, está el derecho a la intimidad o a la protección de datos que se da entre una compañía y sus clientes. En los Estados Unidos, este aspecto de la privacidad se conoce como «privacidad de consumidor» (*consumer privacy*). En segundo lugar, está el derecho a la privacidad que tiene el ciudadano en relación con el Gobierno cuando este último actúa en sus capacidades administrativa y social. Este aspecto de la privacidad tiene que ver con los datos personales que recopila el Gobierno de sus ciudadanos mediante la provisión de educación pública, salud y otros servicios sociales, la administración de los impuestos estatales y otras funciones. El tercer aspecto tiene que ver con el derecho a ser protegido contra la recolección coercitiva de datos por el Gobierno como parte de investigaciones penales o investigaciones relacionadas con la seguridad nacional.

En relación con el primer aspecto de la intimidad, los principios de la protección de datos dentro del contexto del derecho de los consumidores fueron articulados en 1980 cuando la Organización para la Cooperación y Desarrollo Económico (OCDE) estableció una serie de pautas de privacidad (*privacy guidelines*) que contenían definiciones, ocho principios de la privacidad y métodos de aplicación¹¹. Los ocho principios de la OCDE frecuentemente son llamados los Principios de Práctica Justa con la Información (*Fair Information Practice Principles - FIPPS* o *FIPS*). Las pautas de la OCDE y los FIPS han tenido un fuerte impacto global y han sido adoptados en una variedad de medidas legislativas y regulatorias.

En 1995, la UE acogió su directiva para la protección de los datos, que estuvo basada en los FIPS de la OCDE. La directiva estableció una estructura regulatoria detallada para ser adoptada por los miembros de la UE en sus legislaciones nacionales¹². Como nota Villegas, la directiva de la UE tuvo

11. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), disponibles en inglés [en línea] en: http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html. [Nota del editor: consultada el 7/11/11.]

12. Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, véase [en línea] en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML>. [Nota del editor: consultada el 7/11/11.]

influencia en América Latina, especialmente en la Argentina. Los Estados Unidos no han adoptado los FIPS en su totalidad, pero cuentan con una serie de leyes de protección de datos dirigidos a sectores específicos –una para la información financiera, otra para los archivos de información de salud, otra para datos de telecomunicaciones, etcétera– que incorporan los FIPS parcialmente y dejan ciertas esferas sin regulación. Sin embargo, la Comisión Federal de Comercio de los Estados Unidos (*us Federal Trade Commission*) ha reconocido a los FIPS como el mejor marco para la privacidad del consumidor¹³, y la administración Obama ha propuesto la adopción de una legislación federal completa sobre privacidad¹⁴.

El marco de privacidad adoptado en noviembre de 2004 por los veintiún miembros del Foro de Cooperación Económica Asia-Pacífico (por sus siglas en inglés, APEC) también es relevante para América Latina¹⁵. Muy recientemente, el APEC ha tocado el tema que Villegas identifica como uno de los más complejos: la aplicación de leyes nacionales divergentes para los datos en tránsito internacional. En septiembre de 2011, el Grupo Dirigente de Comercio Electrónico (*Electronic Commerce Steering Group*) del APEC aprobó la iniciativa de las Reglas de Privacidad Transfronterizas (*Cross Border Privacy Rules* o *CBPR*) en un esfuerzo por facilitar el tránsito de los datos y asegurar, a la vez, un nivel significativo de privacidad dentro de la región. El sistema de las CBPR busca establecer un equilibrio entre los valores de privacidad, comercio y soberanía nacional¹⁶.

13. Comisión Federal de Comercio (Federal Trade Commission) de los Estados Unidos, *Bureau of Consumer Protection, A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* del 1º de diciembre de 2010, puede verse [en línea] en: <<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>>. [Nota del editor: consultada el 7/11/11.]

14. Departamento de Comercio (Department of Commerce) de los Estados Unidos, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, de diciembre de 2010, puede verse [en línea] en <http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf>. [Nota del editor: consultada el 7/11/11.]

15. *Marco de Privacidad de la APEC* (APEC Privacy Framework), 2005, disponible en inglés [en línea] en: <http://publications.apec.org/publication-detail.php?pub_id=390>. [Nota del editor: consultada el 7/11/11.]

16. Brookman, Justin, «Can Cross-Border Privacy Rules Trump Divergent Data Protection Laws» en el CDT, el 4 de octubre de 2011, disponible [en línea] en: <<http://www.cdt.org/blogs/justin-brookman/410can-%E2%80%9Ccross-border-privacy-rules%E2%80%9D-trump-divergent-data-protection-laws>>. [Nota del editor: consultada el 7/11/11.]

Las reglas para el segundo aspecto de la privacidad, que tiene que ver con la relación entre el ciudadano y el Gobierno en sus capacidades administrativas, también están basadas en los FIPS. La Directiva Europea es aplicable tanto a entidades comerciales como a entidades gubernamentales (aunque excluye operaciones gubernativas que tienen que ver con la seguridad pública, defensa, seguridad del Estado y la justicia penal). En relación con este aspecto de la privacidad, los Estados Unidos estuvieron un paso más adelante que Europa. El Congreso de los Estados Unidos adoptó la Ley de Privacidad (*Privacy Act*) en 1974, aplicando muchos de los FIPS a los archivos estatales recopilados y mantenidos por el Gobierno federal en su capacidad administrativa. La Ley de Privacidad de los Estados Unidos no excluye completamente los archivos de la policía y de seguridad nacional, pero estos archivos están exentos de muchas de las provisiones de la ley.

Finalmente, el tercer aspecto de la privacidad tiene que ver con el poder del Gobierno de interferir por la fuerza en la vida privada, incluyendo el hogar y la confidencialidad de las comunicaciones. En los Estados Unidos, este aspecto de la privacidad está protegido por la Constitución Federal. La cuarta enmienda protege al público del registro e incautación arbitrarios (*unreasonable search and seizure*).

En América Latina, los tres aspectos de la privacidad tienen sus raíces en el Artículo 11 de la Convención Americana, así como, también, en la mayoría de las Constituciones nacionales, que incluyen el derecho tradicional de *habeas data*. Sin embargo, probablemente es acertado decir que no existe un país en América (incluyendo a los Estados Unidos) que tenga un marco legal que proteja completamente el derecho a la privacidad en los tres aspectos. Y para complicar el escenario, como indica Villegas, Internet introduce nuevas preocupaciones. También hace surgir tensiones entre derechos. Es necesario evitar que el derecho a la privacidad sea utilizado para socavar otros principios democráticos.

Por ejemplo, Internet tiene un enorme potencial para aumentar la transparencia y la rendición de cuentas por parte del Gobierno al posibilitar que la información gubernamental esté disponible en línea. Sin embargo, a la vez, hace falta tener cuidado en la medida en que la información se refiera a individuos. Considere, por ejemplo, los archivos judiciales. En la era predigital, muchos de estos datos, como presentaciones judiciales y otros documentos introducidos en los procedimientos *tribunales*, técnicamente eran públicos. Pero aún siendo públicos, era difícil acceder a esta información. Hoy en día, a medida que los tribunales transfieren sus archivos a la red, esta información es mucho más fácil de buscar. La Corte

Suprema de los Estados Unidos ha dicho que «hay una diferencia amplia entre los archivos públicos que se pueden encontrar a partir de una búsqueda diligente de los archivos de los tribunales, del condado y de estaciones de policía locales en todo el país y el resumen computarizado alojado en un solo lugar de información»¹⁷.

Las dependencias gubernamentales no deben usar la privacidad como una excusa para evitar la transparencia. Estas deben ser cuidadosas en el trabajo de digitalizar y hacer accesible a través de Internet los archivos de los tribunales, además de asegurarse de que la información privada (como información financiera o de salud personal) sea protegida¹⁸.

Villegas plantea una pregunta, tal vez la más fundamental en torno a la privacidad: ¿qué datos deben ser protegidos? En los Estados Unidos y Europa, esta pregunta es planteada con frecuencia en relación con la pregunta de qué información es «personalmente identificativa» (*Personally Identifiable Information, pii*). La pregunta de cómo clasificar las direcciones IP, que también plantea Villegas, es un punto controversial. En los Estados Unidos, las direcciones IP no están clasificadas como información personalmente identificativa, mientras que en Europa, el Grupo de Trabajo del Artículo 29 sobre Protección de Datos (*Article 29 Working Party*) consideró que sí lo son¹⁹. Es importante reconocer que los cambios en la tecnología están haciendo que la distinción entre la información personalmente identificativa y la que no lo es sea menos pertinente, porque cada vez es más posible reidentificar datos que son supuestamente anónimos²⁰. La Comisión Federal

17. Nota del editor: la traducción es de los autores. A continuación citamos el texto original:

[T]here is a vast difference between the public records that might be found after diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989). Puede consultarse [en línea] en: <<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=489&invol=749>>. [Nota del editor: consultada el 7/11/11.]

18. CDT, «A Quiet Revolution in the Courts: Electronic Access to State Court Records, A CDT Survey of State Activity and Comments on Privacy, Cost, Equity and Accountability», de agosto de 2002, disponible [en línea] en: <<http://cdt.org/publications/020821courtrecords.shtml>>. [Nota del editor: consultada el 7/11/11.]

19. Véase [en línea]: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>. [Nota del editor: consultada el 7/11/11.]

20. CDT, «Encouraging the Use of, and Rethinking Protections for De-Identified (and “Anonymized”) Health Data», de junio de 2009, disponible [en línea] en: <http://cdt.org/healthprivacy/20090625_deidentify.pdf>. [Nota del editor: consultada el 7/11/11.]

de Comercio de los Estados Unidos (*us Federal Trade Commission* o *FTC*) ha advertido a las compañías que no deben confiar en concepciones desactualizadas de lo que es o no información personalmente identificativa. La *FTC* también ha sugerido que quizás extenderá su competencia para incluir los datos anteriormente considerados como información que no es personalmente identificativa²¹.

La cuestión de la responsabilidad de los intermediarios también aparece en el contexto de la privacidad. La tendencia de responsabilizar a los intermediarios (como los servicios de búsqueda y alojamiento) por las violaciones a la privacidad instigadas por otros es peligrosa y amenaza la apertura de Internet²².

Villegas analiza la polémica reciente sobre la retención de datos, a la que hicimos referencia brevemente con anterioridad. Como es conocido, los proveedores de servicios de telecomunicaciones e Internet recopilan y almacenan gran cantidad de datos sobre sus clientes. En años recientes, sin embargo, algunos Gobiernos se han mostrado insatisfechos con la cantidad de información que los proveedores de servicios recopilan y retienen en el ejercicio de sus negocios. Estos Estados han impuesto o han considerado imponer requerimientos legales que exigen a los proveedores retener ciertos datos de todos sus usuarios por un plazo determinado, aun cuando no sean necesarios para los fines de sus negocios. En general, bajo estos requerimientos, los datos tienen que ser recopilados y almacenados de forma tal que quedan ligados a los nombres u otra información identificativa de los usuarios. Por otra parte, los funcionarios estatales pueden requerir el acceso a esos datos en virtud de las legislaciones de sus países para fines de investigaciones penales y a menudo, también, para investigaciones sobre seguridad nacional. Las leyes que requieren que las compañías de tecnologías de información y comunicaciones almacenen datos sobre sus usuarios típicamente se conocen como «leyes de retención de datos» (*data retention laws*)²³.

21. Véase Comisión Federal de Comercio (Federal Trade Commission) de los Estados Unidos, *supra* nota 13.

22. Véase *CDT*, *supra* nota 3.

23. *CDT*, «Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development», de octubre de 2011, disponible [en línea] en: <http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf>. [Nota del editor: consultada el 7/11/11.]

Al crear archivos que enlazan descripciones muy detalladas de las actividades de usuarios en Internet con información personalmente identificativa, la retención de datos viola no solo el derecho a la intimidad, sino, también, el derecho a la libertad de expresión y el derecho a la presunción de inocencia. Dar cumplimiento con los requerimientos de retención de datos acarrea costos altísimos para las compañías e impone riesgos significativos para la privacidad y la seguridad. Existe el riesgo de abusos por parte de los Gobiernos en relación con los datos compilados, aun si desarrollan estas políticas para cumplir con metas legítimas. Estos datos también son vulnerables al robo de identidad.

El Convenio sobre Cibercriminalidad del Consejo de Europa²⁴ toma otra perspectiva. Los países que firman el Convenio deben adoptar leyes que autoricen a los funcionarios gubernamentales a requerir a los proveedores de servicios de comunicación que empiecen, después de recibir el requerimiento, a guardar datos específicos pertenecientes a un usuario o dispositivo relevantes para una investigación o proceso penal. En general, se exige al proveedor conservar estos datos por un plazo máximo, por ejemplo de noventa días, mientras los agentes gubernamentales obtienen la autorización necesaria para exigir que sean revelados. Este proceso es conocido como «conservación de datos» y ofrece un método para satisfacer muchas necesidades del Gobierno que es preferible a la retención de datos.

II.C. Filtrado

En su artículo, Varon, Affonso, Magrani y Britto exponen cómo el filtrado puede tener un impacto significativo sobre la libertad de expresión. Cualquier propuesta de filtrado en Internet debe ser evaluada bajo los criterios de derechos humanos de necesidad, efectividad, proporcionalidad y alternativas menos restrictivas. Para evaluar un sistema de filtrado, se deben considerar cuatro preguntas clave:

- a) ¿en qué punto en la red ocurre el filtrado?;
- b) ¿qué tipo de contenido está siendo filtrado?;

24. Consejo de Europa: Convenio sobre cibercriminalidad, 16 de abril de 2011, disponible [en línea] en: <<http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm>>. [Nota del editor: consultada el 7/11/11.]

- c) ¿es el acto de filtrado voluntario o está siendo llevado a cabo bajo un requerimiento gubernamental?; y
- d) ¿cuál es el contexto más amplio respecto al acceso y posibilidad de elección de servicios por parte del usuario?

Además, al evaluar propuestas de filtrado, los legisladores y los defensores de la red abierta tienen que considerar los métodos particulares de filtrado y los riesgos que pueden traer. Demasiado a menudo, en los debates sobre contenidos en Internet, los proponentes del filtrado se concentran únicamente en cómo el filtrado serviría a un determinado interés social. Suponen que el filtrado propuesto funcionaría perfectamente y que solo afectaría a los contenidos ilegales, sin pensar en los posibles daños colaterales que los mecanismos de filtrado pueden causar sobre contenidos legales²⁵. Como sugieren los autores, los objetivos del filtrado pueden ser legítimos, pero hace falta que los legisladores tengan en cuenta los posibles efectos negativos sobre contenidos legales.

Como explican Varon y sus colegas, el filtrado puede ocurrir en todos los puntos de la red, en las aplicaciones en línea, en el sistema de nombres de dominio, en los enrutadores de los proveedores de servicios de Internet (ISPs) y en la computadora del usuario final²⁶. Identificar el punto en la red

25. Existe mucha evidencia de que el filtrado es, con frecuencia, excesivamente amplio. Véanse *Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004), en el que se nota la amplitud excesiva del filtrado de direcciones de IP y nombres de dominio; Claburn, Thomas, «ICE Confirms Inadvertent Web Site Seizures», en *Information Week*, 18 de febrero de 2011; disponible [en línea] en: <http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959&cid=RSSfeed_IWK_All>, en el que se describe un caso de bloqueo no intencional en una acción policial, y Kameney, Marina, «First, China. Next: the Great Firewall of... Australia?», en *Time* del 16 de junio de 2010, disponible [en línea] en: <http://www.time.com/time/world/article/0,8599,1995615,00.html?xid=rss-world&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+time/world+%28TIME:+Top+World+Stories%29>, artículo que menciona que las páginas web de un dentista y de un establecimiento veterinario aparecieron en una lista negra australiana que había sido propuesta para ser la base de un sistema de filtrado obligatorio por parte de los proveedores de servicios de Internet. [Nota del editor: estas últimas fueron consultadas el 7/11/11.]

26. Para más información sobre los aspectos técnicos del filtrado en Internet, véase Zittrain, Jonathan y John Palfrey, «Internet Filtering: The Politics and Mechanisms of Control», en Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MIT Press, 2008; disponible [en línea] en: <<http://opennet.net/accessdenied>>. [Nota del editor: consultada el 7/11/11.]

donde tiene lugar el filtrado es clave para evaluar la proporcionalidad y el impacto de la medida. Mientras que el filtrado por parte de los proveedores de servicios de Internet (ISPs) puede ser preocupante, el realizado por operadores de redes sociales y plataformas de contenidos generados por usuarios plantea consideraciones muy diferentes. Los sitios web tienen la libertad de escribir e implementar sus propias condiciones de servicio y reglas comunitarias que determinarán qué contenido será permitido y qué contenido, no. Considere, por ejemplo, una red social como Facebook u Orkut. Estos sitios establecen condiciones para sus usuarios según las cuales cierto tipo de contenido está prohibido y voluntariamente vigilan sus redes para remover tal contenido. De igual manera, un sitio como YouTube establece reglas sobre qué contenido es aceptable alojar en el sitio²⁷.

La transparencia y el debido proceso legal (*due process*) son sumamente importantes cuando los proveedores de servicios en línea limitan el contenido que se puede subir a sus sitios. Mientras que los operadores de estos sitios tienen la libertad de aceptar o no aceptar ciertos tipos de contenido en sus sitios, los usuarios deben ser informados sobre cómo se tomarán estas decisiones. También debe darse a los usuarios la oportunidad de reclamar contra las decisiones del operador²⁸. En los casos de filtrado automático, los proveedores de servicios deben tener conciencia del riesgo de filtrar contenidos de una manera excesivamente amplia y hacer lo posible para evitar este resultado. En caso de duda, quizá deban optar por admitir el contenido²⁹. En la medida en que estas prácticas sean verdaderamente voluntarias, el proveedor del servicio las ejerce con transparencia e

27. Las normas para la comunidad (Community Guidelines) de YouTube prohíben los contenidos que muestran pornografía, el abuso de animales, el uso de las drogas, el discurso de odio, entre muchas otras cosas, consúltelas [en línea] en: <http://www.youtube.com/t/community_guidelines>. Además, YouTube ha implementado un sistema de filtrado antipiratería (Content ID), que impide subir videos que violan protecciones de derecho de autor, véase [en línea]: <<http://www.youtube.com/t/contentid>>. [Nota del editor: ambas fueron consultadas el 7/11/11.]

28. CDT, «Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users», del 21 de septiembre de 2011, disponible [en línea] en: <http://cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf>. [Nota del editor: consultada el 7/11/11.]

29. Esta medida podría consistir, en el contexto de filtrado por contenido protegido por el derecho de autor, en una política de permitir que pequeños segmentos de trabajos protegidos, los cuales probablemente quedarían comprendidos dentro de las excepciones al derecho de autor, puedan pasar a través del filtro.

imparcialidad y haya espacios alternativos donde los individuos puedan distribuir sus contenidos, estos métodos voluntarios de filtrado o control probablemente no sean objetables. Cualquier restricción que tales decisiones editoriales puedan imponer sobre la libertad de expresión puede ser mitigada, en muchos casos, por la disponibilidad de otras plataformas y servicios en el mercado que tienen políticas distintas.

Los proveedores de servicios de Internet (ISPs) se encuentran en una posición muy diferente. El ISP es el único a través del que pasa todo el contenido; si un proveedor bloquea cierto contenido, los usuarios serán incapaces de acceder a tal contenido por medio de cualquier fuente en línea. Más aún, en muchos países, los usuarios tienen pocas opciones de elegir entre distintos proveedores de servicios de Internet, por lo que el filtrado a nivel de estos proveedores puede dejar al usuario sin un camino alternativo para acceder a la información bloqueada. Además, cuando los proveedores de servicios de Internet (ISPs) se enfrentan a requerimientos estatales de filtrar ciertos contenidos, frecuentemente recurren a la implementación de métodos técnicos de filtrado que son sumamente excesivos —o demasiado invasivos—. Los autores comentan sobre el fallo revocado de Daniela Cicarelli en Brasil, que había ordenado que los ISPs bloquearan YouTube en respuesta a un reclamo por un solo video. Este caso demuestra cómo el filtrado por parte de los proveedores de servicios de Internet puede afectar mucha más expresión de la deseada³⁰. Para ellos, el nivel de inspección de tráfico necesario para bloquear sitios o contenidos específicos implicaría un alto nivel de intrusión a la privacidad y podría afectar negativamente el funcionamiento de la red. Estos riesgos no se dan, sin embargo, cuando los proveedores de servicios de Internet (ISPs) ofrecen herramientas de filtrado que son verdaderamente controladas por el usuario, como, por ejemplo, los programas para padres que permiten al usuario final restringir el contenido al cual pueden acceder.

La posición única en la que se encuentran los proveedores de servicios de Internet (ISPs) es el principal motivo por el cual las reglas de neutralidad de la red de los Estados Unidos solo son aplicables a los proveedores de servicios de Internet (ISPs) y no a las redes sociales, los buscadores o los servicios que alojan contenidos creados por usuarios como YouTube. Dada la posición única en la que se encuentran los proveedores de servicios de

30. Véase *Center for Democracy & Technology v. Pappert*.

Internet, es apropiado imponerles reglas para evitar su comportamiento arbitrario o anticompetitivo con respecto al contenido.

En los años recientes, han surgido varias iniciativas para imponer requerimientos de filtrado a través del sistema de nombres de dominio (DNS). Usar el DNS para controlar contenido genera un alto riesgo de suprimir expresión legal y también puede aumentar riesgos de ciberseguridad. También, usar el DNS para tomar acción contra sitios extranjeros generará conflictos intrajurisdiccionales en los que cada país intentará usar el DNS para ejercer jurisdicción doméstica sobre sitios extranjeros³¹.

También es importante considerar la naturaleza del contenido filtrado. Filtrar para proteger la seguridad de la red o para proteger a los usuarios de amenazas a su seguridad puede ser menos dañino para la libertad de expresión que filtrar para responder a intereses de terceros o a políticas culturales más amplias. Por ejemplo, generalmente es permisible que los ISPs filtren *spam*, emails de *phishing* y software malicioso dañino. No obstante, los estándares para el filtrado deben ser transparentes y deben ser aplicados coherentemente, y los ISPs deben contar con un mecanismo de debido proceso legal para aquellos cuyas comunicaciones han sido bloqueadas. Si respetan estos principios, los proveedores de servicios de Internet deberían poder proteger sus servicios y a sus usuarios del *spam*, fraude y de intentos de interferir el servicio.

Como cuestión técnica, también es importante considerar en qué medida cierto contenido puede ser identificado por un filtro. Un filtro puede ser diseñado para reconocer un contenido particular protegido por el derecho de autor, como una canción o una película. Como indican los autores, la tecnología no es capaz de juzgar los varios factores relevantes para la legalidad, pero al menos puede reconocer la naturaleza del contenido. Un sitio como YouTube puede identificar contenido protegido por el derecho de autor mientras está siendo subido³². Sin embargo, en el caso de contenido difamatorio, este método es técnicamente imposible, porque una cantidad infinita de contenido impredecible podría ser difamatorio.

31. CDT, «The Perils of Using the Domain name System to Address Unlawful Internet Content», de septiembre de 2011, disponible [en línea] en: <<http://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf>>. [Nota del editor: consultada el 7/11/11.]

32. Véanse <<http://www.youtube.com/t/contentid>> y Mills, Elinor, «Google unveils YouTube antipiracy tool», del 15 de octubre de 2007, disponible [en línea] en: <http://news.cnet.com/8301-10784_3-9797622-7.html>. [Nota del editor: ambas fueron consultadas el 7/11/11.]

Un tercer aspecto por considerar es si el filtrado es hecho voluntariamente o si es exigido por el Gobierno. Una obligación legal de filtrar es muy problemática para la libertad de expresión, tanto si es aplicada a los proveedores de servicios de Internet (ISPs) o a los proveedores de servicios en línea. Como notan Varon y sus colegas, los proveedores de servicios que se enfrentan a una multa si no cumplen con un requerimiento de filtrado estarán inclinados a filtrar excesivamente para evitar el castigo. Establecer obligaciones de filtrado a los intermediarios, aun si estas obligaciones están vinculadas con contenido altamente específico, puede resultar tan riesgoso y costoso para los intermediarios que los empuje a dejar de ofrecer su servicio, subir sus tarifas o restringir sus servicios gratuitos y, consecuentemente, a reducir los espacios disponibles para la expresión y el acceso a contenido legal³³.

El Consejo de Europa ha advertido que si el filtrado es aplicado a Internet, debe hacerse cuidadosamente y de acuerdo con el artículo 10 del Convenio Europeo de Derechos Humanos, que protege la libre expresión, que es similar al artículo 13 de la Convención Americana. El Consejo exhorta a que el bloqueo o filtrado por parte del Gobierno solo ocurra cuando las condiciones del artículo 10(2) se cumplan: el filtrado debe estar dirigido a contenido específico y claramente identificable, una autoridad competente debe tomar la decisión basada en la legalidad del contenido, y la decisión debe poder ser revisada por un tribunal o entidad regulatoria independiente e imparcial³⁴.

Además, las leyes nacionales deben incluir protecciones contra el abuso de los filtros y el bloqueo excesivo, así como, también, provisiones de reparación. Aun respecto a la exposición de los niños a contenidos dañinos

33. Véase CDT, *supra* nota 3.

34. Nota del editor: la traducción es de los autores. A continuación citamos el texto original:

...specific and clearly identifiable content, [if] a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body.

Recommendation CM/Rec (2008) 6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, adoptada el 26 de marzo de 2008, disponible [en línea] en: <[https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2008\)6](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6)>. [Nota del editor: consultada el 7/11/11.]

(*harmful content*), el Consejo reconoce que «cada acción dirigida a restringir al acceso a contenido está potencialmente en conflicto con el derecho a la libertad de expresión y de información». De esta manera, el Consejo advierte que cualquier sistema debe desarrollarse en pleno cumplimiento de esos principios³⁵.

Varios de los Relatores Especiales han emitido una declaración conjunta que condena el filtrado por requerimiento gubernamental: «La filtración de sistemas no controlados por usuarios finales –ya sea impuesta por un proveedor gubernamental o comercial del servicio– es una forma de censura previa y no puede estar justificada»³⁶.

Finalmente, el filtrado debe ser examinado a la luz del contexto más amplio para el acceso y la posibilidad de elección del consumidor. Varon y sus colegas describen la ausencia de un mercado competitivo para los proveedores de servicios de Internet (ISPs) en muchos países de América Latina (un problema que también se da en los Estados Unidos). Si no hay competencia, hasta el filtrado voluntario puede violar la provisión de la Convención Americana, que prohíbe las restricciones a la libertad de expresión por métodos indirectos y privados.

35. Nota del editor: la traducción es de los autores. A continuación citamos el texto original:

[...] every action to restrict access to content is potentially in conflict with the right to freedom of expression and information.

Recommendation CM/Rec (2009) 5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, adoptada el 8 de julio de 2009, disponible [en línea] en: <<https://wcd.coe.int/ViewDoc.jsp?id=1470045&Site=CM>>. [Nota del editor: consultada el 7/11/11.] El Consejo concluyó que

no es posible eliminar totalmente el peligro de que los niños sean expuestos a contenido o comportamiento dañino, y que, en consecuencia, la educación sobre medios informáticos para los niños, padres y maestros continúa siendo un elemento clave para proporcionar una protección coherente contra esos riesgos.

Nota del editor: la traducción es propia. A continuación citamos el texto original:

it is not possible to eliminate entirely the danger of children being exposed to content or behaviour carrying a risk of harm, and that consequently media (information) literacy for children, parents and educators remains a key element in providing coherent protection for children against such risks.

36. Véase Relatoría para la libertad de expresión - Comisión Interamericana de Derechos Humanos, *supra* nota 9.

II.A. Difamación y jurisdicción

Los principios de derechos humanos no prohíben las leyes de difamación. Al contrario, muchas herramientas de derechos humanos, incluyendo la Convención Americana, reconocen y protegen el derecho a la reputación o el derecho al honor³⁷. Sin embargo, las leyes de difamación pueden disuadir la expresión e interferir en los derechos de libertad de expresión y acceso a la información. El uso de las leyes de difamación para silenciar la crítica representa un peligro tanto en el ámbito en línea como fuera de él y requiere de un cuidadoso balance de los intereses en juego.

El Tribunal Europeo de Derechos Humanos ha desarrollado jurisprudencia que balancea el derecho a la libertad de expresión y la obligación de proteger el honor o los derechos de otros. Cuando el Tribunal investiga si la imposición de responsabilidad por difamación es «necesaria en una sociedad democrática», en general considera varios factores: el tema sobre el que trata la publicación, la posición del autor, la posición de la persona que fue objeto de la crítica, la caracterización de los dichos cuestionados por los tribunales domésticos, las palabras usadas por el autor y la penalidad impuesta por los tribunales domésticos. Al considerar el derecho a la reputación o al honor, el Tribunal otorga el nivel más bajo de protección a los Gobiernos. Así, el Tribunal está menos dispuesto a permitir una violación a la libertad de expresión cuando el contenido en cuestión consiste en la crítica a un Gobierno. El Tribunal ubica en un anteuúltimo lugar, en relación con el nivel de protección otorgado, a los funcionarios públicos que actúan en sus capacidades oficiales y a casos en los que está involucrado el interés público.

Los ciudadanos privados y los aspectos privados de las vidas de los funcionarios públicos reciben las protecciones más altas. En general, parecería que el Tribunal Europeo da más deferencia a la privacidad y al honor que los tribunales en los Estados Unidos. No obstante, para asegurar que se mantenga el equilibrio, en varios casos el Tribunal ratificó un juicio de difamación a la vez que anuló fuertes sanciones económicas o penales por actos difamatorios³⁸.

37. Convención Americana sobre Derechos Humanos, artículo 11, 22 de noviembre de 1969, disponible [en línea]: <<http://www.oas.org/juridico/spanish/tratados/b-32.html>>. [Nota del editor: consultada el 7/11/11.]

38. CDT, «Regardless of Frontiers: Human Rights Norms in the Digital Age», del 21 de abril de 2011, p. 51; disponible [en línea] en: <<http://www.cdt.org/policy/regardless-frontiers-human-rights-norms-digital-age>>. [Nota del editor: consultada el 7/11/11.]

El capítulo de Eduardo Bertoni, que toca el tema de cómo determinar la jurisdicción en casos de difamación, describe uno de los desafíos más complejos y no resueltos dentro de las políticas de Internet: cómo resolver los conflictos de derecho y las teorías divergentes de jurisdicción en el contexto de un medio que tiene una arquitectura que no responde a las fronteras geográficas tradicionales. Los asuntos jurisdiccionales aparecen no solo en el contexto de la difamación, sino, también, en relación con la protección de los datos, la prohibición de expresiones (por ejemplo, con leyes que prohíben los discursos del odio) y el acceso policial a los datos almacenados. En todas estas esferas, dos o más países con distintos estándares legales pueden reclamar jurisdicción sobre los mismos datos o contenidos. Las naciones alrededor del mundo están tratando de dilucidar cuándo un litigante privado, un regulador del Gobierno o un oficial policial pueden legítimamente ejercer jurisdicción sobre datos digitales o expresiones en línea que son almacenados o alojados fuera del país de la persona o la entidad que reclama la jurisdicción.

No ha emergido una teoría coherente de la jurisdicción, ni global ni regionalmente, pero el tema implica los derechos constitucionales y derechos humanos, el debido proceso legal y el principio de legalidad. Una declaración conjunta de los Relatores Especiales para la libertad de expresión de la ONU, la OSCE y la OEA da un consejo inicial:

La jurisdicción en casos relativos a Internet debe restringirse a aquellos Estados en los que el autor se haya establecido o a los cuales el contenido se haya dirigido específicamente; no debe establecerse la jurisdicción en un Estado simplemente porque el contenido haya sido descargado allí³⁹.

Aun con esta guía, la pregunta de cómo determinar si un contenido estaba «dirigido específicamente» a una jurisdicción particular sigue siendo compleja.

Como observa Bertoni, los reclamos excesivamente amplios de jurisdicción en los casos de difamación pueden traer efectos particularmente restrictivos para la libertad de expresión. Las personas que se expresan en línea frecuentemente tienen poco control sobre quién accede a los contenidos

39. Véase Relatoría para la libertad de expresión - Comisión Interamericana de Derechos Humanos, *supra* nota 9.

que crean, si han subido sus materiales a Internet. Si los individuos temen quedar sujetos a responsabilidad legal bajo la determinación de tribunales extranjeros o tienen dudas sobre si su expresión en línea está regulada por las leyes de otro país, estarán menos dispuestos a ejercer su derecho a la libertad de expresión. El impacto de este hecho sería especialmente duro para autores con menos capacidad económica que no cuenten con la posibilidad de contratar a un abogado que los pueda asesorar sobre sus derechos o defenderlos en tribunales en cualquier parte del mundo. Estos individuos estarían más dispuestos a autocensurarse para evitar la posibilidad de ser castigados con fuertes penalidades.

En otras esferas, en las que leyes divergentes y múltiples reclamos de jurisdicción están creando tensiones parecidas –más notablemente en el área de la protección de datos–, las personas encargadas del desarrollo de políticas públicas de Gobiernos, industria y sociedad civil están buscando alcanzar una mayor armonización de los estándares legales con el fin de minimizar los conflictos y las tensiones jurisdiccionales. La armonización por sí sola, sin embargo, no es suficiente, dado que la libertad de expresión está en juego, es sumamente importante que el estándar armonizado esté basado en principios de derechos humanos. De acuerdo con ello, Bertoni recomienda una armonización bajo los estándares articulados por la CIDH. Esta vía podría ser beneficiosa: la armonización regional minimizaría las tensiones jurisdiccionales, mientras que tomaría en cuenta normas regionales fuertes que reconocen tanto la libertad de expresión como el derecho al honor.

Como parte de este esfuerzo de armonización, hace falta considerar la posibilidad de despenalizar la difamación. Las instituciones de derechos humanos han alentado a los Estados a despenalizar la difamación y sostenido que la difamación solo debe ser accionable en el ámbito civil⁴⁰.

40. Véase Relatoría para la libertad de expresión - Comisión Interamericana de Derechos Humanos, «Declaración conjunta del décimo aniversario: diez desafíos claves para la libertad de expresión en la próxima década» del Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, el Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la Libertad de los Medios de Comunicación, 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) 2010, disponible [en línea] en: <<http://www.cidh.org/relatoria/showarticle.asp?artID=784&IID=2>>. [Nota del editor: consultada el 7/11/11.]

Si los líderes de las políticas públicas en América Latina avanzaran hacia la despenalización de la difamación, los países de la región podrían dar un ejemplo poderoso a la comunidad global.

Este capítulo también plantea preguntas específicas sobre el rol de los intermediarios. Como mencionamos en nuestro comentario sobre el capítulo escrito por Ruiz y Lara, cualquier regla que haga a los intermediarios responsables por los contenidos difamatorios creados por usuarios puede generar problemas para la libertad de expresión. Los proveedores de servicios que se enfrentan al riesgo de responsabilidad pueden decidir eliminar contenidos presuntamente difamatorios con demasiada rapidez para evitar la responsabilidad y porque no están habilitados para hacer una determinación sobre si cierto contenido es difamatorio⁴¹.

Las medidas cautelares también presentan otro asunto importante para los intermediarios: cuando los tribunales deciden en favor del demandante, frecuentemente dan órdenes demasiado amplias a los intermediarios en relación con la ejecución de la medida y, consecuentemente, generan problemas adicionales para la libertad de expresión. Por ejemplo, Ruiz y Lara citan varios fallos en la Argentina en los que los tribunales emitieron medidas cautelares demasiado amplias que ordenaban a los intermediarios de Internet restringir el acceso o los enlaces a contenidos que difamarían a la víctima en el futuro⁴². Para los intermediarios, las órdenes de este tipo pueden resultar en un bloqueo excesivo que restrinja expresión legal y no difamatoria. Si bien los estándares de derechos humanos permiten imponer límites a la libertad de expresión con el fin de proteger el derecho al honor de otros, estas medidas tienen que ser tomadas bajo estándares de proporcionalidad y necesidad.

Un tema que merecería más investigación es una exploración acerca de cómo las medidas cautelares podrían ser redactadas para que sean más proporcionales en los casos de difamación, es decir, cómo estrechar el ámbito de las medidas cautelares emitidas por los tribunales para que estas estén dirigidas solamente a la expresión difamatoria y se minimice su impacto sobre la expresión legal y no difamatoria.

41. Véase *CDT*, *supra* nota 3.

42. Véase, por ejemplo, Sreeharsha, Vinod, «No Safe Harbors in Argentina», en *New York Times*, 20 de agosto de 2010, disponible [en línea] en: <<http://bits.blogs.nytimes.com/2010/08/20/no-safe-harbors-in-argentina>>. [Nota del editor: consultada el 7/11/11.]

III. Conclusión

Internet será cada vez más importante para casi todos los aspectos de nuestra vida política, social y económica. Millones de ciudadanos en América Latina se están uniendo a la comunidad global de internautas cada año. Hasta la fecha, Internet ha demostrado su potencial como un motor poderoso para los derechos humanos, la participación ciudadana y el desarrollo económico. Sin embargo, como muestran los capítulos de este libro, la naturaleza abierta y libre de la red no está determinada por la tecnología. Para asegurar el mayor beneficio para el desarrollo económico y los derechos humanos, Internet debe estar apoyada por un marco de políticas que protejan la privacidad, promuevan la libre circulación de la información, desalienten la responsabilidad de intermediarios, y promuevan la innovación y la competencia.

Aun así, las características únicas de Internet presentan nuevos retos que los Gobiernos y los miembros de la sociedad civil necesitan enfrentar: ¿cómo promover la libertad de expresión, la privacidad, y el acceso al conocimiento en línea y a la vez proteger a los niños, mantener la seguridad, luchar contra el crimen y hacer cumplir los derechos de propiedad intelectual? La forma en la que América Latina responda a las preguntas sobre políticas en la red va a tener un impacto de larga duración.

América Latina está en una buena posición para liderar al mundo en la promulgación de leyes que apoyen una Internet abierta. La Convención Americana sobre Derechos Humanos articula fuertes normas que defienden la libertad de expresión y la privacidad. A pesar de que aún existe incertidumbre sobre cómo aplicar estándares ya existentes a nuevas tecnologías en la red, un enfoque hacia las políticas de Internet que esté basado en fuertes normas de derechos humanos puede generar un marco legal que maximice el potencial de Internet en la región.

Conclusiones y recomendaciones para América Latina

Eduardo Bertoni

El 12 y 13 de septiembre de 2011, el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) organizó el taller regional *Libertad de expresión e Internet: aspectos regulatorios en América Latina*, que se realizó en la Facultad de Derecho de la Universidad de Palermo. Este taller se llevó a cabo en el marco del proyecto Libertad de expresión e Internet de esa entidad, que se propone explorar, en relación con los temas enumerados a continuación, el impacto de la legislación y las decisiones judiciales y políticas de los Estados latinoamericanos sobre libertad de expresión e Internet:

Responsabilidad de los proveedores de servicios de Internet (ISPs): formas en que se impone la responsabilidad a los ISPs.

Filtrado de contenido: exploración de las regulaciones y políticas sobre filtrado de contenido en Internet.

Retención y protección de datos personales: regulación y políticas relacionadas con la retención y protección de datos personales.

Difamación y jurisdicción: difamación en línea y el problema del turismo de difamación (*libel tourism*).

El grupo de participantes incluyó a profesores, académicos y especialistas en Derecho y regulación de Internet de distintos países latinoamericanos; entre ellos, Brasil, Chile, Perú, Colombia, Uruguay, Puerto Rico y la Argentina. Los participantes locales constituyeron una muestra de la comunidad jurídica que reunió a profesores, abogados, representantes del Poder Judicial y de organizaciones no gubernamentales. La preeminencia y diversidad de los participantes contribuyó a tener un debate abierto y una discusión en profundidad de los temas del taller.

La metodología de las sesiones de trabajo del lunes 12 y el martes 13 de septiembre incluyó una presentación inicial de un artículo sobre uno de los cuatro temas que abordaba el proyecto. A continuación, otro participante formuló un comentario sobre los temas del artículo, y al finalizar las presentaciones, se realizó un debate abierto entre los participantes. Los trabajos presentados en el taller están incluidos en este libro.

Las recomendaciones y conclusiones que se detallan a continuación, para cada uno de los temas tratados, han sido elaboradas por el CELE y son el fruto de las cuestiones analizadas que tuvieron lugar durante el taller y de los estudios que el CELE llevó adelante durante la ejecución del proyecto mencionado previamente¹.

a) Responsabilidad de los proveedores de servicios de Internet (ISPs) e intermediarios

- Existe escasa y fragmentaria regulación sobre el tema de responsabilidad de intermediarios en América Latina.
- Es conveniente que el tema de la responsabilidad de los intermediarios sea regulado de forma específica, de modo que garantice que los ISP y otros intermediarios no sean responsables por los contenidos de terceros, cuando no controlen estos, ni tengan un conocimiento efectivo de su ilicitud.
- Resulta recomendable que las normas no sean ambiguas. Cuando estas no son claras, ante el temor a ser considerados responsables, se pueden crear incentivos a intermediarios a retirar contenidos por decisión propia, lo que potencialmente afectaría los derechos de libertad de expresión.

1. Estas recomendaciones y conclusiones no surgen necesariamente de un consenso de todos los participantes. En algunos temas, se escucharon opiniones diversas. El CELE agradece a todos los participantes por los aportes realizados. Estas recomendaciones no deben entenderse como una compilación de todos ellos.

- Una regulación específica del tema requiere una ponderación de los derechos e intereses en juego en cada ámbito en el que se puede generar algún tipo de responsabilidad de los intermediarios, como puede ser el área de difamación, de pornografía infantil o de propiedad intelectual. Un acercamiento general que intente cubrir todos estos espacios, sin atender las particularidades de cada contexto –el bien jurídico tutelado así como los intereses de expresión en juego–, podría ser inadecuado.
- Para que exista responsabilidad de tipo penal de los intermediarios, si ello es admisible, es imperativo que cualquier regulación de esta índole cumpla con los principios fundamentales que rigen el derecho penal.
- Al regular la responsabilidad civil de los intermediarios, debe quedar claro que las actividades mediante el uso de Internet no pueden considerarse actividades riesgosas.
- Pueden establecerse eximentes de responsabilidad de los intermediarios vinculados con los modelos de notificación y baja de contenido (*notice and take down*). Sin embargo, al implementarse estas circunstancias eximentes, debe considerarse la posibilidad de que las notificaciones sean judiciales; que se notifique también al creador del contenido que se quisiera bajar y que se procure, en todos los casos, llevar a cabo procesos judiciales sencillos y expeditos.
- Es conveniente estudiar la imposición de responsabilidad a intermediarios por la baja de contenidos que pudieran hacer de manera arbitraria, discriminatoria y sin debido proceso.

b) Retención y protección de datos personales

- Es importante resaltar la importancia de acordar en la región la definición de *dato personal*. Un tema que hay que debatir en este sentido es si la dirección IP debe considerarse dato personal. Se destaca que la dirección IP no es directamente identificatoria de una persona y que una respuesta positiva a la pregunta podría desdibujar el bien jurídico que se intenta proteger. Sin embargo, la inevitable migración desde las tecnologías de IPv4 a IPv6 podría llevar a la identificación única de dispositivos electrónicos y con ello, la necesidad de que el IP se considere un dato personal.

- Cualquier política sobre retención de datos tiene que incluir información acerca de por qué se retienen, por cuánto tiempo, quién retiene y qué se hace con los datos.
- Respecto a por qué se retienen los datos personales, un aspecto fundamental para tener en cuenta es el otorgamiento del consentimiento del titular de los datos. Sin embargo, pueden existir casos en los cuales no sea necesario, pero cuando lo fuera, el asentimiento debe ser claro y cierto.
- En lo referente al tiempo de retención de los datos, debe tenerse en consideración el impacto económico que puede acarrear este hecho durante un largo plazo de tiempo.
- Con relación a quién retiene los datos, deberían implementarse mecanismos de notificación a los titulares de los datos.
- En relación con qué se hace a partir de la obtención de los datos retenidos, deberían existir regulaciones sobre la transmisión de estos y la intervención judicial.
- No resulta aconsejable la regulación del llamado *derecho al olvido*, que en principio aparece como violatorio de la libertad de expresión y el acceso a la información.

c) Filtrado de contenido

- América Latina se encuentra en un momento particular, ya que existen muchos proyectos de ley sobre regulaciones que permitirían la posibilidad de filtrado de contenidos en Internet. Esto resulta preocupante, dado que, en principio, el filtrado de contenido es considerado una limitación a la libertad de expresión y el acceso a la información, por lo que debería implementarse excepcionalmente.
- Para llevar a cabo la implementación de políticas públicas sobre este tema, resulta necesario contar con datos certeros sobre actividades de filtrado, entre las que se incluyen las realizadas tanto por entidades privadas como gubernamentales.
- Se recomienda que exista más transparencia en torno a los mecanismos y decisiones de filtrado. Existe filtrado voluntario por parte de intermediarios que no está siendo controlado de manera adecuada. Muchas veces, los usuarios no conocen los motivos por los cuales cierto contenido ha sido removido.

- Los países de América Latina tienen una tradición de filtrado de contenido relacionado con la pornografía infantil, pero los delitos contra la honra, los derechos de autor y cuestiones políticas han sido los principales motivos de remoción de contenido, sin que hayan existido regulaciones claras que lo permitieran.
- Se aconseja que se implementen políticas de capacitación a los operadores judiciales. Se advierte desconocimiento por parte de muchos jueces sobre cuestiones tecnológicas, lo cual pudo haber derivado en órdenes judiciales de remoción excesiva de contenidos.
- En caso de regularse el filtrado de contenido, como ya mencionáramos, debería ser excepcional y seguir las pautas que establece el artículo 13 de la Convención Americana de Derechos Humanos (conocido como *test tripartito*). Además, como mínimo, deben establecerse las siguientes pautas:
 - * El filtrado debe ser delimitado, sus razones, objetivas y deben definirse estándares adecuados que minimicen la discreción de quien decide el filtrado.
 - * Deben implementarse reglamentaciones que establezcan la transparencia cuando se efectúan mecanismos de filtrado para permitir que los usuarios de Internet estén advertidos sobre posibles casos de censura, a fin de permitir procesos de apelación y/o responsabilidad por filtrados ilegítimos.
 - * Se deben implementar recursos judiciales sencillos y de resolución rápida contra decisiones de filtrado.
 - * Las órdenes de bloqueo o filtrado deben ser claras y estar delimitadas para que se apliquen solamente a contenidos que pudieran ser ilegales. La implementación de esas órdenes no puede ir más allá del bloqueo o filtrado del contenido específico que se solicita.
- La prohibición de la censura previa del artículo 13 de la Convención Americana sobre Derechos Humanos podría implicar la prohibición absoluta de cualquier tipo de filtrado en Internet, a excepción de lo previsto en el inciso 4 del mencionado artículo. Para aclarar este punto, podría instarse a los órganos pertinentes del sistema interamericano –entre ellas, la Comisión Interamericana de Derechos Humanos– a solicitar una opinión consultiva ante la Corte Interamericana de Derechos Humanos. La consulta a la Corte, de manera concreta, podría ser «si las regulaciones de filtrado de contenido que existen son compatibles con la libertad de expresión

y con la prohibición de censura previa prevista en el artículo 13 de la Convención Americana de Derechos Humanos».

d) Difamación y jurisdicción

- Resulta fundamental definir las pautas de jurisdicción para los casos que se lleven a juicio a quienes manifiesten contenidos que puedan ser considerados como difamatorios. La inseguridad sobre la ley aplicable o sobre el tribunal que trata el caso puede causar un efecto de autocensura en quienes se quieren expresar por Internet.
- Cuando los jueces en América Latina se han enfrentado a reclamos penales o civiles sobre difamación por expresiones en Internet, han adoptado distintos criterios para determinar la competencia territorial.
- Los criterios tradicionales sobre jurisdicción ocasionan problemas al aplicarse al ámbito de Internet, la que multiplica las posibilidades de calificar dónde se ha producido la conducta o dónde se originan sus efectos.
- Entre los criterios existentes, debería prevalecer el que otorga competencia al lugar del domicilio del autor de la expresión, ya que, si bien puede generar incongruencias, garantiza un mayor derecho de defensa por parte del autor y minimiza los efectos negativos sobre la libertad de expresión.
- Otra solución posible que se puede implementar para resolver las tensiones que genera el problema de la determinación de la competencia territorial consiste en adoptar normas que impidan ejecutar sentencias contrarias a los estándares internacionales que garantizan la libertad de expresión.

Sobre los autores y autoras

Bertoni, Eduardo. Abogado de nacionalidad argentina, egresado de la Universidad de Buenos Aires; ex becario del Instituto de Derechos Humanos de la Escuela de Derecho de la Universidad de Columbia, en Nueva York. Tiene una maestría en Políticas Internacionales de la Universidad George Washington. Asimismo, es profesor de la Facultad de Derecho de la Universidad de Palermo y profesor adjunto de Derecho Penal y Procesal Penal en la Facultad de Derecho de la Universidad de Buenos Aires. Director del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. Fue director ejecutivo de la Fundación para el Debido Proceso Legal, con sede en la ciudad de Washington D.C. Entre 2002 y 2005, fue Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) en la Organización de Estados Americanos (OEA).

Cerda Silva, Alberto. Profesor de Derecho Informático de la Facultad de Derecho de la Universidad de Chile. Máster en Estudios Legales Internacionales (International Legal Studies) por la Universidad de Georgetown (2010); Magíster en Derecho Público por la Universidad de Chile (2003). Actualmente es becario de la Comisión Fulbright, donde prosigue sus estudios doctorales en Derecho en la Universidad de Georgetown, y realiza una tesis en Derechos humanos y regulación de los derechos de autor en línea en Latinoamérica.

Dempsey, Jim. Vicepresidente del área de Políticas Públicas del Centro para la Democracia y Tecnología (Center for Democracy & Technology [CDT]). El CDT es una organización no gubernamental con sede en Washington D.C., cuyo objetivo es mantener Internet abierta, innovadora y libre. Se unió al CDT en 1997 y fue su director ejecutivo entre los años 2003 y 2005. En la actualidad, lidera la oficina en la Costa Oeste del CDT en San Francisco, California. En esta institución, ha concentrado su trabajo en el tema de privacidad en Internet y su monitoreo por parte del Gobierno. Antes de unirse al CDT, fue director de la organización no gubernamental Centro de Estudios en Seguridad Nacional (Center for National Security Studies). Entre 1985 y 1995, fue asesor legal del Subcomité de Derechos Civiles y Constitucionales (Subcommittee on Civil and Constitutional Rights) en el Congreso de los Estados Unidos. Ha dado testimonios ante comités del Congreso en numerosas oportunidades. Obtuvo su título en Derecho (J.D.) en la Universidad de Harvard.

Lara Gálvez, Juan Carlos. Abogado y Licenciado en Ciencias Jurídicas y Sociales por la Facultad de Derecho de la Universidad de Chile. Actualmente es ayudante de Investigación en el Centro de Estudios en Derecho Informático de la misma casa de estudios. Desde inicios de 2008, trabaja en la ONG Derechos Digitales, organismo independiente y sin fines de lucro dedicado al estudio y a la promoción de los derechos fundamentales y el interés público en el entorno digital, en el que se desempeña como investigador en jefe y responsable editorial de contenidos. Está a cargo de líneas de investigación relacionadas con la propiedad intelectual en el entorno digital, el otorgamiento de licencias abiertas para contenidos creativos y el acceso a la información pública, siempre desde un punto de vista de los intereses del público.

Meléndez-Juarbe, Hiram. Catedrático asociado de la Escuela de Derecho de la Universidad de Puerto Rico. BA por la Universidad de Puerto Rico (1997); J.D. por la Universidad de Puerto Rico (2000); LL.M. por la Universidad de Harvard (2002); LL.M. por la Universidad de Nueva York (2008); candidato a J.S.D. por la Universidad de New York. Dicta clases de Derecho constitucional; Derechos de autor; Derecho a la intimidad y tecnología; Derecho del ciberespacio; Derecho administrativo y seminarios en Derecho constitucional y el ciberespacio. Es fundador

de la Clínica de Nuevas tecnologías, propiedad intelectual y sociedad (CNTPIS) de la Escuela de Derecho de la Universidad de Puerto Rico, así como cofundador y codirector legal de Creative Commons-Puerto Rico. Actualmente cursa estudios de doctorado (J.S.D.) en la Escuela de Leyes de la Universidad de Nueva York (New York University Law School), donde investiga la intersección entre la libertad de expresión y el derecho de propiedad intelectual.

Nunziato, Dawn. Profesora de la Escuela de Derecho de la Universidad George Washington (George Washington University Law School). Reconocida experta internacional en el área de libertad de expresión e Internet. Autora del libro *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*, publicado por Stanford University Press en 2009. Ha dictado cursos sobre Derecho e Internet en la Universidad de Oxford; en el Munich Intellectual Property Law Center; en la Universidad de Tsinghua, en Pekín, y en el Instituto Tecnológico Autónomo de México.

Pereira de Souza, Carlos Affonso. Abogado y miembro de la comisión de la Ley de Derecho de Autor de la Asociación Nacional de Abogados (Río de Janeiro). Tiene un doctorado y una maestría en Derecho civil (Universidad del Estado de Río de Janeiro [UERJ]). Vicecoordinador del Centro de Tecnología y Sociedad (CTS) de la Fundación Getulio Vargas (FGV) en Río de Janeiro. Miembro de la Comisión de Derecho de Autor de la Orden de Abogados del Brasil (OAB). Miembro de la Iniciativa por Principios y Reglas en Internet (IRP) creada en el Foro de Gobernanza de Internet (IGF). Enseña propiedad intelectual, contratos y agravios en la FGV y la Universidad Católica de Río de Janeiro (PUC-Río). Siendo uno de los miembros fundadores de CTS/FGV, ha estado trabajando en una serie de proyectos relacionados con la propiedad intelectual, las nuevas tecnologías y la gobernanza de Internet, como Creative Commons-Brasil, Acceso al Conocimiento Brasil y Communia Red (un proyecto europeo dedicado al estudio del dominio público). Recientemente, como miembro de CTS/FGV, ha estado involucrado en una iniciativa de colaboración con el Ministerio de Justicia para elaborar un proyecto de ley de Derechos de Internet para Internet en Brasil. La iniciativa se llama Marco Civil da Internet Brasileira (Marco Civil de Internet brasileña <<http://culturadigital.br/marcocivil>>).

Roberts Biddle, Ellery. Encargada de Programas en el Centro para la Democracia y Tecnología (Center for Democracy & Technology [CDT]), donde trabaja en cuestiones globales en torno a la libertad en Internet, y se concentra en el tema de la libertad de expresión en América Latina. Antes de unirse al CDT, trabajó como pasante e investigadora con la Iniciativa OpenNet (OpenNet Initiative) en el Centro Berkman de Internet y Sociedad. Recibió una maestría doble en Estudios Latinoamericanos y Políticas Públicas de la Universidad de Chicago, donde investigó a la comunidad bloguera de Cuba. Escribe sobre tecnología y cultura en Cuba para *Voces globales (Global Voices Online)*.

Ruiz Gallardo, Claudio. Presidente de la ONG Derechos Digitales Chile y líder público de Creative Commons en Chile. Estudió en la Facultad de Derecho de la Universidad de Chile, donde se especializó en derechos fundamentales y regulación de nuevas tecnologías. Ha sido profesor de Teoría de la Constitución y Derechos Fundamentales en la Universidad Nacional Andrés Bello. Actualmente es profesor de Derecho y tecnología en la Universidad Diego Portales, además de profesor del Magíster en Periodismo Digital de la Universidad Andrés Bello y en el Diplomado en Propiedad Intelectual de la Universidad Finis Terrae. En la ONG Derechos Digitales, dirige proyectos vinculados con la defensa y promoción de los derechos fundamentales en el entorno en línea, particularmente libertad de expresión, nombres de dominio y acceso al conocimiento. Es consultor en materia de software libre y regulación de propiedad intelectual para el Banco Interamericano del Desarrollo. Es consejero del Consejo Nacional de Nombres de Dominio y números IP, además de ser miembro del Comité Consultivo Nacional de la Estrategia Digital de Chile.

Varon Ferraz, Joana. Coordinadora del proyecto A2K Brasil e investigadora del Centro de Tecnología y Sociedad de la Fundación Getulio Vargas (CTS/FGV). Tiene una maestría en Derecho y Desarrollo por la Escuela de Derecho de San Pablo de la Fundación Getulio Vargas (EDESCP/FGV). Graduada en Relaciones Internacionales por la Pontificia Universidad Católica de San Pablo (PUC/SP) y en Derecho por la Universidad Mackenzie, con especialización en Derecho y nuevas tecnologías y

en Derecho de la propiedad intelectual. Es representante de la Escuela de Derecho de Río de Janeiro de la Fundación Getulio Vargas en la Organización Mundial de la Propiedad Intelectual (OMPI/ONU), en la que acompaña las reuniones del Comité sobre Desarrollo y Propiedad Intelectual (CDIP) y del Comité Permanente de Derecho de Autor (SCCR). También es investigadora asociada del Centro Brasileño de Análisis y Planificación (CEBRAP) y del Observatorio de Innovación y Competitividad del Instituto de Estudios Avanzados de la Universidad de San Pablo (IEA/USP), los que presentan un enfoque en las áreas de desarrollo institucional, economía del conocimiento e innovación.

Villegas-Carrasquilla, Lorenzo. Abogado y Politólogo por la Universidad de los Andes (Bogotá, Colombia). Tiene una maestría en Derecho constitucional de la Universidad París 2 (Francia), un máster en Derecho público de la economía realizada en la misma institución y es candidato a doctor en Derecho público para esa casa de estudios. Profesor de la Universidad de los Andes (Bogotá), de la Universidad Externado de Colombia (Bogotá) y de la Pontificia Universidad Javeriana (Bogotá) en Derecho de TICS.

Wong, Cynthia. Abogada en el Centro para la Democracia y Tecnología (CDT) y Directora del proyecto de CDT sobre Libertad Global en Internet. Desarrolla gran parte del trabajo del CDT en promover la libertad global en Internet. Antes de unirse a esa institución, fue becaria Robert. L. Bernstein de Derechos Humanos Internacionales en Derechos Humanos en China (Human Rights in China [HRIC]), donde contribuyó al trabajo de esa entidad en las áreas de negocios y derechos humanos y libertad de expresión online. Recibió su título de Derecho (J.D.) en la Escuela de Derecho de la Universidad de Nueva York y su título de Bachiller en Ciencias en Ingeniería Eléctrica de la Universidad de Texas, en Austin.

Hacia una Internet libre de censura

Propuestas para América Latina

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) fue creado en el año 2009 dentro del ámbito de la Facultad de Derecho de la Universidad de Palermo con el objetivo de realizar estudios e investigaciones que se constituyan como herramientas útiles para periodistas, instituciones gubernamentales, sectores privados y de la sociedad civil dedicados a la defensa y promoción de estos derechos, especialmente en América Latina.

La creación del CELE responde a la necesidad de construir espacios de debate dedicados a reflexionar sobre la importancia, los contenidos y los límites de estos derechos en la región. Para esto, el centro se propone dialogar y trabajar en conjunto con otras unidades académicas del país y de Latinoamérica.

En este marco, los objetivos específicos del CELE son:

- Desarrollar estudios y guías de recomendaciones que tengan impacto en las políticas públicas vinculadas con el acceso a la información y a la libertad de expresión.
- Fomentar junto con distintas unidades académicas la profundización de estudios en cuestiones vinculadas con estos derechos.
- Contribuir a la generación de conciencia sobre la importancia de estos derechos en sociedades democráticas, fundamentalmente en las nuevas generaciones.

Esta publicación se realiza en el marco de un proyecto auspiciado por Open Society Institute.



Facultad de Derecho

Centro de Estudios en Libertad de Expresión y Acceso a la Información

Mario Bravo 1050, 7° P. (C1175ABT) Buenos Aires | Tel.: (54 11) 5199-4500 int. 1213

www.palermo.edu/cele