Revista de Derecho Vol. XXVIII - Nº 1 - JUNIO 2015 Páginas 33-54

Los intermediarios de Internet como agentes normativos*

*Salvador Millaleo Hernández***

Resumen

Los intermediarios de Internet, comprendidos en sentido amplio, están integrando diversas actividades que hacen que, mediante la expansión de sus capacidades de regulación por código o diseño, trasciendan su rol clásico de neutralidad frente a los contenidos. Este cambio ha permitido a nivel global a los gobiernos resolver el problema de la falta de control normativo de la red mediante el uso de las capacidades normativas de los intermediarios. El incremento de poder normativo se ha traducido en una expansión de las responsabilidades criminales de los intermediarios en los últimos tiempos, correspondiendo a políticas criminales que refuerzan el control público de los usuarios de las redes en situaciones identificadas como de riesgo social, tal y como se puede apreciar en materia de vulneraciones a la privacidad, pornografía infantil y ofensas a la reputación.

Intermediarios – Internet – responsabilidad

The Internet Intermediaries as Legal Agents

Abstract

Internet intermediaries, broadly understood, participate in various activities that expand their ability to use coding or designing, which transcend their classic role of neutrality regarding the online content. This change has enabled governments globally to solve the problem of the lack of control of the network by using the normative capabilities of intermediaries. The increase of normative power in recent times has leaded to an expansion of criminal liability of intermediaries. These criminal policies have strengthened public control of network users in situations considered as social danger, for example, on violations of privacy, child pornography and offences to honour.

Intermediaries – Internet – Liability

* Artículo escrito en el marco del Proyecto Fondecyt de Postdoctorado Nº 3130479.

** Dr. Phil., Profesor de Derecho, Facultad de Derecho, Universidad de Chile. Correo electrónico: salvador.millaleo@googlemail.com.

Artículo recibido el 28 de septiembre de 2014 y aceptado para su publicación el 27 de marzo de 2015.

Introducción

La Internet es una red que permite cada vez mayores posibilidades de interacción entre los usuarios, para diversos propósitos. Estas capacidades son posibles gracias a la intervención de una pléyade de intermediarios en las diversas capas que componen la red.

La visión tradicional relativa a la libertad de la red ha dependido, por tanto, de la comprensión acerca de la autonomía del rol de los intermediarios y, con ello, respecto de las obligaciones y cargas legales que ellos soportan.

El objeto de esta investigación consiste en comprender cómo las tendencias en la regulación de la responsabilidad de los intermediarios han cambiado hacia un paradigma de corregulación, el que a su vez ha hecho posible una amplia regulación de la red y del comportamiento de sus usuarios. Dentro de estas transformaciones observamos como una de las novedades más importantes la expansión de la responsabilidad penal de los intermediarios.

La responsabilidad penal de los intermediarios refuerza el control de los gobiernos sobre los actores principales de Internet y con ello condicionan que estos últimos incrementen sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes. Con ello se terminan de derribar las concepciones iniciales de la anomia y desorden normativo de la red y nos coloca frente a poderosas arquitecturas de control que se están expandiendo de la mano de políticas criminales basadas en nociones de riesgo.

Esta investigación ha sido realizada desde la perspectiva de las relaciones entre derecho y sociedad, procurando entender los efectos de los conjuntos normativos en las relaciones sociales de control. El foco ha sido para ello colocado en las prácticas más importantes que se pueden ofrecer en el panorama global para ilustrar dichas relaciones, procediendo a un análisis comparado de precitadas prácticas.

En primer lugar analizaremos el paso de las nociones de la autorregulación a la corregulación como enfoques normativos dominantes de la red. En segundo lugar revisaremos los cambios específicos acerca de las capacidades y naturaleza normativa de los intermediarios de Internet. En tercer lugar observaremos cómo se ha desarrollado la responsabilidad penal de los intermediarios en los temas de invasión a la privacidad, pornografía infantil y difamación, produciendo como efecto el incremento de los poderes de control de los intermediarios sobre sus usuarios, aunque en tensión con los regímenes subsistentes de limitación y exención de responsabilidad de los intermediarios. Hemos escogido estas áreas porque son menos conocidas que otras donde se ha concentrado la atención de investigadores, especialmente la propiedad intelectual o vigilancia por razones de seguridad pública o contraterrorismo.

Para los efectos de este artículo, entenderemos el concepto de intermediarios de Internet definido de manera amplia. Según esta noción, los intermediarios de Internet son todos aquellos agentes que facilitan o realizan transacciones para terceras partes en Internet[1]. En este sentido, los intermediarios realizan en las diferentes capas en que se estructura la red actividades múltiples, ellas posibilitan las comunicaciones entre los

[1] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing, Paris, 2011, p. 21.

extremos de la red Internet donde se encuentran los usuarios finales. Estas actividades van mucho más allá de la construcción de infraestructuras físicas de comunicación y del servicio de acceso a Internet, sino que abarcan también a los proveedores de servicios de *hosting*, procesamiento de datos y entrega de información, como a los proveedores de servicios de pagos *on line*, navegadores, motores de búsqueda, mensajería de correo e instantánea, plataformas de *e-commerce* y plataformas colaborativas (redes sociales).

Esta definición amplia difumina la clásica distinción entre proveedores de servicios de Internet y proveedores de contenidos, que estaba destinada a aislar y mantener neutrales a los proveedores de Internet como meros conductores del contenido. Frente a ellos, los proveedores de contenido intermediaban los contenidos creados por los usuarios, el que conocían y respecto del que no eran neutrales[2].

I. Regulación por código: De la autorregulación al control corregulatorio sobre los intermediarios

El enfoque más conocido para la regulación de la red en sus comienzos ha sido la autorregulación. A este enfoque subyacía la idea de que los Estados y sus sistemas legales no pueden imponer sus reglas al llamado ecosistema digital, de tal manera que cualquier intento de hacerlo estaba condenado al fracaso. Una de las formulaciones más claras de este ideario la podemos encontrar en la Declaración de Independencia del Ciberespacio de 1993, escrita por John Perry Barlow. Barlow sostendrá entonces para el ciberespacio que: *Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here*[3].

Para muchos autores, la fluidez de las redes de información hacía inoperantes e inútiles las regulaciones estatales sobre la red, de manera que podía concebirse una verdadera soberanía del ciberespacio[4]. Por lo demás, los procesos de digitalización e interconexión mundial se realizan de manera decisiva por parte de actores no estatales, los intermediarios de la red, quienes responden mejor a un entorno cambiante e incierto[5].

El Estado no contaba, según dicha visión inicial, con las capacidades para regular Internet. Si un gobierno quiere imponer su derecho en Internet se encontraría que no tiene el control físico de la red necesario para imponer su autoridad[6]. Además, los estados tienen dificultades para perseguir y encontrar personas que pudieran ser responsables por daños o que puedan ser sujetos a castigo penal, debido a que una de las características clave de

[2] Bayer, J., *Liability of Internet Service Providers for Third Party Content*, Victoria University of Wellington, Wellington, 2008.

[3] Ver https://projects.eff.org/~barlow/Declaration-Final.html visto 10-08-2014.

[4] Wu, T., "Cyberspace Sovereignty? - The Internet and the International System", en *Harvard Journal of Law & Technology,* Vol. 10, Nº 3, summer 1997, 647-666, p. 649.

[5] Muñoz Machado, S.*, La Regulación de la Red, Poder y Derecho en Internet*, Taurus, Madrid, 2000, p. 33.

[6] Mefford, A., "Lex Informatica: Foundations of Law on the Internet"*,* en *Indiana Journal of Global Legal Studies,* Vol. 5, Issue 1, 1997, 211-237, p. 214.

Internet es que está configurada para operar lógicamente antes que geográficamente[7]. La operación de Internet quedaba así fuera de los conceptos jurisdiccionales del Estado. Las jurisdicciones estatales tampoco pueden funcionar a la velocidad necesaria para satisfacer las necesidades del ciberespacio y carecen del conocimiento experto para tales efectos.

En esta visión, el déficit de seguridad de las expectativas normativas en la red sería, sin embargo, colmado por varias reglas de origen no estatal, elaboradas espontáneamente por los propios actores de la red. La Internet debía ser gobernada como un espacio global que no es controlado por ninguna soberanía estatal, sino que se realiza de una manera descentralizada, careciendo de estructuras reguladoras centrales y basada en la aceptación consensuada de reglas por parte de los actores de la red[8]. Tales reglas que rigen el tratamiento de la información digital deben ofrecer la estabilidad y previsibilidad para que los participantes tengan suficiente confianza en sus comunidades para realizar las diferentes transacciones *on line*, como lo posibilitaban las reglas espontáneas de los mercaderes medievales, la llamada *lex mercatoria*[9].

El ejemplo más claro de esto son los protocolos de comunicación de Internet, los cuales fueron regulados mediante directrices conocidas como *Requests for Comments* (RFC), las que fueron elaboradas desde la base por los mismos actores de la comunidad global de Internet en sus primeros momentos, involucrando a los desarrolladores técnicos y a los proveedores de servicios de Internet y grupos de usuarios más importantes en aquella época[10]. Ese conjunto normativo, por cierto no sistemático ni jerarquizado, es lo que se denominó como Lex Informática. La Lex Informática estaba constituida por reglas fragmentarias, de origen no estatal, basadas en gran parte en los contratos y siendo influenciadas determinantemente por las condiciones fácticas impuestas por la técnica. Estas reglas se presentaban principalmente en la forma de *soft law* y reglas programáticas, en lugar de reglas de obligación[11].

En la muy conocida tesis de Lawrence Lessig podemos distinguir cuatro formas fundamentales de regulación social: reglas legales, mercados, normas sociales y la arquitectura o código[12]. La novedad de esta distinción consistía en la cuarta forma, la "arquitectura" o

[7] Johnson, D.; Post, D., "Law and Borders - The Rise of Law in Cyberspace", en *Stanford Law Review,* Vol. 48, Nº 5, 1996, 1367-1402.

[8] Johnson, D.; Post, D., "And How Shall the Net be Governed? A Meditation on the relative virtues of decentralized, emergent law", en Kahin, B.; Keller, J. (Eds.), *Coordinating The Internet*, The MIT Press, Boston, 1997, 62-91.

[9] Reidenberg, J, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", en *Texas Law Review,* Vol. 76, Nº 3, 1998, 553-593, p. 554.

[10] El procedimiento de las RFC se diferencia del proceso tradicional de elaboración intergubernamental de estándares que llevan adelante cuerpos de estandarización como ISO, IEC o ITU en que está basado en un consenso robusto antes que en un consenso puro, en cuanto el proceso de comenatrios y observaciones a propuestas iniciales es moderado por los iniciadores del proceso, actualmente los diversos cuerpos de gobernanza de Internet, que son los que al final toman las decisiones.

[11] Trudel, P., "La Lex Electronica", en Morand, Ch. (dir.), *Le droit saisi par la mondialisation*. Éditions Bruylant, Bruxelle, 2002, pp. 221-268.

[12] Cfr. Lessig, L., *Code and other Laws of Cyberspace, V. 2.0.* Basic Books, New York, 2006.

código, que se refiere a las limitaciones materiales que definen los límites de la conducta humana en una situación o lugar específico. La arquitectura de Internet, consiste en la conjunción de elementos del *hardware* y el *software*, que al igual que la arquitectura física, permite y anima a los seres humanos para comportarse de ciertas formas, haciendo más probables algunas actividades que otras. Las capacidades tecnológicas y opciones de diseño del sistema imponen así reglas de comportamiento sobre los participantes[13]. La arquitectura de Internet está construida de diversos componentes tecnológicos que actúan en varios niveles o capas. Los estándares arquitectónicos, como el protocolo http, definen una estructura básica y los valores de los flujos de información en las redes.

La fuente normativa principal de ella es predeterminada por el desarrollador de la tecnología. Los técnicos diseñan la infraestructura básica con características que crean e implementan políticas de la información por defecto. Aunque los gobiernos pueden influir en las decisiones tomadas por los tecnólogos por medio de restricciones jurídicas a las opciones de política, los técnicos elaboran y aplican normas técnicas y los usuarios adoptan aplicaciones precisas de estas en sus prácticas.

Tabla 1
Comparación entre reglas y estándares técnicos[14]

	Derecho	Estándares técnicos
Tipo de reglas	Derecho estatal	Estándares arquitecturales
Jurisdicción	Territorio	Red
Contenido	Reglas generales, reglamentos, decisiones judiciales	Capacidades técnicas, prácticas consuetudinarias
Fuente	Estado	Técnicos
Reglas de los destinatarios	Contrato	Configuración
Negociación de reglas por destinatarios	Bajo costo Costo medio Alto costo	*Off the shelf* Instalación configurable Elección del usuario
Ejecutabilidad primaria	Tribunales	Autoejecución, automático

La Lex Informática permite la regla automatizada y de aplicación directa del cumplimiento. Los estándares tecnológicos pueden estar diseñados para evitar que tengan lugar acciones sin los permisos de la autoridad competente.

Podemos identificar las siguientes características ventajosas de la Lex Informática relacionadas con su eficacia frente a las normas jurídicas: 1. La Lex Informática se aplica por medio de las fronteras y no se enfrenta al mismo problema jurisdiccional que los

[13] Reidenberg, J. *Op. cit*., p. 555.

[14] Fuente: Reidenberg, J. *Op. cit*., p. 569.

regímenes jurídicos territoriales; 2. permite reglas adaptables a situaciones concretas, para poder aplicarse a diversas situaciones de la red y preservar opciones para las personas participantes; 3. ofrece dos formas para la aplicación normativa, en cuanto los dispositivos tecnológicos pueden ser fácilmente desarrollados para vigilar el cumplimiento de las reglas; y que a diferencia de la aplicación *ex post* de las reglas legales, la Lex Informática se basa normalmente en las medidas previas de autoejecución.

La característica clave de la arquitectura de Internet es el modelo de capas. Debido a que una red informática no es más que un conjunto de equipos conectados entre sí, la arquitectura de red será determinada por la arquitectura de los protocolos que permiten la conexión en red. Un protocolo de red es un conjunto de normas y convenciones de los equipos que pueden comunicarse entre sí[15]. El protocolo de red TCP/IP fue diseñado para ser solo un protocolo de *software*, independiente de cualquier equipo en particular y *hardware* de red, para permitir la interconexión de los diversos equipos a la red.

Tabla 2
Capas de Internet[16]

Capas		Elementos (ejemplos)
Capa física		*Ethernet, Modem*, DSL, cable, T1, fibra óptica, satélite, *Bluetooth*.
Capa de enlace	Capa lógica	Conexión a la capa física.
Capa de red		IP, ICMP, IGMP.
Capa de transporte		TCP, UDP.
Capa de aplicaciones		HTTP, SMTP-*Email*, FTP, *Instant Message*, DNS, *Web Browser*, Procesadores de texto, *software* de procesamiento de imágenes y edición de videos, ripeo de MP3, etc.
Capa de contenidos		Datos: textos, video, música, animaciones, etc.

a) X[Capa física: Es el medio físico sobre el cual la transferencia real de *bits* se lleva a cabo.
b) Capa lógica:
   a. Capa de enlace: Se encarga de todos los detalles de la interfaz física con el *hardware* del equipo y el *hardware* de red. Como tal, esta capa es responsable de la independencia del protocolo TCP/IP respecto del *hardware*.
   b. Capa de red: Maneja el movimiento de paquetes de datos alrededor de la red. La codificación de las direcciones IP y el enrutamiento de los paquetes de datos de conmutación ocurre en este nivel.
   c. Capa de transporte: Proporciona un flujo de datos entre dos sistemas principales para la capa de aplicaciones. Aquí es donde los datos recibidos desde la capa de aplicaciones se dividen en paquetes de datos para ser entregados a la red o capa IP, y los paquetes de datos recibidos desde la capa IP se montan en un flujo de datos para ser entregados a la capa de aplicaciones.
   d. Capa de aplicaciones: Se encarga de los detalles de la aplicación particular de los datos, incluyendo las aplicaciones que manejan esos datos en la interface con el usuario.
   e. Capa de contenidos: Son los datos de los usuarios.

[15] Solum, L; Chung, M., "The Layers Principle: Internet Achitecture and theLaw", en *Notre Dame Law Review,* Vol. 79, Nº 3, 2004, 815-948, p. 21.

[16] Fuente: Basado en Solum, L; Chung, M., *op. cit.*, pp. 21-22.

La regulación por código ocurre principalmente en la capa lógica, donde los protocolos determinan la forma en que se producen, circulan y se usan los contenidos de información de los usuarios. Pero cada vez más cobra importancia la capa de contenidos, por la expansión de aplicaciones de última milla para hacer los contenidos adaptables a las necesidades específicas de los usuarios y que permiten el aporte de contenidos por ellos, y por el consecuente incremento exponencial de contenidos digitales.

Quien define el código puede decidir qué puede o no puede hacerse, y esta capacidad se ha radicado en las manos de agentes privados que constituyen los grandes monopolios de la sociedad de información, creando un orden privatizado donde esos poderes administran los interruptores maestros de la red[17]. Estos son los precisamente intermediarios de Internet en todas sus variedades.

Los intermediarios son empresas que facilitan las infraestructuras y aplicaciones para el funcionamiento de cada una de las capas. El rol normativo que cumplen, en el enfoque original de la autorregulación, era ejercido de una manera espontánea, con diversas formas de consulta con los pocos usuarios que tenía la red en sus momentos iniciales. Con el paso del tiempo este enfoque de regulación espontánea será superado por la realidad de la expansión de nuevas formas de control sin consentimiento de los usuarios.

La tendencia es que, en la medida que el código es producido por un número cada vez menor de empresas, el ciberespacio se vuelve más regulable y regulado por dichas empresas, es decir, lo contrario a lo que sostenía la tesis de la autorregulación de la red. Las empresas que controlan determinados productos o aplicaciones pueden, debido a la expansión escalar del uso de estos, pasar a definir mercados enteros en poco tiempo en virtud del ejercicio unilateral de su poder de mercado, controlándolos al definir estándares de hecho para ellos mediante la regulación por código[18]. Aunque no todos los intermediarios de Internet son elefantes de su mercado, el rol de los intermediarios a menudo involucra la posibilidad de crecimiento dentro de ese mercado debido a un "efecto red"[19, 20].

Las corporaciones que manejan las capas pueden cambiar las características de estas para maximizar sus beneficios, pero también los gobiernos descubrieron desde hace tiempo que pueden obligar a estas empresas a modificar el código según sus propios intereses. De esa forma mediante una estrategia de control sobre los intermediarios el Estado puede efectivamente regular la red y el comportamiento de los usuarios[21].

---

[17] Cfr. Wu, T., *The Master Switch: The Rise and Fall of Information Empires*, Vintage Books, New York, 2010.

[18] Cfr. Coates, K., *Competition Law and Regulation of Technology Markets.* Oxford University Press, New York, 2011.

[19] Rowland, D.; Kohl, U.; Charlesworth, A., *Information Technology Law,* Routledge, London, Fourth Edition, 2012, p. 73.

[20] El efecto red se refiere al fenómeno que implica que el valor de determinados bienes y servicios crece con el incremento del número de sus usuarios.

[21] Goldsmith, J.; Wu, T., *Wo Controls the Internet?: Illusions of a Borderless World: Illusions of a borderless world,* Oxford University Press, Oxford, 2006, p. 73.

De acuerdo con John Palfrey[22], al principio del siglo XXI los Estados y otros agentes reguladores llegaron a pensar que las actividades en Internet pueden y necesitan ser regulados o administrados de diversas maneras. Los responsables políticos cambiaron el enfoque de los años noventa en la medida que Internet fue expandiendo su accesibilidad y el valor de sus contenidos con la banda ancha, así como también los actores económicos de Internet se redujeron desde una miríada de emprendedores virtuales hacia unas pocas corporaciones privadas (ISP, motores de búsqueda, proveedores de *e-commerce*)[23].

El enfoque de los noventa da paso a una arquitectura de control donde los intermediarios que actuaban en la red se transforman, debido a sus capacidad de regulación por diseño o código, en instrumentos de regulación por parte de los gobiernos. Los gobiernos individualmente dentro de sus propias jurisdicciones, o actuando en el escenario internacional, e inclusive entidades regulatorias internacionales –como cuerpos de estandarización– pueden influir determinantemente en el entorno de Internet y así orientar indirectamente a los usuarios[24].

Según Ian Brown y Christopher Mardsen aseguran al respecto:

> "Tal uso del poder de mercado de los gigantes del *software* y servicios para ejercer medidas regulatorias de preferencia de los legisladores nacionales ha llegado a ser un lugar común –requiriendo reescribir el código de Facebook, Google, Skype y Microsoft para forzar a las empresas a obedecer las normas legales–. Esta es una técnica regulatoria únicamente apropiada para esos bienes informacionales"[25].

Los Estados están regulando a las empresas privadas tanto para restringir directamente lo que las empresas pueden hacer como para exigir a las empresas para llevar a cabo el control de las personas. Además, los Estados están estudiando la manera de limitar lo que las empresas basadas en su jurisdicción pueden hacer en otros países, como una forma de contrarrestar la reglamentación de otros Estados. Y también, los estados se esfuerzan por encontrar formas de limitar lo que otros Estados pueden hacer por medio de su actividad en Internet[26].

Los reguladores, junto con la legislación directa –o precedentes judiciales como en los célebres juicios acerca de la propiedad intelectual–, están probando nuevas formas de regulación. Entonces empieza a surgir la corregulación como el nuevo enfoque regulatorio

---

[22] Cfr. Palfrey, J., "Four Phases of Internet Regulation". Harvard Law School Public Law & Legal Theory Working Paper Series Paper Nº 10-42, 2010.

[23] Marsden, C., *Internet Co-Regulation European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge, 2011, p. 9.

[24] Pattberg, Ph., "The institutionalization of private governance: How Business and nonprofit organizations agree on transnational rules", En *Governance: An International Journal of Policy, Administration and Institutions* Nº 18, 2005, 589-610.

[25] Brown, I.; Mardsden, C., *Regulating Code, Good Governance and better regulation in the information age,* The MIT Press, Cambridge & London, 2013, p. xiii.

[26] Palfrey, J., *op. cit.*

dominante para Internet[27]. Esta es definida –por la agencia regulatoria del Reino Unido, Ofcom– como aquella situación en que un organismo de derecho público con autoridad reguladora delega la responsabilidad en la industria relevante para el mantenimiento y la aplicación de un código de prácticas que ha aprobado el organismo regulador oficial, continuando en la supervisión de la corregulación, reteniendo los poderes de intervenir cuando se considere necesario[28].

La corregulación consiste en una forma híbrida de regulación, donde el poder normativo de las empresas privadas intermediarias de Internet es empleado por mandato de la autoridad estatal para lograr ciertos propósitos. Este mandato puede ser estricto o más bien amplio en sus términos, pero se realiza mediante el control gubernamental de las empresas y sus oportunidades de negocio en sus jurisdicciones, de manera que también varía con el poder y la importancia de los gobiernos para los mercados.

La corregulación ha sido empleada profusamente en los últimos años, para tratar diversos temas jurídicos de Internet: las regulaciones de *safe harbor* en EE.UU. y Europa para la privacidad *on line*, los códigos de buena conducta respecto de la pornografía infantil, la regulación administrativa de la neutralidad de red que en EE.UU. hace la FTC, y los diversos sistemas de filtrado de contenidos que se han impuesto sobre los intermediarios tanto por gobiernos autoritarios como por gobiernos democráticos para diversos fines, entre muchos otros ejemplos.

II. Los intermediarios de Internet como reguladores de contenidos y de los usuarios

La transformación descrita en la forma de regulación de la red ha afectado directamente los regímenes de responsabilidad de los intermediarios de Internet por los actos y contenidos de los usuarios de sus redes. Estos regímenes fueron instalados a fines de los noventa para proteger a los intermediarios, y por ello a su rol para la generación y funcionamiento de Internet, respecto de las demandas de responsabilidad que pudieran hacerse valer por los conflictos crecientes que se provocaban por los contenidos ofensivos para los derechos de otros o para la legislación nacional.

En Internet es evidente que hay posibilidad y probabilidad de patologías y conflictos, incluyendo la producción de daños, que determinará el nacimiento de responsabilidades desde la perspectiva del derecho civil y eventualmente del derecho penal.

La masividad del acceso a Internet y la diversidad y complejidad de los comportamientos de los usuarios en Internet ha hecho aparecer riesgos y posibilidades de perjuicios muy graves. Esto se incrementa por la complejidad técnica. Desde luego el anonimato

[27] Weiser, Ph., "The Future of Internet Regulation", Legal studies research paper series Working, Paper Number 09-02, University of Colorado Law School, February 2, 2009.

[28] Ofcom, *Online protection: a survey of consumer, industry and regulatory mechanisms and systems*, 2006, p. 12, On line in: http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/onlineprotection visto 15-09-2014.

de muchos usuarios de la red y la naturaleza global de los flujos de información colocan una complejidad adicional a estos riesgos.

Frente a ello, los intermediarios parecen blancos perfectos para las expectativas normativas que surgen de la ocurrencia de perjuicios, debido a su determinabilidad –a diferencia de los usuarios amparados en el anonimato–, al tamaño y solidez patrimonial de las empresas que ejercen el rol de intermediación, y a las posibilidades de control del comportamiento de los usuarios que les da su rol normativo de facto que ya hemos descrito más arriba.

Estas razones influyeron para que hacia el fin de la primera etapa de la Internet se comenzara a regular la responsabilidad de los intermediarios provocadas por los actos de sus usuarios.

Los regímenes instalados entonces consisten en el sistema de inmunidad general que establece la sección 230 de la Communications Decency Act de 1996 en EE.UU. al no considerar a los intermediarios como editores, y la inmunidad condicionada o sistema de *safe harbor*[29] de la sección 512 de la Digital Millenium Copyright Act de 1998, para los casos de derecho de autor. Por lo demás, la Unión Europea también estableció un sistema de inmunidad condicionada o *safe harbor* en su Directiva de Comercio Electrónico 2000/31/CE, pero de naturaleza horizontal, esto es, aplicable a cualquier materia[30]. Este último sistema funciona sobre la base de conceder inmunidad frente a la ausencia de selección o iniciativa y conocimiento efectivo de los intermediarios respecto de contenidos ilícitos y en su diligencia para bloquear o retirar contenidos en cuanto ese conocimiento es obtenido o notificado.

Como todo régimen de responsabilidad, el diseño de la responsabilidad de los intermediarios de Internet atiende tanto a las consideraciones del sistema jurídico de cómo realizar justicia correctiva para reparar el daño a terceros[31] como a la adjudicación de estímulos para que los sujetos de responsabilidad tomen las medidas efectivas para prevenir los daños a la vez que puedan desarrollar su actividad sin cargas excesivas[32].

Por lo anterior, los regímenes de responsabilidad son, primero que todo, regímenes de limitación y exención de responsabilidad por actos de terceros. De hecho, la decisión de limitar la responsabilidad de los intermediarios fue una de las decisiones de política

[29] Para ver en detalle el concepto y funcionamiento de las excepciones de *safe harbor* o puerto seguro ver Peguera, M., "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems", en *Columbia Journal of Law & the Arts,* Vol. 32, Nº 4, 2009, 481-512.

[30] Estos regímenes los hemos descrito en detalle en otro lugar, Cfr. Millaleo, S., "Transformaciones Globales en la Responsabilidad de los Intermediarios de Internet por los Contenidos de sus Usuarios", en prensa. También se puede ver Article 19, *Internet Intermediaries: Dilemma of Liability*, Article 19, London, 2013; Seng, D., *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, WIPO, Ginebra, 2010; Kleinschmidt, B., "An International Comparison of ISP's Liabilities for Unlawful Third Party Content", en *International Journal of Law and Information Technology,* Vol. 18, Nº 4, 2010, 332-355.

[31] Cfr. Weinrib, E., "Restitutionary Damages as Corrective Justice", en *Theoretical Inquiries in Law*, Vol. 1, Nº 1, 2000: Weinrib, E., *Corrective justice*, Oxford University Press, Oxford, 2012.

[32] Cfr. Peguera, M., *Mensajes y Mensajeros en Internet: La responsabilidad civil de los proveedores de servicios intermediarios,* UOC, Barcelona, 2001.

pública más importantes que dieron forma al diseño de la Internet y la libertad de sus usuarios[33].

En los primeros días de la Internet, los intermediarios fueron percibidos como los facilitadores del nuevo mundo de la Internet, al permitir la comunicación directa e inmediata entre los usuarios, desplazando a los viejos intermediarios del discurso, a saber, los periódicos y otros medios de comunicación masivos. Dicha comunicación directa y descentralizada entre los usuarios reflejó un cambio dramático en el ambiente cultural de las industrias de contenidos y medios. Dichas industrias y medios tradicionales controlaban tanto los contenidos como el acceso a ellos, mediante sus funciones de producción y de revisión editorial. En cambio, los nuevos medios digitales, en manos de los intermediarios *on line*, ponen a disposición del público el contenido que ha sido generado, la mayor parte de las veces, por los mismos usuarios de las redes en diversos formatos (imágenes, videos, sonido, texto, etc.). El desarrollo de las herramientas tecnológicas y plataformas facilitadas por los intermediarios para el libre aporte, difusión y acceso a los contenidos es lo que explica la proliferación de contenidos que le brinda a la red su actual valor económico, cultural e inclusive político.

Los legisladores y las cortes que conocieron los primeros casos en que se disputaba acerca de la responsabilidad de los intermediarios por hechos ajenos, animaron a estos a mantenerse como facilitadores neutrales y abstenerse de intervenir en los datos, para asegurar eximirse de responsabilidad[34]. Con esta solución, se evitaba hacer valer vínculos causales poco claros entre las actividades del intermediario y los contenidos dañinos, así como cargar a los intermediarios con deberes de monitoreo y vigilancia de los contenidos en sus redes, encareciendo sus costos de operación y, finalmente, para no brindar estímulos a los intermediarios a funcionar como porteros respecto de los contenidos aportados por los usuarios que podrían comprometerlos porque incrementan las posibilidades de censura por parte de ellos y autocensura por los mismos usuarios[35].

La responsabilidad de portería (*gatekeeping*) consiste en aquella que se adjudica a un sujeto –no necesariamente vinculada a una culpa– por tener los menores costos para poder detectar y evitar ciertas conductas dañosas de terceros, o bien orientar su conducta en cierta dirección. La idea original de la limitación de responsabilidad es no adjudicar dicha responsabilidad a los intermediarios para no transformarlos en una policía de Internet y mantener a esta libre de censura[36].

---

[33] Elkin-Koren, N., "After Twenty Years: Copyright Liability of Online Intermediaries", en Frankel, S.; Gervais, D. (eds), *The Evolution and Equilibrium of Copyright in the Digital Age*, Cambridge University Press, Cambdrige, 2014.

[34] Elkin-Koren, N., "Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability for Bulletin Board Operators", en *Cardozo Arts and Entertainment Law Journal*, 13, 1995, 345-413, p. 363.

[35] Rowland, D.; Kohl, U.; Charlesworth, A., *op. cit.*, p. 74.

[36] Mann, R.; Belzley, S, "The Promise of Internet Intermediary Liability", en *William and Mary Law Review*, Vol. 47, 2005, 239-307, pp. 22 ss.

La política pública que refleja las limitaciones de responsabilidad hacia los intermediarios en línea se ha basado en la ecuación entre la inmunidad de ellos y la libertad de los usuarios, cual es que los intermediarios estarían exentos para que no intervengan en la comunicación directa entre los usuarios, y preservar así el libre flujo de información. Esta ecuación, desarrollada a lo largo de la década de los noventa, va a ser puesta en cuestión durante la década pasada.

Los gobiernos cambiaron su política hacia los intermediarios, toda vez que ellos representan la vía más sencilla y segura para obtener control sobre las comunicaciones de Internet, sin tener que buscar a los usuarios. De esa manera, los objetivos regulatorios de los gobiernos respecto de la Internet se pueden alcanzar interviniendo en la cadena de intermediaciones, donde aparecen como los eslabones más débiles para fines de vigilancia, control o censura. Si los gobiernos persiguen objetivos políticos o de otra índole, siempre será más rentable y sencillo dirigirse contra los intermediarios tecnológicos, antes que a la masa de usuarios distribuidos y muchas veces anónimos que han aportado los contenidos que disgustan a aquellos.

Los intermediarios de Internet, por su parte, en la actualidad muestran una tendencia al aumento de la convergencia de control, esto quiere decir, entre la convergencia de control sobre el acceso, el control de los contenidos y el control sobre los usuarios. Esta convergencia se distancia del clásico rol neutral de los intermediarios de Internet[37], mostrando los siguientes rasgos[38]:

i) Esta convergencia tiene una primera dimensión en la fusión de acceso y control, en cuanto los intermediarios están brindando acceso a los contenidos en nuevas formas sofisticadas, por ejemplo, mediante los motores de búsqueda que arrojan resultados priorizados para las búsquedas de los usuarios, o las redes sociales que orientan el acceso a la información según la red de contactos de los usuarios. La suscripción a cambio de ser priorizado en las búsquedas es parte del negocio habitual de intermediarios como Apple (*App store*) o Youtube (canales pagados).
ii) Otro elemento de convergencia consiste en que los intermediarios por medio de procesos de integración vertical o acuerdos comerciales, han pasado de ser meros distribuidores a convertirse en editores de contenidos. Este es el caso de las posibilidades de autopublicación que ofrece Kindle de Amazon a los autores (Kindle Direct Publishing). Los intermediarios actuales ya no son simplemente un medio para conectar usuarios y contenidos, sino que funcionan cada vez más como minoristas de contenido.

[37] De Beer, J.; Clemmer, C., "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?", en *Jurimetrics Journal,* Nº 49, 2009, 375-409.

[38] Elkin-Koren, N., "After Twenty Years: Copyright Liability of Online Intermediaries", en Frankel, S.; Gervais, D. (eds), *The Evolution and Equilibrium of Copyright in the Digital Age*, Cambridge University Press, Cambdrige, 2014.

Cuando ejercen labores editoriales, los intermediarios pueden empezar a controlar la forma en que los contenidos se vuelven disponibles y su formato. Se puede controlar el uso de un video *on line*, si es posible archivar un *e-book* para su lectura posterior y en qué dispositivos, o si son interoperables las plataformas para ver archivos –por ejemplo no podemos ver libros de Kindle en otros dispositivos–.

La otra variante del control sobre los contenidos consiste en las alianzas comerciales de los intermediarios con proveedores y administradores de contenidos. Como ejemplo, podemos citar el sistema de identificación de contenidos de Youtube, que permite a los titulares de contenidos rentabilizar sus derechos por el uso de sus contenidos en la plataforma de Youtube, o los acuerdos de Google con las editoriales para compartir los ingresos por la visualización de los libros digitalizados en Googlebooks. Con estos acuerdos se puede obstaculizar a la competencia mediante el uso del poder de mercado para priorizar los contenidos propios y los de los aliados comerciales.

iii) Cuando los intermediarios tienen interés en proteger sus propios contenidos y los de sus socios comerciales, tienen estímulos para vedar el acceso a contenidos libres o gratuitos que puedan amenazar la influencia de dichos contenidos y así bloquear su acceso o circulación en su plataforma.

iv) Los intermediarios también pueden controlar la demanda de contenidos, por medio de los filtros que se aplican en la relación con sus usuarios[39]. Estos filtros se alimentan de las preferencias pasadas de los usuarios en sus búsquedas de contenidos, proporcionando datos de dichos usuarios que son administrados por los intermediarios. Los datos acerca de los usuarios y su uso de contenidos se recoge de forma continua, siendo usados para el diseño de estrategias de *marketing* y la promoción de la demanda de contenidos particulares propios del intermediario o de sus socios comerciales, usando filtros que hacen a los usuarios ver en sus búsquedas los contenidos priorizados en tales estrategias. Si bien estos mecanismos de filtrado pueden ser utilizados para servir mejor a las preferencias de los consumidores, a menudo se utilizan antes para darles forma.

III. Responsabilidad penal de los intermediarios como forma de corregulación sobre los usuarios

La discusión de la responsabilidad intermediaria se planteó en primer lugar en el ámbito de la responsabilidad civil extracontractual por los daños que contenidos de los usuarios provocaban a terceros. Sin embargo, a partir del cambio de política pública de la década anterior han emergido diversas formas y casos de responsabilidad criminal de los intermediarios. Los casos más conocidos han sido los relacionados con la propiedad

[39] Pariser, E., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Books, New York, 2011.

intelectual en la jurisprudencia norteamericana y europea[40]. Sin embargo, en otras áreas también se ha desarrollado una expansión similar de la responsabilidad por los contenidos de los usuarios.

Estas situaciones tienen en común los siguientes rasgos:

i) Corresponden a situaciones identificadas como riesgos para las estructuras de control sobre las interacciones en la sociedad de la información. Los temas en los cuales se procura el uso de la capacidad normativa de los intermediarios son situaciones donde otros agentes sociales de control tradicionales fallan para resolver los vacíos normativos, de manera que son definidas como riesgos que exigen imponer responsabilidades urgentes[41], como aquellas responsabilidades de portería que se adjudican a los intermediarios de Internet, transformándoles en correguladores con los gobiernos respecto de los usuarios.
ii) El principal riesgo asociado con la red consiste en su ingobernabilidad, de manera que las actividades de control miran en primer lugar a establecer condiciones de ejercicio del control limitando el anonimato y la invisibilidad de los comportamientos de los usuarios[42].
iii) Las responsabilidades que recaen sobre los intermediarios se dirigen a crear una considerable orientación a ejercer funciones de policía sobre la red, obteniendo datos de los usuarios, conservándolos, entregándolos a las autoridades a la vez que los usan para sus propios fines. Se trata de labores de policía privada, informal, basada en la vigilancia continua (*low policing*)[43], y además muy efectiva debido a las propiedades de gobierno por diseño que tienen las capacidades normativas de los intermediarios. Gracias a estas características se ha organizado un sistema de corregulación de Internet cada vez más expansivo.
iv) Los efectos de las políticas de expansión de responsabilidad subyacentes a la situación de los intermediarios permiten a la vez técnicas de control sobre categorías completas de sujetos y su máxima individualización mediante el cruce de la información y la configuración de perfiles de los usuarios vigilados. Por lo demás, las técnicas de control (acumulación individualizada de información más criminalización selectiva) permiten limitar con mucha eficacia los riesgos tratados[44].

---

[40] Ver Farano, B., Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. ApproachesW, TTLF Working Paper Nº 14, Stanford-Vienna Transatlantic Technology Law Forum, 2012; Garrote, I., *Comparative Analysis on National Approaches to The Liability of Internet Intermediaries for Infringement of Copyright and Related Rights*, WIPO, Ginebra, 2013; Edwards, L., *Role and responsability of Internet Intermediaries in the Field of Copyright and related rights*, WIPO, Ginebra, 2011.

[41] Clear, T.; Cadora, E., "Risk and community practice", en Stenson, K.; Sullivan, R. (eds.), *Crime, Risk and Justice: The Politics of Crime Control in Liberal Democracies*, Willan Publishing, Cullompton 2001.

[42] Borja Jiménez, E., *Curso de Política Criminal,* Tirant Lo Blanch, Valencia, 2011, pp. 278 ss.

[43] Brodeur, J.-P., *The Policing Web*, Oxford University Press, Oxford, 2010, pp. 223 ss.

[44] Hudson, B., *Justice in the Risk Society. Challenging and Re-affirming Justice in Late Modernity*, Sage, London, 2003, p. 41.

v) Existe una ambivalencia fundamental en la política criminal aplicada a los riesgos de la sociedad de la información, cual es la simultaneidad del acceso y el control, de manera que ninguna política del control puede llevar a limitar de manera extrema la libertad del acceso, por ello los métodos de control de la responsabilidad intermediaria deben ser siempre reequilibrados con la libertad de los flujos de información.

A continuación observaremos las tensiones de la responsabilidad de los intermediarios y sus obligaciones como correguladores de los usuarios en los temas de vulneraciones a la privacidad, pornografía infantil y difamación.

a) *Privacidad*

Para revisar cómo ha evolucionado la aplicación de la responsabilidad de los intermediarios respecto de la privacidad, el caso más ilustrativo es el francés.

En Francia, para las cortes ha sido muy difícil trazar una línea divisoria entre las funciones editoriales y las de mero conductor de información. La ley francesa de Economía Digital, LCEN (loi pour la confiance dans l'économie numérique), sigue las excepciones europeas a la responsabilidad de los intermediarios. Sin embargo, en el caso de servicios de plataformas de la *web* 2.0[45] a menudo los tribunales han expandido la responsabilidad de los intermediarios.

En el caso *Dahan v. Duperri*, el tribunal de primera instancia de Nanterre condenó en 2008 al propietario de un agregador de noticias por invasión a la privacidad[46]. En el caso, un cineasta francés presentó una demanda contra el propietario del lespipoles.com por haber publicado un vínculo a un sitio *web* que contienía información acerca de la presunta relación del cineasta con la actriz Sharon Stone. El tribunal determinó que lespipoles.com había indicado diversas fuentes de información en su sitio *web*. Se encontró que el contenido disponible en el sitio *web* se compone de títulos de artículos, resúmenes y enlaces, como contenido que se trajo a la página *web* utilizando la tecnología Really Simple Syndication (RSS). Por haber suscrito el servicio RSS de una manera preestablecida y específica, el tribunal consideró a lespipole.com como editor.

En el caso *fuzz.fr*[47], en 2008 el tribunal de primera instancia de París decidió que el propietario de la página *web* Eric Dupin tenía una responsabilidad criminal por haber hecho una decisión editorial al publicar un *link* con una noticia del *blog* "elebrites-stars.blogspot.com" que invadía la privacidad del actor Oliver Martínez. Dicha noticia hacía

[45] Herrelson, W., *Filtering the Internet to Prevent Copyright Infringement: Part II - ISP Safe Harbors and Secondary Liability in the U.S. and France,* On line in: http://www.jdsupra.com/documents/045cf8b4-3388-412d-9322-e10395852ba8.pdf visto 01-09-2014.

[46] Tribunal de Grande Instance de Nanterre Ordonnance de Référé 28 Février 2008, Olivier Dahan v Eric Duperri.

[47] Tribunal de grande instance de Paris, ordonnance de re'fe're' rendue le 26 mars 2008, Olivier M. / Boobox Net

referencia a la relación sentimental de él con la cantante pop Kylie Minogue. Dicha decisión fue tomada, a pesar que dicho sitio se desempeñaba como un servicio de agregación de noticias –donde los usuarios pueden votar qué noticias son priorizadas– y obligó a Dupin pagar € 1.000 por infracción de privacidad del actor y € 1.500 adicionales en gastos legales. El Tribunal de Casación francés, sin embargo, en 2011 considerará a fuzz.fr y a otros dos sitios similares como sitios de alojamiento en términos de LCEN y por lo tanto no responsables por el contenido publicado en él.

Según el Informe de la Comisión de Reforma Australiana para la ley de privacidad (Australia Law Reform Commission)[48], en algunas circunstancias, un intermediario puede ser encontrado responsable para poseer la condición de intencionalidad después de haber sido notificado de una invasión de la privacidad. Se podría entonces encontrar que ha tenido la intención de invadir la privacidad, o que ha sido imprudente, si sabe el intermediario que su servicio ha sido utilizado por un tercero para invadir la privacidad de alguien, y esté en condiciones razonables para detener la invasión de la privacidad, pero no decide hacerlo.

Estas tendencias resultan paradojales, en el sentido que uno de los derechos más afectados con la imposición de obligaciones de portería[49] a los intermediarios es precisamente la privacidad. A partir de dichas obligaciones, los intermediarios se sienten obligados a vigilar activamente sus servicios en cuanto a los contenidos que circulan por ellos –que a su vez puede requerir vigilar ampliamente las actividades del usuario–. Para los intermediarios, especialmente para los ISP, la vigilancia del mal comportamiento requiere en términos generales la inspección de las comunicaciones de los usuarios. Por tanto, los intermediarios pueden decidir recoger más información de los usuarios y conservarla por mayor tiempo para facilitar las acciones legales contra los usuarios infractores y evitar responsabilidades. De esas formas se pueden socavar las expectativas razonables de privacidad que tengan los usuarios de Internet[50].

b) *Pornografía infantil*

A pesar del régimen de inmunidad creado por la Directiva Europea, la jurisprudencia y legislaciones nacionales europeas han puesto de manifiesto que ella no ha sido completamente seguida en la política de medidas estrictas que han sido impuestas por varias naciones europeas contra la pornografía infantil[51].

[48] ALRC, *Serious Invasions of Privacy in the Digital Era, Final Report*, ALRC Report Nº 123, 2014 Recomendation 11.103, p. 208.

[49] Ver más arriba la responsabilidad de portería o *gatekeeping*.

[50] CDT, *Shielding The Messengers: Protecting Platforms For Expression And Innovation,* CDT, Washington DC, 2012, p. 22.

[51] Anchayil, A.; Mattamana, A., "Intermediary Liability And Child Pornography: A Comparative Analysis", en *Journal of International Commercial Law and Technology* Vol. 5, Issue 1, 2010, 48-57, p. 53.

En Alemania la Teledienstgesetz de 1996 estableció deberes para los intermediarios de Internet, haciéndolos responsables de los contenidos ajenos en cuanto tuvieran la capacidad técnica para evitarlos y sea exigible hacerlo.

El caso *CompuServe* en Alemania abrió precisamente las posibilidades de persecución criminal de los intermediarios por difusión de contenidos de pornografía infantil en sus redes. En 1997, el gerente general de Compuserve fue declarado culpable de asistir a la difusión de material de pornografía infantil y otros contenidos ilegales con los grupos de discusión de Usernet, debido a que tenía pleno conocimiento de esos contenidos y deliberadamente no los bloqueó para obtener ventaja económica de su difusión, según sostuvo el juez[52]. Este caso, pese a no ser un precedente en sentido estricto, ha marcado el enfoque germano respecto de los deberes de los intermediarios frente a contenidos ilegales como la pornografía infantil[53].

En el caso de EE.UU. en 1998 se puso en vigor la Child Online Protection Act (COPA) que criminalizaba todas las transmisiones de pornografía infantil. En un caso acerca de la constitucionalidad de esa ley, el caso *Ashcroft vs. ACLU*[54], la Corte Suprema sostuvo que, incluso sin un mandato, fomentando el uso de *software* de filtrado en las escuelas y bibliotecas (por medio de la Ley de Protección de Niños en Internet) y alentando a los padres a utilizar dicho *software*, el Congreso habría podido lograr el mismo objetivo de evitar que los niños tengan acceso a material dañino. De esa manera, la corte determinó que el estatuto violaba la primera enmienda, habiendo alternativas menos restrictivas que la COPA, como el bloqueo y el *software* de filtrado. Con estas herramientas los adultos sin hijos pueden tener acceso a información que tienen el derecho de ver sin tener que identificarse y los adultos con niños pueden apagar sus filtros para acceder a material que desean ver.

En Sudáfrica, en virtud de la Ley de Cine y Publicaciones (Ley Nº 65 de 1996), los intermediarios de Internet pueden ser hechos responsables por el contenido en sus redes que ha sido censurado, o no se clasifica por el Consejo de Cine y Publicaciones. La Ley de Cine y Publicaciones (FPA) requiere que "Cualquier persona que distribuya, transmita o muestre cualquier película o juego" se inscriba en la Junta de Cine y Publicaciones (FPB) como distribuidor o exhibidor de películas o juegos, lo que incluye a los intermediarios e incluso a los cibercafés. De otra manera se configura un delito que está sancionado con una multa o hasta seis meses de prisión, o ambas. Cuando se exhiban películas –o incluso cuando se haga publicidad a ellas– que tengan escenas de ponografía infantil, la sanción puede incrementarse hasta 5 años. Adicionalmente, la reforma de 2009 (Film and Publications Amendment Act, Ley 3 de 2009) ha establecido para los intermediarios que provean servicios orientados a los niños que moderen y monitoreen sus servicios para asegurar que ellos no están siendo usados para cometer ofensas o abusos contra los niños.

---

[52] Amtsgericht Munich, File No.: 8340 Ds 465 Js 173158/95.

[53] Holznagel, B., "Responsibility for Harmful and Illegal Content as well as Free Speech on the Internet in the United States of America and Germany". Paper at Max Planck Institut für kollektive Güter, 2013.

[54] Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002).

Para sus críticos, este régimen parece equivaler a una obligación de supervisión onerosa y potencialmente muy costosa para los intermediarios, abarcando a todos ellos, incluyendo a los proveedores de contenido y los sitios de redes sociales, con un efecto portencial perverso en la libertad de expresión[55].

En EE.UU., el 23 de julio de 2013, 43 fiscales generales estatales recientemente propusieron una enmienda a la Communications Decency Act (CDA) que permita la persecución penal de las empresas y sus ejecutivos por las leyes estatales penales que han sido vulneradas por sus usuarios[56].

La propuesta enmendaría la Sección 230 (e) (1) de la CDA de la siguiente manera: "Nada en esta sección se interpretará en menoscabo del cumplimiento de [las disposiciones específicas de la ley Federal] o cualquier otra ley penal federal o estatal". La razón de esta modificación consiste en frustrar los anuncios de prostitución *on line*, esto impondría responsabilidad de los intermediarios en varias leyes penales estatales, incluyendo también (en la mayoría de los estados) difamación y abusos contra la privacidad.

c) *Difamación*

En un caso reciente sobre difamación, *Sara Jones v. Dirty World Entertainment*[57], se decidió en primera instancia que el intermediario no gozaba de inmunidad debido a que sus acciones cosntituyeron una creación o desarrollo de información y así se convertía en un proveedor de contenidos. El 16 de junio de 2014, el Sexto Circuito de Apelación anuló la decisión del tribunal del distrito favoreciendo al intermediairo Dirty World.

En general la práctica judicial norteamericana ha confirmado a las redes sociales como protegidas por la inmunidad por contenidos difamatorios que sus usuarios viertan en sus sitios[58, 59].

Sin embargo, en las redes sociales los daños que se pueden producir a la reputación de una persona son mucho más graves y mucho más diversos que los que se pueden producir en otras plataformas. Pese al gran volumen de información que manejan, estos pueden administrarla en gran medida por la capacidad de automatizar las búsquedas y filtros mediante algoritmos y codificaciones[60].

En cuanto a los sitios de *blogs*, en cambio, ha existido una clara expansión de la responsabilidad penal. En el caso *Payam Tamiz v. Google Inc.* de 2013[61], se indicó claramente

[55] Comninos, A., "Intermediary Liability in South Africa", Association for Progressive Communications, Intermediary Liability in Africa Research Papers, Nº 3, 2012.

[56] https://www.eff.org/sites/default/files/cda-ag-letter.pdf visto 15-07-2014.

[57] Sarah Jones v. Dirty World Entertainment Records LLC, Dist. Court Kentucky 2011.

[58] Guo, R. "Stranger Danger and the Online Social Network", en *Berkeley Technology. Law Journal,* Vol. 23, Issue 1, 2008, 618-644.

[59] Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007), affd 528 F.3d 413 (5th Cir. 2008); Doe v. SexSearch, 502 F. Supp. 2d 719 (N.D. Ohio 2007).

[60] Monaghan, J., "Social Networking Websites' Liability For User Illegality", **en** *Seton Hall Journal of Sports and Entertainment Law,* Vol. 21, Nº 2, 499-532, p. 516.

[61] Payam Tamiz v Google Inc [2013] EWCA Civ 68.

que si los proveedores de servicios en línea no bajan de inmediato el contenido que es presuntamente difamatorio, pueden ser hechos responsables por él. En el caso de Payam Tamiz, un político conservador inglés, este demandó a Google Inc. y a Google UK por comentarios difamatorios anónimos en un *blog* creado en la plataforma Blogger de Google llamado "London Musulman". En la Corte de Apelación se sostuvo que una vez que Google había sido notificada de contenido presuntamente difamatorio, se convirtió en una "editora por aquiescencia" y por lo tanto puede ser considerada responsable por no eliminar el contenido. El papel de Google en la operación de su plataforma Blogger no es puramente pasivo, ya que proporciona herramientas de diseño, un URL, anuncios, servicios en términos de su elección y puede eliminar o bloquear el acceso a cualquier *blog*.

En Brasil, en el caso de 2011, el Tribunal de la 19ª cámara de Rio de Janeiro condenó a Google Brasil a pagar daños a un menor de 13 años que había sido difamado por comentarios en la red social Orkut durante el 2008 en la comunidad "Eu odeio Pedro". La Corte condenó a Google indemnizar al menor por cada día que los contenidos hayan permanecido *on line* y ordenó a la empresa evitar el posteo de contenidos similares en el futuro.[62] La ditación de la ley de marco civil de Internet, Ley 12.965, de 23 de abril de 2014, busca precisamente poner un dique a esta jurisprudencia, al menos en cuanto a los daños civiles, reforzando las inmunidades de los intermediarios por los contenidos de sus usuarios.

En India, la Ley sobre Tecnología de la Información (IT Act de 2000) implica varias posibilidades de responsabilidad para los intermediarios, sobre todo por las posteriores directrices que la desarrollan, especialmente las directrices de 2011 para los intermediarios, que los guían cómo cumplir con las diversas interpretaciones de la ley respecto del acceso a los contenidos y los contenidos generados por los usuarios. Pese a que un régimen de excepciones de responsabilidad similar al europeo fue introducido en una reforma a dicha ley en 2008, en muchos casos se ha expandido la responsabilidad penal de los intermediarios por actos de sus usuarios.

Según las directrices de 2011, cuando los intermediarios reciben de una parte agraviada por un contenido en sus redes el reporte de la posible ofensa, tienen un plazo de 36 horas para reaccionar, tomando la decisión si el reclamo tiene una base legal. La mayor parte de las veces el contenido es removido sin mayor cuestionamiento[63].

En el caso del blogero Indijobs en 2012[64], este publicaba en hubpages.com relativo a el gurú Nirmal Baba, llamándolo de "estrella del fraude", entre otras cosas. Uno de los seguidores del gurú notificó a hubpages.com de los comentarios, solicitando su eliminación, pero hubpages.com se negó a retirar dicho contenido y aconseja ponerse en contacto con el bloguero directamente, sin estar dispuestos a proporcionar información de contacto en ausencia de una notificación judicial. Al no eliminar el contenido, hubpages.com cayó en la situación de responsabilidad según las referidas directrices de

[62] Processo Nº 0048941-58.2009.8.19.0002

[63] Global Network Initiative, *Closing the Gap - India On line Intermediaries and a Liability System not yet fit for the purpose*, Copenhagen: Copenhagen Economics, 2014, p. 19.

[64] Nirmaljit Singh Narula vs Indijobs At Hubpages.Com, Delhi High Court, CS (OS) No.871/2012.

2011, de manera que la Corte de Delhi levantó la inmunidad del intermediario y consideró su acción como control editorial sobre los contenidos. Adicionalmente, ordenó a hubpages.com monitorear los posteos de sus blogueros para evitar cualquier forma de difamación en el futuro contra el gurú Nirmal Baba[65].

IV. Conclusiones

Los cambios en los roles de los intermediarios han interactuado con la expansión de la aplicación de los regímenes de responsabilidad a los intermediarios de Internet. Estos regímenes buscan resolver varios problemas normativos que corresponden a los riesgos que son percibidos para la gobernanza de la sociedad de la información. Para la gestión de dichos riesgos, los gobiernos han implementado políticas que hacen que los intermediarios, debido a sus capacidades normativas, ejerzan actividades de policía informal y privada sobre los comportamientos de los usuarios considerados riesgosos.

En los casos de invasión a la privacidad, persecución de la pornografía infantil y de la difamación *on line*, han mostrado cómo, mediante la aplicación de formas de responsabilidad más severas –involucrando al derecho penal–, a la vez se sujetan los nuevos roles de los intermediarios (agregación de noticias, reproducción de vínculos, subscripción de RSS, puesta a disposición de plataformas para blogueros, entre otras) a disciplinas más estrictas que exigen labores de monitoreo o *low policing* de los contenidos que los usuarios ponen en circulación en sus redes.

Pese a que hay un esfuerzo en muchos casos judiciales y desarrollos legislativos por evitar que esos cambios se reequilibren en las democracias con los derechos fundamentales de privacidad y libertad de expresión, manteniendo el carácter libre y abierto del acceso a las redes, esos esquemas someten a control a riesgos percibidos como urgentes para las formas de gobernanza de la sociedad de la información, limitando ese acceso.

En los años venideros veremos cómo en el mundo, y también en nuestro país, estos desarrollos globales continuarán incrementando las tensiones entre acceso y control, usando dentro de otros mecanismos a la responsabilidad penal y sus límites mediante el sistema de derechos fundamentales que se ponen en juego en dichos casos.

Bibliografía

Anchayil, A.; Mattamana, A., "Intermediary Liability And Child Pornography: A Comparative Analysis", en *Journal of International Commercial Law and Technology* Vol. 5, Issue 1, 2010, 48-57.

Article 19, *Internet Intermediaries: Dilemma of Liability*, Article 19, London, 2013.

[65] Wu, T., "Shooting the Messenger? Intermediary Liability in Southeast Asian Cyberspace", Asia Pacific Foundation of Canada, http://www.asiapacific.ca/thenationalconversationonasia/*blog*/shooting-messenger-intermediary-liability-southeast-asian-cy visto 10-08-2014.

BAYER, J., *Liability of Internet Service Providers for Third Party Content*, Victoria University of Wellington, Wellington, 2008.

BORJA Jiménez, E., *Curso de Política Criminal,* Tirant lo Blanch, Valencia, 2011.

BRODEUR, J.-P., *The Policing Web*, Oxford University Press, Oxford, 2010.

CDT, *Shielding The Messengers: Protecting Platforms For Expression And Innovation,* CDT, Washington DC, 2012.

BROWN, I.; Mardsden, C., *Regulating Code, Good Governance and better regulation in the information age,* The MIT Press, Cambridge & London, 2013.

CLEAR, T.; Cadora, E., "Risk and community practice", en Stenson, K.; Sullivan, R. (eds.), *Crime, Risk and Justice: The Politics of Crime Control in Liberal Democracies*, Willan Publishing, Cullompton, 2001.

COATES, K., *Competition Law and Regulation of Technology Markets.* Oxford University Press, New York, 2011.

COMNINOS, A., "Intermediary Liability in South Africa", Association for Progressive Communications, Intermediary Liability in Africa Research Papers, Nº 3, 2012.

DE BEER, J.; Clemmer, C., "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?", en *Jurimetrics Journal,* Nº 49, 2009, 375-409.

EDWARDS, L., *Role and responsability of Internet Intermediaries in the Field of Copyright and related rights,* WIPO, Ginebra, 2011.

ELKIN-KOREN, N., "After Twenty Years: Copyright Liability of Online Intermediaries", en Frankel, S.; Gervais, D. (eds), *The Evolution and Equilibrium of Copyright in the Digital Age*, Cambridge University Press, Cambdrige, 2014.

FARANO, B., "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches", TTLF Working Paper Nº 14, Stanford-Vienna Transatlantic Technology Law Forum, 2012.

GARROTE, I., *Comparative Analysis on National Approaches to The Liability of Internet Intermediaries for Infringement of Copyright and Related Rights*, WIPO, Ginebra, 2013.

GLOBAL Network Initiative, *Closing the Gap - India On line Intermediaries and a Liability System not yet fit for the purpose*, Copenhagen: Copenhagen Economics, 2014.

GOLDSMITH, J.; Wu, T., *Wo Controls the Internet?: Illusions of a Borderless World: Illusions of a borderless world,* Oxford University Press, Oxford, 2006.

GUO, R. "Stranger Danger and the Online Social Network", en *Berkeley Technology. Law Journal,* Vol. 23, Issue 1, 2008, 618-644.

HERRELSON, W., *Filtering the Internet to Prevent Copyright Infringement: Part II - ISP Safe Harbors and Secondary Liability in the U.S. and France,* On line in: http://www.jdsupra.com/documents/045cf8b4-3388-412d-9322-e10395852ba8.pdf visto 01-09-2014.

HOLZNAGEL, B., "Responsibility for Harmful and Illegal Content as well as Free Speech on the Internet in the United States of America and Germany". Paper at Max Planck Institut für kollektive Güter, 2013.

HUDSON, B.,*Justice in the Risk Society. Challenging and Re-affirming Justice in Late Modernity*, Sage, London, 2003.

JOHNSON, D.; Post, D., "Law and Borders - The Rise of Law in Cyberspace", en *Stanford Law Review,* Vol. 48, Nº 5, 1996, 1367-1402.

JOHNSON, D,; Post, D., "And How Shall the Net be Governed? A Meditation on the relative virtues of decentralized, emergent law", en Kahin, B.; Keller, J.(Eds.), *Coordinating The Internet*, The MIT Press, Boston, 1997, 62-91.

KLEINSCHMIDT, B., "An International Comparison of ISP's Liabilities for Unlawful Third Party Content", en *International Journal of Law and Information Technology,* Vol. 18, Nº 4, 2010, 332-355.

Lessig, L., *Code and other Laws of Cyberspace, V. 2.0.* Basic Books, New York, 2006.

Mann, R.; Belzley, S, "The Promise of Internet Intermediary Liability", en *William and Mary Law Review*, Vol. 47, 2005, 239-307.

Marsden, C., *Internet Co-Regulation European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge, 2011.

Mefford, A., "Lex Informatica: Foundations of Law on the Internet*",* en *Indiana Journal of Global Legal Studies,* Vol. 5, Issue 1, 1997, 211-237.

Monaghan, J., "Social Networking Websites' Liability For User Illegality", en *Seton Hall Journal of Sports and Entertainment Law,* Vol. 21, Nº 2, 499-532.

Muñoz Machado, S.*, La Regulación de la Red, Poder y Derecho en Internet*, Taurus, Madrid, 2000.

OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing, París, 2011.

Ofcom, *Online protection: a survey of consumer, industry and regulatory mechanisms and systems*, 2006, p. 12, On line in: http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/onlineprotection visto 15-09-2014.

Palfrey, J., "Four Phases of Internet Regulation". Harvard Law School Public Law & Legal Theory Working Paper Series Paper Nº 10-42, 2010.

Pariser, E., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Books, New York, 2011.

Pattberg, Ph., "The institutionalization of private governance: How Business and nonprofit organizations agree on transnational rules", En *Governance: An International Journal of Policy, Administration and Institutions* Nº 18, 2005, 589-610.

Peguera, M., *Mensajes y Mensajeros en Internet: La responsabilidad civil de los proveedores de servicios intermediarios,* UOC, Barcelona, 2001.

Reidenberg, J, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", en *Texas Law Review,* Vol. 76, Nº 3, 1998, 553-593.

Rowland, D.; Kohl, U.; Charlesworth, A., *Information Technology Law,* Routledge, London, Fourth Edition, 2012.

Seng, D., *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, WIPO, Ginebra, 2010.

Solum, L.; Chung, M., "The Layers Principle: Internet Achitecture and theLaw", en *Notre Dame Law Review,* Vol. 79, Nº 3, 2004, 815-948.

Trudel, P., "La Lex Electronica", en Morand, Ch. (dir.), *Le droit saisi par la mondialisation*. Éditions Bruylant, Bruxelle, 2002, 221-268.

Weinrib, E., "Restitutionary Damages as Corrective Justice", en *Theoretical Inquiries in Law*, Vol. 1, Nº 1, 2000.

Weinrib, E., *Corrective justice*, Oxford University Press, Oxford, 2012.

Weiser, Ph., "The Future of Internet Regulation", Legal studies research paper series Working, Paper Number 09-02, University of Colorado Law School, February 2, 2009.

Wu, T., "Cyberspace Sovereignty? - The Internet and the International System", en *Harvard Journal of Law & Technology,* Vol. 10, Nº 3, summer 1997, 647-666.

Wu, T., *The Master Switch: The Rise and Fall of Information Empires*, Vintage Books, New York, 2010.

Wu, T., "Shooting the Messenger? Intermediary Liability in Southeast Asian Cyberspace", Asia Pacific Foundation of Canada, http://www.asiapacific.ca/thenationalconversationonasia/*blog*/shooting-messenger-intermediary-liability-southeast-asian-cy visto 10-08-2014.