Capítulo siete

Desarrollando políticas de Internet en Latinoamérica: una perspectiva global

Cynthia M. Wong, James X. Dempsey, y Ellery Roberts Biddle[1]

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 accede[2].

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 Internet[3].

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 del 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 Autor[6] 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 legal[7]. 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 recomienden 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 anónima[8]. Los instrumentos internacionales de derechos humanos también recomiendan que las leyes nacionales preserven las oportunidades para la expresión anónima[9]. 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&lID=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 coherencia[10]. 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 aplicación[11]. Los ocho principios de la OECD frecuentemente son llamados los Principios de Práctica Justa con la Información (*Fair Informacion 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 OECD. La directiva estableció una estructura regulatoria detallada para ser adoptada por los miembros de la UE en sus legislaciones nacionales[12]. 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 consumidor[13], y la administración Obama ha propuesto la adopción de una legislación federal completa sobre privacidad[14].

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 Latina[15]. 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 nacional[16].

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 *tribunalicios*, 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 protegida[18].

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 son[19]. 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 anónimos[20]. 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 identificativa[21].

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 Internet[22].

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 Europa[24] 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 legales[25]. 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 final[26]. 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 sitio[27].

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 operador[28]. 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 contenido[29]. En la medida en que estas prácticas sean verdaderamente voluntarias, el proveedor del servicio las ejercite 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 deseada[30]. 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 extranjeros[31].

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 subido[32]. 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 legal[33].

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 imparcial[34].

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>. [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 principios[35].

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 honor[37]. 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 anteúltimo 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 difamatorios[38].

---

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 allí[39].

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 civil[40].

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&lID=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 difamatorio[41].

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 futuro[42]. 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.

Epílogo

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 previamente[1].

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.