Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital

Documento producido por la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, Argentina.[1]

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador del iLei en el CELE. La investigación y elaboración del documento fue dirigida y contó con los comentarios de Eduardo Bertoni, director del CELE. Cortés es abogado de la Universidad de Los Andes, Colombia, con maestría en 'Gobernanza de Medios' del London School of Economics.

Resumen

El objetivo de este documento es ofrecer un sustento teórico y un contexto mínimo para el debate sobre la responsabilidad de los intermediarios en Internet con énfasis en los problemas relacionados con contenidos.

El primer capítulo explica el fundamento teórico general sobre los intermediarios y su relación con la responsabilidad civil. Allí se explica la importancia del balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de guardián.

Posteriormente se describen los antecedentes que llevaron a los intermediarios en Internet a convertirse en guardianes de los usuarios. Una vez desmontado el argumento de la imposibilidad tecnológica –explica el documento– quedó claro que el Prestador de Servicios de Internet estaba llamado a ejercer el rol de guardián de los usuarios.

El tercer capítulo se refiere a los tipos de guardianes y sus deberes, haciendo énfasis en los modelos más comunes. Ninguna de las leyes sobre responsabilidad de intermediarios ha establecido un régimen de responsabilidad objetiva. Las leyes varían entre lo que se conoce como una inmunidad total o una inmunidad condicionada.

En seguida se hace un breve análisis de lo que se avizora en el horizonte en este tema. Algunos autores consideran que en el futuro los intermediarios usarán cada vez más el filtrado de contenidos como estrategia para ejercer su papel como guardianes. Y siguiendo la idea de que así como la tecnología puede restringir el entorno digital lo puede fortalecer, se recomienda explorar soluciones tecnológicas para equilibrar el debate en Internet.

Por último, y a partir de lo expuesto, el documento hace las siguientes recomendaciones:

- Es importante considerar el balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de ama de llaves. Un desequilibrio entre éstos implica una estrategia fallida que además impacta negativamente en actividades socialmente deseables y afecta derechos fundamentales como el debido proceso y la libertad de expresión.
- Establecer un régimen de responsabilidad objetiva para los intermediarios de Internet resulta inadecuado. Por un lado, implica imponerle obligaciones difusas a éstos, más allá de las que realmente podrían cumplir. Por el otro, se traduciría en mayores restricciones para los usuarios de Internet, en contravía de derechos y garantías fundamentales. Las decisiones judiciales en Argentina ilustran el problema de que el intermediario esté obligado a hacer juicios de valor sobre la legalidad de las acciones del usuario.
- La inmunidad condicionada parece adecuada como régimen de responsabilidad cuando establece incentivos razonables para el guardián. Es decir, cuando no le impone deberes difusos o desproporcionados de monitoreo y vigilancia. Sin embargo, en algunos modelos de inmunidad condicionada –como el del DMCA de Estados Unidos– los costos que no asume el intermediario

terminan en cabeza de los usuarios y la comunidad en general. En este caso los costos son vulneraciones a derechos como la libertad de expresión y el debido proceso.

- En esos términos, y sin subestimar el problema del contenido agresivo y difamatorio que pulula en la red, una inmunidad condicionada en materia de responsabilidad de intermediarios por contenidos de sus usuarios podría implicar, en la práctica, la derogación de la libertad de expresión y el debido proceso en Internet.
- Los debates sobre la responsabilidad de los intermediarios deben prestarle atención a la práctica del filtrado de contenidos, que aparece en el horizonte como una estrategia invisible para que el amo de llaves ejerza la guardia. Esto implica, de paso, empezar a mirar las condiciones que acepta el usuario cuando adhiere a los términos de referencia del servicio.
- Vale la pena explorar la idea de implementar soluciones tecnológicas –en todas sus versiones– para enfrentar los contenidos difamatorios que abundan en Internet. Particularmente, es posible pensar en adaptar un derecho de réplica a diferentes tipos de servicios y plataformas.

Introducción

En un día cualquiera frente al computador usamos, al menos, dos servicios que nos presta alguna empresa –nacional o extranjera–: el de la conexión a la red y el del correo electrónico. Pero por supuesto el número es mayor: entramos a algún portal de información; miramos las actualizaciones en Facebook; recomendamos un artículo por Twitter; buscamos información en Google; comentamos un blog; miramos libros en Amazon; oímos música en Spotify o Lastfm… La lista es interminable.

Estas empresas –los intermediarios– no solo hacen posible nuestra actividad en línea sino que también la moldean. Para algunos servicios necesitamos clave, para otros debemos pagar, en algunos podemos escribir extensamente, en otros solo unas cuantas palabras. De manera creciente el espacio abre más posibilidades y a la vez está sujeto a mayores reglas y obstáculos.

A medida que esa vida digital se expande, tanto el Estado como las empresas incrementan su interés por controlar nuestra actividad en línea y prevenir hechos indeseados. Los contextos sociales se trasladan a Internet. Algunos problemas, como la piratería, parecen magnificados y otros, como la pornografía infantil, revisten gravedad.

En medio de esta situación de evolución y cambio, de tensiones y agendas opuestas, los Estados vienen diseñando fórmulas para que los intermediarios en Internet respondan por los posibles delitos cometidos por sus usuarios. Y en medio de esa agenda de regulación y órdenes judiciales, derechos como la libertad de expresión o el debido proceso parecen quedar en paréntesis.

El objetivo de este documento es ofrecer un sustento teórico y un contexto mínimo para el debate sobre la responsabilidad de los intermediarios en Internet con énfasis en los problemas relacionados con contenidos. Con esa idea en mente, no encontrarán acá un estudio comparativo de los regímenes existentes ni un análisis meramente jurídico. El objetivo es trazar puentes disciplinarios y abstraer los elementos más relevantes del tema para identificar problemas y ofrecer algunos puntos de análisis.

El documento está divido de la siguiente manera: el primer capítulo explica el fundamento teórico sobre los intermediarios y su relación con la responsabilidad civil; el segundo describe los antecedentes generales que llevaron a los intermediarios en Internet a convertirse en guardianes de los usuarios; el tercero explica los tipos de guardianes y sus deberes, haciendo énfasis en los modelos más comunes; el cuarto da cuenta de lo que viene más adelante, incluyendo la discusión sobre una propuesta de solución tecnológica, y, finalmente, el quinto capítulo hace un breve recuento y deja unas conclusiones.

I. Fundamentos de la responsabilidad de los intermediarios

1. La teoría del guardián o ama de llaves

La mayoría de nuestras actividades están mediadas por personas, instituciones y espacios privados que posibilitan y a la vez definen la manera en que las desarrollamos. El empleado de la aerolínea es el encargado de validar nuestros documentos para subirnos a un avión comercial, y solo a través de este servicio podemos viajar a otro país; la médica es quien nos entrega una autorización para adquirir un medicamento, y solo en ciertos lugares –farmacias y droguerías– podemos adquirirlo; el cajero del banco recibe un dinero que queremos girar al extranjero, y solo a través de este servicio –u otros semejantes– podemos hacer que llegue a su destino.

Esta interacción e interdependencia con actores privados es de especial interés para el Estado. En muchas ocasiones es más fácil para el regulador influir en la conducta del individuo a través de esos terceros que de manera directa. Así, le resulta más fácil al Estado que la aerolínea verifique si tenemos una visa vigente o que el banco cobre un impuesto por el dinero que enviamos al extranjero. Esta estrategia es conocida como teoría de intermediarios, amas de llaves o guardianes.

Según Emily Laidlaw, los guardianes o *gatekeepers* son agentes no estatales con la capacidad de alterar la conducta de terceros en circunstancias en que el Estado difícilmente puede hacerlo.[1] Usualmente al guardián le es indiferente la conducta que el Estado busca controlar, sin embargo, por los recursos, la información o la autoridad que posee, está en una posición ideal para regularla. Julia Black lo llama 'regulación descentralizada', donde el núcleo de la actividad reguladora se mueve del Estado a espacios privados.[2]

Por mandato legal, los guardianes o amos de llaves controlan entonces el acceso a un servicio o insumo: la médica emite la fórmula para que el paciente no abuse del uso de un medicamento; la aerolínea bloquea el paso a inmigrantes ilegales a través de su servicio; el tendero sólo vende cigarrillos a mayores de edad. En todos los casos hay una actividad legalmente indeseable que el intermediario previene o controla. *"Este respaldo, usualmente en la forma de un bien especializado o una forma de certificación esencial para que la irregularidad prospere, es la 'compuerta' que el guardián vigila*", explica Reinier Kraakman.[3]

Algunos intermediarios son guardianes por la naturaleza misma del servicio o el insumo que prestan. Por ejemplo, la aerolínea es un paso obligado para quien quiere viajar en avión (a menos que usted sea Carlos Slim y tenga uno propio) y, hablando específicamente de Internet, la empresa que

[1] Cfr. Laidlaw, E. A framework for identifying Internet information gatekeepers. International Review of Law, Computers and Technology, 24:3, p. 264.
[2] Cfr. Ibidem, p. 264.
[3] Cfr. Kraakman, R. Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy. Yale Law School. Journal of Law, Economics and Organization. II:1, 1986 p. 54.

provee la conexión es un paso obligado para que podamos acceder a la red. Por el contrario, otros agentes se vuelven guardianes por creación legal. Es el caso del médico que se vuelve un guardián virtual y ejerce como punto de control entre el paciente y el acceso a los medicamentos.

El uso de intermediarios para regular ciertos comportamientos surge como alternativa frente a las limitaciones o riesgos de la intervención estatal directa sobre el ciudadano. Por un lado, al Estado le resulta imposible o demasiado dispendioso desincentivar o castigar cierta conducta –el abuso de una droga, la inmigración ilegal– enjuiciando a cada persona de manera individual. Por el otro, la imposición de penas altas para desestimular dicha conducta puede tener un efecto desproporcionado frente a personas que no están incurriendo en ella pero temen el castigo por cuenta de un error propio o de una aplicación equivocada de la ley.[4] En otras palabras, controlar el acceso a un medicamento o impedir la inmigración ilegal no puede desembocar en que la gente prefiera no adquirir un medicamento o dejar de viajar al extranjero.

Decíamos que al guardián generalmente no lo afecta la posible conducta irregular del individuo. Para la médica puede resultar indiferente que el paciente compre drogas no prescritas; para la aerolínea puede ser irrelevante que el pasajero no tenga una visa válida; al prestador del servicio de Internet no lo afecta que un usuario descargue música ilegal. Es bajo ese presupuesto, entonces, que la estrategia de usar guardianes o amas de llaves debe incluir incentivos legales para que los intermediarios colaboren. Y la mejor manera es haciéndolos responsables legalmente por la conducta indeseada del tercero, a menos que asuman ciertas obligaciones. Este diseño regulatorio se traduce en mecanismos y obligaciones concretas que le permitan al guardián detectar la conducta o el riesgo, bien sea para prevenir que suceda del todo o para minimizar su ocurrencia.

Las obligaciones que asume el guardián dependen en gran medida de qué tipo de rol tiene. La teoría se refiere, en general, a dos tipos de guardianes: el 'bouncer' y el chaperón. El 'bouncer' –siguiendo la figura del empleado que controla la entrada a la discoteca– simplemente se niega a proveer el servicio o autorizar el acceso; el 'chaperón', por su parte, establece una relación con el tercero y lo acompaña y lo vigila para que no incurra en la acción indeseada.[5] Y mientras el 'bouncer' tiene que tomar decisiones entre lo que es y no es aceptable –situaciones de sí o no, de blanco o negro–, el chaperón tiene una misión más compleja: al desarrollar una relación con el sujeto y al estar prestándole un servicio, debe monitorearlo y a la vez influir en su conducta.

Es fundamental considerar el balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de guardián –como 'bouncer' o chaperón–. Un desequilibrio entre unos y otros implica una estrategia fallida de amo de llaves, lo cual impacta negativamente a terceros e inhibe actividades socialmente deseables. Kraakman distingue cuatro factores clave para instaurar un esquema de guardianes o amas de llaves:[6]

[4] Cfr. Ibidem, p. 57.
[5] Cfr. Zittrain, Jonathan. A History of Online Gatekeeping. Harvard Journal of Law & Technology. Volume 19, No. 2, Spring 2006, p. 253-298.
[6] Cfr. Op. Cit. Kraakman, p. 61.

i) Existe una conducta indeseada que no se logra disuadir a través de las sanciones existentes. Éste es el punto de partida. Como ya se señaló, la idea del Estado de usar intermediarios pasa por el análisis previo de la conveniencia para el fin propuesto. Si existen mejores alternativas a través de las sanciones existentes y del poder directo del Estado, el uso de guardianes es una estrategia equivocada.

ii) No hay incentivos privados suficientes para que los guardianes intenten controlar o detener dicha conducta. Si al intermediario le conviene controlar la conducta, la mejor alternativa para el Estado puede ser abstenerse de intervenir en la relación entre aquel y el ciudadano. Por ejemplo, a un centro comercial le conviene que sus almacenes no vendan productos robados o que las zonas comunes sean seguras para los visitantes. Instaurar un incentivo legal para obligar a que el centro comercial controle ambos frentes puede ser innecesario y, al contrario, puede generar costos que antes no existían.

iii) Existen intermediarios que pueden prevenir la conducta indeseada de manera confiable sin importar qué alternativas hay en el mercado para los infractores. El uso de guardianes tiene sentido si éstos pueden prevenir o controlar la conducta en una escala y medida razonable. Al contrario, no parece adecuada como política pública si, a pesar de algunas amas de llaves rigurosas, la conducta indeseada se lleva a cabo por otras vías –mediante intermediarios flexibles o mercados negros ampliamente disponibles–. De ser así, el efecto negativo es múltiple: el intermediario incurre en costos ineficientes, sólo los asume el ciudadano que no desea incurrir en la conducta indeseada, y ésta no se ve afectada (aún peor, los más interesados en perpetrarla serán los primeros en buscar alternativas). Como contra-argumento puede decirse que tener algunos intermediarios ejerciendo como guardianes sirve para mover la conducta a espacios marginales y, por lo tanto, para desalentar la conducta en el grueso de la población.

iv) Los costos para inducir a los intermediarios a que colaboren son razonables. Éste último punto está relacionado con todos los anteriores. Si partimos del supuesto de que al intermediario le es indiferente que el ciudadano incurra en la actividad indeseada, los costos que éste debe asumir deben ser razonables para que colabore con el Estado. Por supuesto, el Estado puede ejercer su poder punitivo contra un intermediario –en el fondo el incentivo no es otra cosa que una amenaza de sanción legal–. Pero el problema radica en que ante costos muy altos el intermediario optará por no prestar el servicio (así como un futuro intermediario preferirá no aventurarse a ofrecerlo del todo), o lo hará en condiciones deficiente o demasiado gravosas para el beneficiario. En esos términos, la estrategia de ama de llaves podrá lograr el control de una actividad indeseada, pero acabará por afectar otras necesarias y, a la postre, tal vez más importantes.

La teoría sobre guardianes o amos de llaves también aparece, entre otros, en los estudios académicos sobre medios masivos de comunicación. En ese contexto, el rol central de los medios en la sociedad

consiste en *"escoger y moldear un sinnúmero de pedazos de información para volverlos un número limitado de mensajes que llegan a la gente diariamente"*.[7] En ese proceso, el medio es el intermediario principal –el guardián de lo que entra o queda fuera del debate público–.

Basándose tanto en esta aproximación como en la general, Barzilai-Nahon considera que la teoría sobre guardianes tiene unas características propias en Internet. En un contexto interconectado, con nodos y relaciones dispares, el principal rol del guardián –paralelo al ejercicio de su servicio– es controlar el flujo de información. Este rol abarca tres objetivos: amurallar al usuario (o 'encerrado') en la red del guardián, ejercer la guardia para evitar que agentes externos al entorno cerrado atraviesen el portón, y mantener sin sobresaltos la actividad permitida dentro de la red.[8]

2. La responsabilidad civil

La doctrina sobre responsabilidad civil extracontractual –similar al *tort* en países de *common law*– también ha sido propuesta para resolver el vacío sobre la responsabilidad de los intermediarios de Internet frente a los hechos cometidos por sus usuarios. En la medida en que se trata de un riesgo legal que genera un incentivo para controlar una actividad indeseada, tiene alguna relación con la teoría del guardián. El planteamiento básico es el siguiente: un intermediario puede llegar a ser responsable bien sea por los daños que cause un usuario o porque gracias al servicio que aquel presta fue que se produjo y potenció el daño.

Tomemos un ejemplo: a través de Twitter una persona difunde rumores falsos sobre otra, por cuenta de los cuales ésta última pierde su trabajo y la posibilidad inminente que tenía de hacer un negocio. Bajo un análisis general de responsabilidad civil, la persona afectada podría iniciar una acción judicial contra Twitter para buscar que se le repare el daño. En ese caso, tendría que probar ante el juez que efectivamente el daño existió, que hay un nexo causal entre ese daño y la actuación de Twitter, y que Twitter fue negligente a la hora de evitarlo.

Más allá de que bajo este análisis el intermediario puede terminar respondiendo por la actuación de sus usuarios, éste sería el enfoque menos gravoso para Twitter, ya que implica demostrar que estuvo involucrado directamente en el hecho indeseado. Sin embargo, dentro del mismo régimen de responsabilidad civil se han propuesto alternativas que pueden hacer más exigente el deber del intermediario: la responsabilidad por el hecho de otro y la actividad peligrosa.

Por regla general, una persona debe responder legalmente por los daños que cause. Dependiendo de la gravedad de la conducta, la persona puede estar obligada a resarcir económicamente al afectado e, incluso, puede estar sujeta a una sanción penal. Es lo que acabamos de ilustrar. No obstante, una persona también puede ser responsable por los hechos de otra persona o un

[7] Shoemaker, P. Gatekeeping Theory. Routledge, 2009, introducción (traducción informal).
[8] Barzalai-Nahon, K. Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control. Journal of the American Society for Information, Science and Technology, 59(9), 2009, p. 1493-1512.

objeto a su cargo. Es el caso, por ejemplo, del daño causado por un hijo o una mascota, y se conoce como responsabilidad por el hecho de otro.[9]

En este renglón de la responsabilidad civil, y siguiendo con el ejemplo, se parte del supuesto de que los daños que puedan producir los usuarios de Twitter a través de la plataforma son responsabilidad de Twitter. Y aunque la carga probatoria para el afectado es similar al del escenario anterior, el intermediario tendría un deber de vigilancia más complejo, lo que implica demostrar que obró con diligencia para supervisar las acciones del usuario (haber actuado como un 'buen padre de familia').

Por último, está la responsabilidad objetiva, y específicamente la tesis de que la actividad de un intermediario como Twitter implica la creación de un riesgo público –tanto como la extracción de minerales con explosivos o el uso de armas por parte del Estado–. Bajo este estándar, y volviendo al ejemplo, habría una presunción de que la actividad que desarrolla Twitter es peligrosa y, por lo tanto, tendría que ser éste el que pruebe que el daño se produjo por un hecho imposible de prever o por fuera de su órbita de control.

La idea de instaurar un régimen de responsabilidad objetiva para los intermediarios de Internet fue impulsada principalmente por las industrias creativas para proteger el derecho de autor.[10] Pero esta propuesta no tiene mayor vigencia hoy en día. Ante un riesgo de responsabilidad objetiva –y de una sanción pecuniaria cuantiosa– el intermediario podría optar por no prestar el servicio o implementaría cambios estructurales para ofrecerlo en condiciones sumamente controladas. Refiriéndonos por última vez al ejemplo, llevaría a Twitter a instaurar un sistema para verificar los contenidos antes de su publicación, o a no ofrecer el servicio del todo. Y en términos de la estrategia de crear un guardián o ama de llaves, generaría efectos no deseados o amenazaría la existencia misma del intermediario.[11]

Los demás planteamientos sobre la responsabilidad extracontractual –por el daño producido y por el hecho del tercero–, aún tienen vigencia. Por un lado, apuntalan algunas de las leyes existentes y, por el otro, algunos jueces los han aplicado en procesos judiciales contra intermediarios. En este caso, un elemento problemático ha sido determinar en qué consiste, concretamente, la diligencia a la que está obligado el intermediario para eximirse de responsabilidad (esto es, por ejemplo, si debe bloquear contenidos, monitorear permanentemente el servicio o atender la queja de una persona afectada, entre otros). Se trata, en últimas, de otra manera de llegar a la pregunta de en qué consiste la guardia que debe llevar a cabo el guardián. A esto volveremos más adelante.

[9] Cfr. Mazeaud, H; Mazeaud, L. Compendio del tratado teórico y práctico de la responsabilidad delictuosa y contractual. Tomo I. Editorial Colmez, México, 1945.
[10] Cfr. Jessica Litman en Digital Copyright. Selected Works, 2006; Peguera Poch, M. 'La exención de responsabilidad civil por contenidos ajenos en Internet'. Jornadas de Responsabilidad Civil y Penal de los Prestadores de Servicios en Internet. Barcelona, noviembre de 2001. Disponible en: http://www.uoc.edu/in3/dt/20080/#bibliografia (verificado el 6 de agosto de 2013).
[11] Cfr. Hylton, K. Property Rules, Liability Rules, And Immunity: An Application To Cyberspace. Boston University School of Law, Working Paper Series, Law and Economics No. 06-19, 2006.
Ver también, Carrasco Blanc, H. 'Algunos aspectos de la responsabilidad de Proveedores de Servicios y Contenidos de Internet. El caso ENTEL'. En: REDI, No. 26, agosto de 2000.

II. Los antecedentes: metiendo a las ovejas al redil

1. Los intermediarios como editores o distribuidores

Zittrain ubica el origen de los primeros debates judiciales sobre responsabilidad de intermediarios de Internet en Estados Unidos en decisiones de los noventa. Para entonces, aunque el *World Wide Web* era apenas una idea en marcha y no había las aplicaciones que hoy conocemos, varias empresas suministraban simultáneamente la conexión y una navegación limitada a los confines de sus servicios.[12] En ese entonces los usuarios compartían información y publicaban mensajes en el tablero (*bulletin board*) del operador, un espacio sin configuraciones sofisticadas ni fines específicos.

Que la principal actividad en Internet en ese entonces fuera la difusión de contenidos llevó a que se buscaran analogías entre los intermediarios de este espacio naciente y los medios de comunicación tradicionales. *"Los primeros debates jurisprudenciales y legislativos sobre cómo categorizar el Internet giraron en torno a si clasificar a los intermediarios usando los modelos tradicionales de medios escritos, radiodifundidos y de transmisión común"*, afirma Laidlaw.[13] El punto central era definir alguna responsabilidad similar para esos actores por la difusión de contenidos difamatorios que hacían sus usuarios.

Optar por una u otra categoría implicaba asignarles niveles distintos de responsabilidad por lo que se dijera o transmitiera. Si el intermediario era considerado como un medio escrito, podría responder por cualquier contenido que pasara por o estuviera en su servicio. En cambio, si era considerado un transmisor común o *common carrier* –como cualquier compañía de teléfonos o de servicio postal– no tendría que responder por lo que dijeran o hicieran sus usuarios.

Los casos a los que se refiere Zittrain son los siguientes: en 1990, la empresa Cubby Inc. demandó por difamación a Compuserve por cuenta de un material producido por un particular pero distribuido por este operador a sus suscriptores. De manera similar, en 1994 una firma inversionista demandó a Prodigy por una acusación de fraude hecha por un usuario anónimo –esta vez a través de un foro sobre temas económicos–.[14]

Ante la ausencia de legislación específica (la cual llegó poco después), los jueces acudieron al precedente análogo. Según éste, aunque tanto una editorial como un medio de comunicación pueden llegar a ser responsables legalmente, el estándar es más bajo para el primero. De manera general se considera que la editorial es un mero distribuidor o conductor pasivo de un contenido –los libros–, mientras el medio de comunicación interviene en lo que se publica –el periódico o la revista– y, por lo

[12] Cfr. Op. Cit. Zittrain.
[13] Op. Cit. Laidlaw, p. 265 (traducción informal).
[14] Cfr. Cubby vs. Compuserve, en Digital Media Law Project. Disponible en http://www.dmlp.org/threats/cubby-v-compuserve, y Stratton Oakmont vs. Prodigy, en Digital Media Law Project. Disponible en http://www.dmlp.org/threats/stratton-oakmont-v-prodigy (verificados el 2 de agosto de 2013).

tanto, tiene injerencia en éste. Esta distinción fue la base para que los jueces resolvieran los casos por vías distintas: Compuserve fue considerado como un simple distribuidor de la información de terceros –una especie de *common carrier*– y Prodigy, como un editor. Es decir: el primero fue declarado inocente y el segundo, culpable.

La idea de que los prestadores de servicios de Internet (PSI) respondieran por la actividad de sus usuarios no se limitaba al problema de la difamación en línea. Ya para finales del siglo XX parecía claro que el entorno digital, más allá de la promesa de acceso al conocimiento, desarrollo y libertad de expresión, abría un espacio para la distribución de pornografía infantil, la comisión de delitos como la estafa o el robo de identidad y, por supuesto, el tráfico no autorizado de películas y música.[15]

Este último tema era especialmente sensible en Estados Unidos. Los estudios discográficos y la industria cinematográfica –los principales titulares de contenido– veían Internet como una amenaza para su negocio, y presionaron al gobierno para que expidiera legislación que hiciera responsables a los PSI por los contenidos ajenos que compartían sus usuarios. Sin entrar en disquisiciones teóricas sobre qué responsabilidad debían tener estos amos de llaves, le hicieron un ultimátum al gobierno de Bill Clinton (1993-2001), que en parte reflejaba la visión que tenían sobre Internet: si dicha protección no existía, no verterían sus contenidos en este nuevo espacio. Sería una red de tubos sin nada adentro. El resultado fue el *Digital Millennium Copyright Act* de 1998, una ley menos radical de lo que las industrias pretendían, pero con un régimen de responsabilidad concreto para los PSI.[16]

2. El fin de la excusa tecnológica

Según Lilian Edwards, los PSI –conscientes de que a través de sus redes y servicios se transmitía y alojaba contenido altamente riesgoso– venían planteando a su favor una razón práctica: *"Los PSI argumentaron vigorosamente que no podían revisar manualmente la legalidad de todo el material que pasara por sus servidores sin incurrir en demoras y costos inconcebibles".*[17] De este argumento se desprendía otro igualmente importante, que era el riesgo de estancar el desarrollo, la innovación y la competencia en Internet (una razón estratégica para Europa, ya rezagada en el tema frente a Estados Unidos).

Esta postura, que sin duda fue determinante para la expedición de normas y decisiones judiciales favorables a los PSI, tuvo un punto de quiebre en 2000. Ese año un francés llamado Mark Knobel demandó a Yahoo en Francia por ofrecer en su portal objetos y recordatorios alusivos a los nazis (distribuir productos nazi es ilegal en ese país). *"La justicia francesa quiere imponer su parecer en una*

[15] Cfr. Edwards, L. The Fall and Rise of Intermediary Liability Online. En: Law and the Internet. Hart Publishing. Oxford and Portland, Oregon, 2009, p. 47-88.
[16] Cfr. Cortes, C. Mirar hacia el norte es mirar hacia atrás: el impacto negativo de la DMCA. El mecanismo de notificación y retiro y las Medidas Tecnológicas de Protección. Documentos Karisma, julio de 2013. Disponible en: http://karisma.org.co/?p=2241 (verificado el 5 de agosto de 2013).
[17] Ibidem, Edwards, p. 59 (traducción informal).

área sobre la que no tiene control", comentó entonces el fundador de Yahoo Jerry Yang.[18] La respuesta fue contundente: *"Existe esta idea naif de que Internet lo cambia todo. Pues no cambia todo. No cambia las leyes en Francia"*, dijo uno de los abogados del caso.[19] Para los demandantes, Yahoo bien podía vender todos los productos nazi que quisiera en Estados Unidos, pero no dentro de las fronteras de su país.

Yahoo se defendió, como era previsible, con el argumento de la 'imposibilidad'. Dijo que no tenía el poder para identificar de dónde venían sus compradores ni la manera de controlar quiénes accedían a sus productos digitales. Y si la empresa removiera la oferta de productos nazi de sus servidores en Estados Unidos, estaría dándole a la ley francesa un alcance mundial. Al juez no pareció impresionarle mucho el planteamiento, y le encargó a un comité que determinara si era posible filtrar automáticamente las solicitudes de contenido desde una localización en particular. La respuesta fue afirmativa, y sustentó la orden judicial. De la misma manera como Yahoo ya situaba publicidad diferenciada para usuarios de diferentes países, podía bloquear el acceso de la mayoría de los franceses a un contenido en particular –a partir de las direcciones IP y los datos de los usuarios–.[20]

Este caso suele usarse para ilustrar el problema de la jurisdicción –o, más bien, de la dispersión de jurisdicciones– en Internet.[21] Pero también es un antecedente fundamental para comprender cómo se fue construyendo –para bien o para mal– el rol de los PSI como guardianes. Una vez desmontado el argumento de la imposibilidad (que aunque pudo ser cierto en un momento no era inmutable), se abrió paso la discusión sobre qué tipo de obligaciones debían tener los PSI como amos de llaves de los usuarios. Y a partir de allí la tecnología dejaba de ser un obstáculo para convertirse en el instrumento que les permitiría a los PSI, tanto por obligación como por conveniencia, ejercer ese papel.

[18] Carr, N. The Big Switch: Rewiring the World, From Edison to Google. W. W. Norton & Company, 2013, p. 199 (traducción informal).
[19] Goldsmith, J.; Wu, T. Who Controls the Internet? Illusions of a Borderless World. Oxford University Press, 2006, p. 2 (traducción informal).
[20] Cfr. Op. Cit. Edwards.
[21] Sobre este tema, ver Bertoni, E. 'La determinación de la jurisdicción en litigios por difamación por contenidos en Internet: algunas observaciones para América Latina'. En: Hacia una Internet libre de censura. Propuestas para América Latina. Bertoni, E. Compilador. Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Universidad de Palermo, 2012, p. 313-339.

III. Los guardianes y su deberes: tipos de intermediarios y responsabilidades

Los intermediarios en línea son, entonces, todos los agentes que de una u otra manera posibilitan y determinan nuestra actividad en Internet. No todos están ubicados en el mismo nivel en la red ni ofrecen el mismo servicio. En una arquitectura de niveles como la de Internet, unos están en la capa física –son la infraestructura de la red– y otros en la de aplicaciones.[22] Y en ésta última son diversos los servicios y las formas de usabilidad para el usuario.

Estas diferencias se concretan en las clasificaciones sobre los tipos de intermediarios. En general, se habla de los que posibilitan el acceso a la red (la empresa a la que pagamos por el servicio de Internet), por un lado, y todos los demás que ofrecen servicios en línea, por el otro (Google, Facebook, Dropbox, Amazon, nytimes.com etc.). Pero hay clasificaciones más detalladas y variadas.

Mann y Belzley se refieren a los Prestadores de Servicios de Internet (PSI), que proveen la conexión y alojan los contenidos; los intermediarios de pago, que posibilitan transacciones económicas (como Paypal o Visa) y los intermediarios de subasta, que ofrecen a la venta productos de terceros (como Ebay o Mercadolibre).[23] De manera similar, Meléndez Juarbe plantea la división entre intermediarios de conexión, de información y financieros.[24] Y Zunino los divide en operadores de redes y proveedores de acceso, proveedores de servicios de búsqueda y enlaces (por ejemplo, Google), y prestadores de servicios de almacenamiento de datos (como Dropbox o Box.net).[25]

Estas clasificaciones suelen actualizarse para tratar de reflejar de manera más precisa el panorama de intermediarios en la red. Y aunque el ejercicio puede quedarse corto frente a la evolución y convergencia de algunos servicios (piénsese, por ejemplo, que hoy por hoy Google ofrece tanto servicios de almacenamiento como de búsqueda), el punto central es entender que estas categorizaciones se hacen con la idea de identificar al intermediario para saber qué función debe asumir como guardián.

En materia de flujo de contenidos en Internet,[26] la mayoría de leyes sobre responsabilidad de intermediarios se han expedido para que el guardián ayude a enfrentar uno de tres problemas: la pornografía infantil, la piratería o las vulneraciones al honor y el buen nombre. En ninguno de estos casos se ha establecido un régimen de responsabilidad objetiva. Las leyes varían entre lo que se conoce como una inmunidad total o una inmunidad condicionada para el intermediario. Y en países sin leyes

[22] Sobre la arquitectura de la red, ver Cortes, C. Vigilancia de la red: ¿Qué significa monitorear y detectar contenidos en Internet? Centro de Estudios en Libertad de Expresión (CELE), Universidad de Palermo, 2012. Disponible en: http://www.palermo.edu/cele/libertad-de-expresion/ilei-investigaciones_realizadas.html (verificado el 6 de agosto de 2013).
[23] Cfr. Mann, R.; Belzley, S. The Promise of Internet Intermediary Liability. Law and Economics Working Paper No. 45, Abril de 2005, The University of Texas School of Law, p. 1-51.
[24] Meléndez Juarbe, H. 'Intermediarios y libertad de expresión: apuntes para una conversación'. En: Op. Cit. Hacia una Internet libre de censura. Propuestas para América Latina, p. 109-123.
[25] Cfr. Zunino, M. La responsabilidad de los proveedores de servicios de Internet y la libertad de expresión. La Ley, 31 de octubre de 2012.
[26] Como se mencionó en la introducción, este documento se centra en la responsabilidad de intermediarios frente a contenidos. No se aborda temas relacionados con comercio electrónico o delitos como estafa en línea.

específicas, los jueces han resuelto algunos casos en estos mismos temas a partir del régimen general de responsabilidad civil (en Latinoamérica, especialmente en Argentina). A continuación se abordan los tres ámbitos, tomando un ejemplo y haciendo énfasis en los deberes que implica para el intermediario.[27] Igualmente, se señalan algunas críticas comunes frente a estos modelos.

1. Inmunidad absoluta

Para explicar el régimen de inmunidad absoluta vamos a tomar el caso de Estados Unidos. En 1996, el Congreso de ese país expidió el *Communications Decency Act* (CDA) con el propósito principal de combatir la pornografía y la obscenidad en línea. Por encontrarla contraria a la Primera Enmienda –que protege la libertad de expresión–, un año después la Corte Suprema de Justicia tumbó la mayor parte de la norma. Sin embargo, dejó vigente la Sección 230, que establece que ningún proveedor o usuario de un 'servicio informático interactivo' puede ser tratado como editor o portavoz de la información proporcionada o difundida por cualquier otro usuario o servicio.[28]

En otras palabras, los intermediarios que alojan, publican o 'repostean' información o expresiones de terceros están protegidos de eventuales acciones judiciales por difamación o similares. Ningún titular de un servicio como Twitter o Facebook, ningún medio de comunicación en línea y ninguna persona con un blog o página personal, es responsable por los comentarios o los contenidos –ya sea texto, audio o video– que otras personas difundan a través del servicio o en el portal respectivo.

Esta inmunidad absoluta no era la intención del legislador. El texto original de la ley incluía unas provisiones 'anti-obscenidad', según las cuales podía ser criminalmente responsable quien, entre otras, usara un 'servicio informático interactivo' para poner a disposición de un menor de 18 años cualquier comentario, sugerencia, propuesta, imagen o contenido que, de conformidad con los estándares contemporáneos de una comunidad, describiera o representara actividades sexuales o escatológicas. En su revisión de esta disposición, la Corte Suprema subrayó la relevancia de la libertad de expresión y la necesidad de que las normas que se relacionen con este derecho no sean desproporcionadas:

> *La CDA carece de la precisión que la Primera Enmienda requiere cuando un estatuto regula el contenido de la expresión. Si bien el gobierno tiene un interés en proteger a los niños de material potencialmente dañino, la CDA persigue ese interés suprimiendo una gran cantidad de expresión que los adultos tienen derecho constitucional de enviar y recibir. Su alcance no tiene precedentes. La carga que la CDA impone en la expresión de los adultos es*

[27] Para un estudio comparado sobre las normas en la materia, ver, Ruiz, C.; Lara, J. 'Responsabilidad de los proveedores de servicios de Internet en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica'. En: Hacia una Internet libre de censura. Propuestas para América Latina. Bertoni, E. Compilador. Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Universidad de Palermo, 2012, p. 109-123.
[28] Ver, 47 USC § 230 - Protection for private blocking and screening of offensive material. Disponible en: http://www.law.cornell.edu/uscode/text/47/230 (verificado el 6 de agosto de 2013).

inaceptable si alternativas menos restrictivas podrían ser al menos igual de efectivas para alcanzar los objetivos legítimos de la ley.29

El razonamiento de la Corte también puede leerse en clave de guardianes y amas de llaves. En su versión original, la CDA introducía el incentivo de la sanción para que los intermediarios colaboraran con la conducta indeseada. Pero los costos de este esquema no eran razonables, no solo para los prestadores del servicio –que habrían tenido que introducir sistemas de monitoreo y vigilancia–, sino también, y principalmente, para el grueso de la sociedad. El costo que se pagaba, la externalidad negativa, era la restricción abierta e inconmensurable del debate público.

Los defensores de la libertad de expresión consideran que la inmunidad absoluta de la CDA es una conquista, y prenden las alarmas cuando se escuchan propuestas de pasar normas similares a la versión original.[30] No sin razón, consideran que una norma distinta posibilitaría el control de contenidos con fines políticos, la censura previa y, en general, una inhibición de la libertad de expresión en línea. No obstante, poco a poco surgen voces autorizadas para quienes la balanza está excesivamente desequilibrada en contra de derechos como la privacidad o el buen nombre.

"La velocidad con la que las reputaciones pueden construirse y alterarse es solo una de las formas en que Internet ha cambiado todo. Con seguridad, la mayoría de estos cambios han sido para bien, pero lamentablemente Internet es una maldición cuando el objeto de información negativa es uno (…)", afirman Levmore y Nussbaum.[31] Para éstos y otros autores, es poco o nada lo que pueden hacer los usuarios afectados frente a la propagación de rumores, el abuso del anonimato, el lenguaje obsceno y abusivo, y la misoginia.

Solove y Leiter, entre otros, proponen que la Sección 230 del CDA se modifique para abandonar un régimen de inmunidad total. *"El daño de la expresión en Internet es suficientemente serio para que debamos repensar las protección legales"*, afirma Leiter.[32] Por su parte, Solove critica el hecho de que la mayoría de la cortes hayan extendido la inmunidad para los intermediarios incluso cuando tienen conocimiento de que el material es difamatorio. En consecuencia, propone que se instaure un sistema de notificación y retiro o notificación y respuesta, un sistema que –como veremos– entraña a su vez otros problemas.[33]

2. Inmunidad condicionada

[29] Corte Suprema de los Estados Unidos. Reno v. American Civil Liberties Union, 521 U.S. 844, Junio 26 de 1997. Disponible en: http://www.law.cornell.edu/supct/html/historics/USSC_CR_0521_0844_ZS.html (traducción informal).
[30] Ver, por ejemplo, 'Section 230 Under Attack: State AGs' Proposal Threatens Internet As We Know It'. Center for Democracy and Technology, julio de 2013. Disponible en: https://www.cdt.org/blogs/andrew-mcdiarmid/2507section-230-under-attack-state-ags%E2%80%99-proposal-threatens-internet-we-know-i (verificado el 6 de agosto de 2013).
[31] Levmore, S.; Nussbaum, M. (eds.). The Offensive Internet. Speech, Privacy, and Reputation. Harvard University Press, Cambridge, 2010. Pos. 45, versión Kindle (traducción informal).
Ver también, Lemley, M. Rationalizing Internet Safe Harbors, Journal of Telecommunications and High Technology Law, Vol. 6, p. 101, 2007.
[32] Ibidem, Pos. 1960.
[33] Ibidem, Pos. 806.

La inmunidad condicionada la encontramos sobre todo en normas sobre protección de derechos de autor en Internet. La idea de este tipo de regímenes es ofrecerle al intermediario un 'puerto seguro' donde esté a salvo de cualquier responsabilidad legal siempre y cuando cumpla con deberes concretos. Aunque los titulares de contenido abogaron por un nivel de responsabilidad mayor, la inmunidad condicionada terminó siendo el punto de encuentro entre los intereses de éstos y de los Prestadores de Servicios de Internet (PSI).[34]

La sección 512 del *Digital Millenium Copyright Act* (DMCA) de Estados Unidos, expedido en 1998, estipula unas condiciones para que un PSI no sea responsable por las posibles violaciones a los derechos de autor llevadas a cabo por sus usuarios. Si el PSI cumple con esas condiciones entra en el puerto seguro de la ley, en cuyo caso el titular del contenido no podrá perseguirlo legalmente por un eventual daño.

El DMCA establece unas categorías de PSI que están amparados por la ley.[35] El propósito es asegurarse de que éstos actúan realmente como intermediarios y no como distribuidores directos del contenido protegido. A partir de esta clasificación, la ley parte del supuesto de que los PSI no tienen por qué saber si un usuario está usando de manera ilegal el contenido de terceros. Es decir, el DMCA no establece un deber permanente de monitoreo. Sin embargo, esta presunción se desvirtúa cuando algún hecho o circunstancia indica que hay una actividad infractora manifiesta o cuando el titular del material notifica al PSI.

Desde ese momento el PSI ya tiene conocimiento de una posible infracción al derecho de autor y, por lo tanto, empieza a abandonar el puerto seguro. Conoce de una posible actividad infractora y la está permitiendo. En consecuencia, si el PSI quiere mantener su inmunidad, debe proceder a bloquear el acceso al material o retirarlo –un video, por ejemplo– y notificar al usuario afectado de lo sucedido.[36] Y si el usuario afectado considera que el material fue removido o bloqueado erróneamente, puede iniciar un proceso de contra-notificación. No obstante, debe estar dispuesto a llevar su caso ante cualquier juez y esperar un lapso de entre 10 y 14 días.[37] Pasado ese término, si el titular del contenido no inició una acción judicial, el PSI debe restablecer el contenido.

Como estrategia de ama de llaves, la inmunidad condicionada del DMCA establece un incentivo claro para el guardián, y aunque impone costos considerables –el PSI debe tener un responsable en su

[34] Ver, entre otros, Drahos, P.; Braithwate, J. Information Feudalism. Who Owns the Knowledge Economy. The New Press, New York-London, 2002; Decherney, P. Hollywood's Copyright Wars. From Edison to the Internet. Columbia University Press, New York, 2012; Jessica Litman en Digital Copyright. Selected Works, 2006.
[35] La DMCA admite cuatro categorías de intermediarios: los que conducen, transmiten o enrutan información, los que hacen copias temporales (caching), los que almacenan información y los que ayudan a localizar información –referido principalmente a los motores de búsqueda–.
[36] Esta obligación no está en cabeza de los intermediarios que enrutan o transmite información y de aquellos que hacen copias temporales. Si no originan la transmisión ni manipulan los datos más allá de lo que técnicamente se requiera, están en una especie de inmunidad absoluta (como si fueran 'common carriers').
[37] Para una explicación más detallada sobre la DMCA y el 'puerto seguro', ver, Op. Cit. Cortes, C. Mirar hacia el norte es mirar hacia atrás: el impacto negativo de la DMCA. El mecanismo de notificación y retiro y las Medidas Tecnológicas de Protección.

empresa para atender estos procedimientos– no impone deberes difusos o desproporcionados de monitoreo y vigilancia.[38] Los costos, en cambio, sí los asumen los usuarios y la comunidad en general.

De una parte, el usuario que resulta afectado por un retiro equivocado corre con el costo de 'perder' el contenido –al menos temporalmente– y asume la carga de defenderlo. De otra parte, la comunidad en general resulta afectada por las expresiones e informaciones removidas de manera excesiva. Por cuenta del balance de los incentivos, el PSI no pierde nada con retirar material y sí gana mucho con la entrada al puerto seguro.[39]

Según Lemley, *"el efecto del sistema de notificación y retiro ha sido fomentar que los intermediarios de Internet bajen cualquier contenido que protesten los titulares de derecho de autor, sin importar cuán frívola pueda ser la queja".*[40] En la misma línea, para Tushnet *"el proceso de notificación y retiro puede usarse para suprimir tanto discursos críticos como infracciones al derecho de autor".*[41]

En contraste con el mecanismo de notificación y retiro del DMCA, diversos países han optado por alternativas que mantengan los incentivos para los intermediarios pero, a la vez, brinden las garantías necesarias a los usuarios. La ley chilena sobre este tema –que implementa una de las obligaciones del tratado de libre comercio con Estados Unidos– incluye un mecanismo de retiro de contenido con intervención previa del juez.[42] Por otra parte, la ley canadiense incorpora un mecanismo de 'notificación y notificación': el reclamo del titular del contenido no obliga al PSI a retirar el contenido sino a notificar al usuario, y solo si el PSI incumple con este deber puede incurrir en una responsabilidad legal.[43]

Explicar en mayor detalle las distintas alternativas de puertos seguros y los debates que las rodean requeriría de un espacio aparte. Para efectos de este documento, es relevante tener en cuenta el balance entre los incentivos y los costos de la inmunidad condicionada, no solo para el intermediario sino también para el usuario y la comunidad en general. Igualmente, es fundamental observar que en la mayoría de estos sistemas de inmunidad condicionada el intermediario está exonerado de un deber permanente de monitoreo, lo cual resulta beneficioso. La inmunidad condicionada –siguiendo la tipología propuesta por Kraakman– vuelve a los PSI chaperones del usuario, pero de manera limitada. Esto se traduce en mayor libertad y autonomía para el ciudadano.

3. Responsabilidad subjetiva

[38] De manera similar a la DMCA, la 'Directiva sobre el comercio electrónico' de la Unión Europea establece que los prestadores de servicios no tienen una obligación general de supervisión. Esto significa, concretamente, que los Estados-parte no les impondrán a éstos "una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas".
Directiva 2000/31/CE. Diario Oficial n° L 178 de 17/07/2000 p. 0001 - 0016. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:ES:HTML (verificado el 5 de agosto de 2013).
[39] Cfr. Seltzer, W. 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment'. Harvard Journal of Law and Technology. Volume 24, Number 1, Fall 2010. Pg. 171 y ss.
[40] Op. Cit., Lemley, p. 114 (traducción informal).
[41] Tushnet, R. Power Without Responsibility: Intermediaries and the First Amendment. The George Washington Law Review, Vol. 76, No. 4, 2008, p. 118. (traducción informal).
[42] Cfr, Álvarez Valenzuela, D. En Busca de Equilibrios Regulatorios: Chile y las Recientes Reformas al Derecho de Autor. ICTSD. Documento de Política Pública, 22, 2011. Disponibe en: http://ictsd.org/downloads/2011/12/en-busca-de-equilibrios-regulatorios-chile-y-las-recientes-reformas-al-derecho-de-autor.pdf (verificado el 6 de agosto de 2013).
[43] Cfr. Copyright Modernization Act, sección 41.25 y ss. Disponible en: http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/FullText.html# (verificado el 6 de agosto de 2013).

Por último tenemos los regímenes de responsabilidad subjetiva que –como vimos– no corresponden a la aplicación de una ley específica sobre intermediarios en Internet, sino al uso de normas y principios generales sobre responsabilidad civil. Decíamos atrás que éste puede ser un régimen menos gravoso para el intermediario en comparación con el de responsabilidad objetiva; no obstante, resulta más desventajoso frente a una inmunidad condicionada –ni qué decir de una absoluta– toda vez que los deberes del PSI no están del todo definidos. Para hablar de esta categoría vamos a centrarnos en un caso argentino (país en el que no hay ley de intermediarios en Internet).

En 2008 Esteban Bluvol se enteró de que existía un blog en Blogger (plataforma de Google) con su nombre y con material injuriante sobre él. Demandó a Google por daños y perjuicios a su vida personal y laboral, y en primera instancia el juez decretó a su favor una indemnización de diez mil pesos argentinos (unos US$1,800). Bluvol apeló el fallo para exigir una indemnización mayor y, en diciembre de 2012, la Cámara Nacional de Apelaciones de la Capital Federal aumentó la cuantía al doble.[44]

Para el tema que nos ocupa, lo interesante del caso fueron los regímenes que aplicaron los jueces de ambas instancias. El de primera instancia consideró que la responsabilidad de Google era objetiva, específicamente por la teoría del riesgo creado (similar a la de la actividad peligrosa). El juez de segunda instancia desestimó esa tesis rápidamente. Consideró que un intermediario como Google no debe *"responder en forma automática por las conductas ilícitas de terceros, teniendo en cuenta que en internet circulan millones de noticias, lo que torna extremadamente dificultoso el control previo de todo lo que se difunde. Ello implicaría obligar a las empresas a monitorear constantemente los miles de perfiles o comentarios que se suben cada minuto".*[45]

Sin embargo, el juez no exoneró a Google ya que consideró que de todas formas había incumplido con su responsabilidad. Previo al proceso judicial, Bluvol se había quejado directamente ante la empresa por la existencia y los contenidos del blog (usando los mecanismos usuales de queja o denuncia de contenido) sin que aquella lo removiera. Google argumentó que no podía hacerlo sin una orden judicial. En contraste, para el juez el incumplimiento se configuró cuando Google se negó a retirar el blog después de la solicitud del afectado. En ese momento había tenido efectivo conocimiento del hecho dañoso y no había obrado con diligencia. Agregó, por último, que más que un caso de libertad de expresión se trataba de uno de suplantación.

El caso Bluvol no es el único en Argentina con un argumento similar frente a la responsabilidad del intermediario como guardián del usuario. En el caso de Belén Rodríguez contra Yahoo y Google, en el que la primera solicitaba que se eliminara de los motores de búsqueda cualquier referencia a páginas de contenido sexual asociadas a su nombre, el juez de segunda instancia afirmó:

[44] Cfr. Poder Judicial de la Nación. Cámara Nacional de Apelaciones de la Capital Federal. Bluvol, Esteban Carlos c / Google Inc. y otros s/ daños y perjuicios" (Exp. n° 59.532/2009).- Rec. N° 607.911.- Juzg. N° 105.-
[45] Ibidem.

> *No creo que este deber del explotador del motor de búsqueda de bloquear los contenidos ilícitos requiera una previa orden judicial, como lo sostiene cierta doctrina. Ese requisito no surge, en nuestro país, de norma alguna, y no resulta compatible con el deber de diligencia que recae sobre las demandadas (…). Por el contrario, basta a mi criterio con que hayan tomado conocimiento –en principio, mediante la comunicación del usuario- de la existencia del contenido nocivo para que se encuentren obligados a bloquearlo con prontitud, pues esa es la conducta esperable de un empresario diligente de la clase de las aquí demandadas.*[46]

De estos casos se extraen al menos dos conclusiones: primero, no existe un deber de monitoreo y vigilancia general. Esto es positivo. Un deber difuso o abstracto de monitoreo implica en la práctica un estándar muy riguroso de responsabilidad, pues el guardián debe ejercer un rol complejo y permanente de chaperón. Tendría que vigilar todas las acciones del usuario. A la postre, con una guardia de este tipo *"el guardián puede ser penalizado por un rango de malas conductas muchos más amplio del que en realidad puede detectar".*[47]

Segundo, el deber de diligencia del PSI está atado a hacer juicios de valor sobre la legalidad de las acciones del usuario. Y esta facultad informal de adjudicación sí es problemática. ¿Cuál sería el criterio para que el intermediario mantenga o elimine un contenido cuando se trate de imputaciones fácticas o afirmaciones subjetivas? ¿Qué hace cuando se encuentra con versiones encontradas o zonas grises?

[46] Poder Judicial de la Nación. Sala Civil A. Rodríguez, María Belén c/ Google Inc. y otro s/ Daños y Perjuicios. Juzgado Civil No. 95 (Expediente No. 99.613/2006)
[47] Op. Cit. Kraakman, p. 77 (traducción informal).

IV. Mirando al horizonte: el riesgo del filtrado y la idea de la solución tecnológica

Los regímenes de responsabilidad para los intermediarios en Internet son, a la vez, la causa y la consecuencia de un proceso de estrechamiento del entorno digital. No es posible analizarlo aquí en detalle. Baste con decir que en él confluyen intereses del Estado –combatir el terrorismo, vigilar a los ciudadanos y proteger algunos derechos individuales, entre otros– y de los particulares –comercializar, sofisticar y controlar la experiencia en línea, principalmente–.[48] No se trata, sin embargo, de una evolución inevitable o lógica. Las alternativas y las divergencias frente a estos modelos también hacen parte de ese proceso.

En el caso de los guardianes en línea, la pregunta –volviendo a Kraakman– radica en cuál es el tipo de guardia que consideramos socialmente deseable. El riesgo, como señalábamos, es múltiple: una guardia desproporcionada, además de ineficiente, terminará por sacrificar actividades en línea y desconocer derechos fundamentales como la libertad de expresión y el debido proceso.

Si el intermediario asume un rol muy activo de chaperón, el impacto para la actividad en línea será manifiesto. Dependiendo del grado del incentivo que tenga para ejercer un control más o menos riguroso, el guardián comenzará a vigilar todos los rincones de su servicio en busca de contenidos indeseables, personas sospechosas o actividades simplemente riesgosas. Así como en un *shopping-mall* los guardias quieren mantener un ambiente aséptico, los intermediarios en la red tratarían de mantener un servicio que no prenda ninguna alarma legal.

Aún no hemos llegado a ese estadio, en parte gracias a las inmunidades absolutas (no nos olvidemos que la mayoría de los servicios que usamos están domiciliados en Estados Unidos). Sin embargo, la protección del derecho de autor ha permeado la libertad de expresión en línea, y en este caso ni las inmunidades son absolutas ni faltan incentivos de otro tipo (económicos y políticos) para que los guardianes ejerzan un mayor control.

En este contexto los regímenes de responsabilidad no solamente llevan a los guardianes a ejercer como chaperones, sino que también puede llevarlos a que sean 'bouncers', en cuyo caso la actividad de control puede quedar invisibilizada, lejos del escrutinio público. El 'bouncer', recordemos, simplemente se niega de plano a admitir la entrada de la persona al bar. No quiere problemas.

Como vimos, bajo el *Communications Decency Act* los intermediarios no tienen deberes legales de diligencia. No son chaperones. Sin embargo, esto no obsta para que en los términos de referencia un intermediario prohíba la difusión de cierto tipo de contenido y establezca filtros para prevenir que algo se publique. En la 'Declaración de derechos y responsabilidades' de Facebook, por ejemplo, el usuario

[48] Cohen, J. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice.Yale University Press, 2012.

acepta que no publicará *"contenido que contenga lenguaje ofensivo, resulte intimidatorio o pornográfico, que incite a la violencia o que contenga desnudos o violencia gráfica o injustificada"*.[49]

El filtrado de contenidos en Internet no es nuevo,[50] y algunos autores lo ven como la alternativa en el horizonte para el problema de la responsabilidad de los intermediarios. Edwards lo pone en estos términos:

> *En el futuro parece que la pregunta no será si el filtrado por parte de intermediarios es posible o no, sino más bien –si es mandatorio– qué grado de precisión será necesario, qué costos se pueden imponer de manera justificada, y qué compromisos y acuerdos serán aceptables en términos de libertad de expresión, privacidad, debido proceso y barreras para el acceso al conocimiento.* [51]

Con este futuro en ciernes el reto para muchos académicos y activistas es –siguiendo una de las críticas de Cohen– aventurase a proponer qué tipo de restricciones arquitectónicas en el entorno digital serían legítimas desde el marco de trabajo de la libertad de expresión. En otras palabras, si la idea es reivindicar este derecho hay que comenzar por explicar cómo reivindicarlo.[52]

El propósito de este documento no es plantear esa hoja de ruta (lo cual, a primera vista, es un reto enorme), pero sí, para terminar, dejar sobre la mesa una propuesta a manera de ejemplo. Regresemos a la crítica que hace Solove sobre los riesgos para la reputación y el buen nombre en línea. Podemos convenir que los discursos de odio, la difamación, el matoneo y el *character assassination,* son un problema real en Internet.[53] No obstante, un régimen de notificación y retiro –como propone Solove– atañe los mismos riesgos que hemos señalado para regímenes similares: habría un incentivo grande para censurar contenidos, el intermediario asumiría un papel de facto como juez y, posiblemente, ajustaría los términos del servicio para ejercer un mayor control. ¿Es esa la única forma de poner esa idea en práctica?

Recientemente se planteó informalmente la propuesta de que los intermediarios generaran una herramienta para que quien se considerara difamado por el contenido pudiera contrarrestarlo en el mismo sitio donde el contenido inicial apareció.[54] La idea de introducir cambios en el código informático para balancear derechos o para promover fines democráticos ha sido propuesta también por

[49] Facebook, 'Declaración de derechos y responsabilidades'. Disponible en: https://www.facebook.com/legal/terms (verificado el 6 de agosto de 2013).
[50] El tema se abordó parcialmente en otro documento del CELE-iLei. Op. Cit. Cortes, C. Vigilancia de la red: ¿Qué significa monitorear y detectar contenidos en Internet?
[51] Op. Cit. Edwards, p. 85 (traducción informal).
[52] Cfr. Op. Cit., Cohen, p. 173 y ss.
[53] Sobre este tema, ver Cortes, C. Centro de Estudios en Libertad de Expresión (CELE), Universidad de Palermo, 2012. Disponible en: http://www.palermo.edu/cele/libertad-de-expresion/ilei-investigaciones_realizadas.html (verificado el 6 de agosto de 2013).
[54] Cfr. 'Una solución tecnológica para el problema de la responsabilidad de intermediarios'. E. Bertoni. En: Global Voices, 30 de mayo de 2013. Disponible en: http://es.globalvoicesonline.org/2013/05/30/una-solucion-tecnologica-para-el-problema-de-la-responsabilidad-de-intermediarios/ (verificado el 7 de agosto de 2013).

Zuckerman, Zittrain, Mayer-Schonberger y Wu, entre otros.[55] Incluso el programa de radio 'On the media' del *National Public Radio* de Estados Unidos abrió una consulta entre sus oyentes para 'arreglar' Twitter.[56]

Por supuesto, cada propuesta tiene muchos obstáculos. Ésta de la herramienta, en particular, merece varias preguntas: ¿sería una implementación requerida por ley?, ¿requeriría de la decisión de un juez?, ¿no terminaría usándose con fines políticos para acallar críticas?, ¿sería suficiente?, ¿qué pasará cuando cambien las configuraciones tecnológicas?

Bien vale la pena explorar la idea y pensar en cómo desarrollarla, sobre todo si estamos hablando de una solución tecnológica. La configuración de la red que hoy conocemos es una de tantas posibles que en medio de avatares y alternativas se fue consolidando. Y de la misma manera como se habla de una tecnología –los filtros– para restringir contenidos, bien podemos hablar de otra para promoverlos.

Un derecho de réplica en un blog o red social, o una glosa informativa en un motor de búsqueda podría desarrollarse de la manera que resulte menos extraña e invasiva para el servicio. En el caso de Twitter, 'On The Media' proponía el uso de colores y banderas para advertir sobre información dudosa, agresiva o desvirtuada; en Youtube, Wu sugería un sistema de alarmas –a partir de la evaluación hecha por una comunidad de usuarios confiables– para advertir sobre discursos de odio que debían ser removidos; y en la propuesta referida se recordaba el *sidewiki* –un pestaña del navegador Chrome para hacer anotaciones sobre páginas web– que alguna vez tuvo Google. Algo similar ya tienen portales como Quartz y Medium, que permiten a los usuarios hacer comentarios en líneas o párrafos del contenido.[57]

Es imposible garantizar que estas alternativas funcionarán y desactivarán todos los posibles litigios por afirmaciones injuriosas y ataques personales. Pero implementarlas no serían del todo extrañas a uno de los fines mismos de la libertad de expresión, que es garantizar un debate equilibrado. Y tal vez la mejor manera de lograr que los intermediarios acojan soluciones como éstas sería mediante una mezcla de regulación y autorregulación. Es decir, leyes que ofrezcan incentivos para que los intermediarios implementen autónomamente –con algún tipo de supervisión– mecanismos tecnológicos para equilibrar estos debates de una manera transparente.

Hablar de equilibrio en materia de libertad de expresión –en palabras de Fiss– es tanto como bajarle el volumen a algunas voces y subírselo a otras.[58] Esa es una forma de ver una solución

[55] Ver, Zuckerman, E. Rewire. Digital Cosmopolitans in the Age of Connection. W.W. Norton and Company, 2013, Pos. 3714 y ss (versión Kindle); Mayer-Schönberger, V. Delete: The Virtue of Forgetting in the Digital Age. Princeton, Princeton University Press, 2009, Pos. 4447 y ss (versión Kindle); Zittrain, J. The Future of the Internet and How to Stop It. New Haven London, Yale University Press, 2008. Pos. 4447 y ss. (edición Kindle); 'When Censorship Makes Sense: How YouTube Should Police Hate Speech'. Wu, T. En: The New Republic, 18 de septiembre de 2012. Disponible en: http://www.newrepublic.com/blog/plank/107404/when-censorship-makes-sense-how-youtube-should-police-hate-speech (verificado el 7 de agosto de 2013).
[56] Ver, 'Let's Fix Twitter'. En: On The Media. Disponible en: http://www.onthemedia.org/blogs/on-the-media/2013/apr/26/lets-fix-twitter/?utm_source=/blogs/on-the-media/2013/may/01/lets-fix-twitter-vol-ii/&utm_medium=treatment&utm_campaign=morelikethis (verificado el 7 de agosto de 2013).
[57] Cfr. 'Quartz Lets Readers Comment on Specific Paragraphs Atlantic Media's business brand elevates role of feedback'. Taintor, D. En: Adweek.com. Disponible en: http://www.adweek.com/news/press/quartz-lets-readers-comment-specific-paragraphs-151690 (verificado el 11 de agosto de 2013). Ver también www.medium.com.
[58] Cfr. Fiss, O. The Iron Of Free Speech. Harvard University Press, 1996.

tecnológica como la expuesta. La crítica obvia a una propuesta semejante es que abrirá el camino para la censura y la imposición de contenidos. Pero tal vez una evaluación más pausada indique que podría servir para fortalecer el debate público en nuestro entorno digital.

V. Recomendaciones

Este documento ha brindado un sustento teórico y un contexto mínimo a la discusión sobre la responsabilidad de los intermediarios en Internet. Y antes que hacer un estudio comparativo de los regímenes existentes, nos ocupamos en resaltar los puntos más relevantes de éstos para identificar los problemas y ofrecer algunos elementos de análisis. Con ese ánimo, a manera de cierre y sin excluir otros puntos señalados en el texto, hacemos las siguientes recomendaciones:

- Es importante considerar el balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de ama de llaves. Un desequilibrio entre éstos implica una estrategia fallida que además impacta negativamente actividades socialmente deseables y afecta derechos fundamentales como el debido proceso y la libertad de expresión.

- Establecer un régimen de responsabilidad objetiva para los intermediarios de Internet resulta inadecuado. Por un lado, implica imponerle obligaciones difusas a éstos, más allá de las que realmente podrían cumplir. Por el otro, se traduciría en mayores restricciones para los usuarios de Internet, en contravía de derechos y garantías fundamentales. Las decisiones judiciales en Argentina ilustran el problema de que el intermediario esté obligado a hacer juicios de valor sobre la legalidad de las acciones del usuario.

- La inmunidad condicionada parece adecuada como régimen de responsabilidad cuando establece incentivos razonables para el guardián. Es decir, cuando no le impone deberes difusos o desproporcionados de monitoreo y vigilancia. Sin embargo, en algunos modelos de inmunidad condicionada –como el del DMCA de Estados Unidos– los costos que no asume el intermediario terminan en cabeza de los usuarios y la comunidad en general. En este caso los costos son vulneraciones a derechos como la libertad de expresión y el debido proceso.

- En esos términos, y sin subestimar el problema del contenido agresivo y difamatorio que pulula en la red, una inmunidad condicionada en materia de responsabilidad de intermediarios por contenidos de sus usuarios podría implicar, en la práctica, la derogación de la libertad de expresión y el debido proceso en Internet.

- Los debates sobre la responsabilidad de los intermediarios deben prestarle atención a la práctica del filtrado de contenidos, que aparece en el horizonte como una estrategia invisible para que el amo de

llaves ejerza la guardia. Esto implica, de paso, empezar a mirar las condiciones que acepta el usuario cuando adhiere a los términos de referencia del servicio.

- Vale la pena explorar la idea de implementar soluciones tecnológicas –en todas sus versiones– para enfrentar los contenidos difamatorios que abundan en Internet. Particularmente, es posible pensar en adaptar un derecho de réplica a diferentes tipos de servicios y plataformas.