Gazeta de Antropología

ISSN 0214-7564

Gazeta de Antropología, 2012, 28 (2), artículo 10 · http://hdl.handle.net/10481/23357 Versión HTML

Recibido 18 octubre 2012 | Aceptado 27 noviembre 2012 | Publicado 2012-12

Propiedad intelectual, seguridad y control de las comunicaciones en Internet. Impacto sociocultural del fenómeno Megaupload

Intellectual property, security and control of Internet communications. Sociocultural impact of Megaupload phenomenon

Miguel Moreno Muñoz
Departamento de Filosofía II. Universidad de Granada.
mm3@ugr.es

RESUMEN
La conceptualización del debate sobre la protección de los derechos de autor en términos de ciberseguridad introduce un sesgo inequívocamente autoritario en diversas propuestas legislativas presentadas al Senado y al Congreso de Estados Unidos entre 2011 y 2012. Numerosas organizaciones defensoras de los derechos civiles y de una Internet libre han advertido de las consecuencias, puesto que sus promotores tienen sobrada capacidad para presionar en las instancias de toma de decisiones de otros países. De ser aprobadas, supondrían el fin de una Internet libre y no fragmentada, donde los Estados, las agencias de seguridad y otras entidades públicas o privadas tendrían mecanismos de control sin precedentes sobre las actividades de internautas y usuarios. Este trabajo propone elementos para adoptar un enfoque más amplio del problema, en un marco que garantice de manera efectiva la libertad política y los derechos civiles.

ABSTRACT
The conceptualization of the debate on copyright protection in terms of cybersecurity brings an unmistakably authoritarian biases in several legislative proposals submitted to the Senate and U.S. Congress between 2011 and 2012. Civil rights organizations defending a free Internet have warned against its consequences, due to the well-known capacity of its sponsors to influence on the decision-making process in other countries. If approved, it would mean the end of an open, not fragmented Internet, where states, security agencies and other public or private entities will have unprecedented control over Internet activities and users. This paper proposes some elements in order to adopt a broader approach to the problem, considering specific trends in consumption patterns of new socio-technical communities and evaluating the socio-cultural impact of services with important business opportunities associated, provided that political freedom and civil rights are unequivocally guaranteed.

PALABRAS CLAVE
Internet | derechos de autor | ciberseguridad | Megaupload | SOPA | CISPA | ACTA
KEYWORDS
Internet | copyright | cibersecurity | Megaupload | SOPA | CISPA | ACTA

1. El mantenimiento de una Internet libre y no fragmentada como objetivo político

Internet constituye el desarrollo tecnológico con mayor potencial para contribuir a articular el ideal de ciudadanía cosmopolita que vislumbró Kant en su ensayo *La paz perpetua* (1795) (cfr. Kant 1998). Esto es así a pesar de las múltiples trabas directas e indirectas que los Estados -democracias liberales incluidas- ponen a la implantación de muchos servicios y aplicaciones que explotan las posibilidades innumerables de información e interacción social a través de las redes digitales.

La organización no gubernamental *Reporteros Sin Fronteras* (RSF) incluye en su informe “Enemigos de Internet”, hecho público el 12 de marzo de 2012, una lista de países cuyos mecanismos de vigilancia, censura y represión les convierten en un entorno abiertamente hostil para la libertad de expresión. El filtrado estricto de contenidos, la ralentización o interrupción temporal del acceso, la persecución de los ciberdisidentes y la propaganda en línea son prácticas habituales en estos países (Birmania, China,

Cuba, Irán, Corea del Norte, Arabia Saudí, Siria, Turkmenistán, Uzbekistán y Vietnam, a los que se han sumado Bielorrusia y Bahréin en el último año) (RSF 2012).

El informe de RSF mantiene "bajo vigilancia" a Australia, Egipto, Eritrea, Francia, Malasia, Rusia, Corea del Sur, Sri Lanka, Tailandia, Túnez, Turquía y Emiratos Árabes Unidos, más India y Kazajstán en el último año. Se trata de países que no han desmantelado por completo sus aparatos de censura y vigilancia, en los que faltan mecanismos de transparencia básicos o que estudian implantar sistemas potentes de filtraje en la Red (Australia, p.ej.). En otros -Malasia, Turquía, Rusia- la pérdida de credibilidad de los medios de comunicación tradicionales ha devuelto el protagonismo a blogueros y activistas, convertidos así en objetivo de acoso y violencia.

La importancia de contribuir al mantenimiento de una Internet libre, no fragmentada y accesible para todos constituye hoy un objetivo socio-político de primer orden. Los cambios políticos que vienen produciéndose en el mundo árabe desde 2011 ilustran con claridad el papel crucial desempeñado por los internautas, motivados por un mismo objetivo de dar a conocer los hechos que presenciaban y mantener redes de coordinación que permitan el flujo informativo. Muchos de ellos, junto con los periodistas que les ayudaron a sortear los mecanismos de censura, han pagado un alto precio:

> "2011 pasará a la historia como un año de violencia sin precedentes contra los internautas. Murieron cinco de ellos mientras trataban de informar. Cerca de 200 blogueros e internautas fueron detenidos, un 30% más que el año anterior. Una cifra nunca registrada antes y que probablemente crecerá a la vista de la violencia ciega desplegada, especialmente, por las autoridades. Más de 120 activistas de la Red están en la cárcel de hoy" (1).

2. Carencias democráticas del marco regulador de las actividades en Internet

En materia de libertad de expresión en Internet, los países democráticos tienen todavía un largo camino por recorrer. Es frecuente que la libertad de expresión y de prensa quede supeditada a los intereses en materia de seguridad interna, guerra contra el terrorismo, delitos cibernéticos o protección de la propiedad intelectual. Por otra parte, no existe una percepción pública lo bastante sólida de los riesgos para el ejercicio de los derechos civiles y políticos en el ciberespacio. En consecuencia, son frecuentes los abusos en la interceptación de comunicaciones telefónicas y en el acceso a datos personales sin orden judicial (RSF 2012: 7).

Los pronósticos pesimistas se han visto superados por la dureza con la que algunas leyes aprobadas entre 2009 y 2011 en países como Australia, Francia, Italia y Gran Bretaña penalizan las descargas de material sujeto a derechos de autor, permiten a los Estados implantar sistemas de filtrado y control de las acciones en la red y las escasas garantías para el internauta del proceso probatorio. Así, el parlamento del Reino Unido dio el visto bueno a la *Digital Economy Act* (2010). Francia, en 2009, a la HADOPI (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*) y en 2011 a la LOPPSI 2 (*Loi d'orientation et de programmation sur la sécurité intérieure*). Y España aprobó la "Ley Sinde" el 15 de febrero de 2011, aunque su reglamento (en el que se establecían las atribuciones de la Comisión de Propiedad Intelectual) entró en vigor el 1 de marzo de 2012.

Entre 2011 y 2012, en otros países se han propuesto numerosas iniciativas para la reforma del marco jurídico que regula la protección de la propiedad intelectual y la seguridad en Internet. Prácticamente todas tienen en común el hecho de que proponen restricciones significativas al ejercicio de derechos civiles y políticos que suelen gozar de sólido respaldo constitucional. Las instancias concernidas aducen como pretexto y justificación su responsabilidad para contribuir a una evolución normativa necesaria, que evitará abusos y permitirá adaptarse a los constantes desarrollos tecnológicos, además de abrir posibilidades inéditas de negocio. Por su naturaleza, las cuestiones de propiedad intelectual se ubican en el centro de una problemática más amplia, puesto que van ligadas a las restricciones en el acceso al

conocimiento del que depende la innovación industrial y la competitividad de empresas y países, sometidos a crecientes y cada vez más sofisticados riesgos de ciberseguridad.

3. Un debate público frecuentemente distorsionado

Una simplificación habitual -pero inaceptable- del problema consiste en presentarlo como un caso típico de conflicto de intereses entre la industria audiovisual (que para garantizar los derechos de los autores intenta mantener o incrementar los márgenes de beneficio por la venta de sus productos) y los internautas, que pretenden conseguir música, libros, películas, juegos o software de manera gratuita, usando cualquier herramienta que les permita "piratear" esos contenidos (Pryor *et al*. 2008; Zentner 2006).

Sin entrar en los problemas metodológicos y técnicos que deben solventar los estudios de mercado en que se basan, los enfoques de este tipo excluyen del conflicto de intereses demasiados elementos para entender su complejidad y pretenden introducir en el debate público un sesgo favorable a los intereses de los grandes sellos discográficos, editoriales, distribuidoras y productoras cinematográficas, por mencionar solo a los actores más destacados (Hong 2007).

Se dispone ahora de una literatura especializada abundante, en la que se estudian y analizan con detalle los múltiples aspectos (tecnológicos, económicos, sociológicos, axiológicos, etc.) de la convergencia de medios y productos en el soporte digital y su impacto cultural o simbólico en nuevas dinámicas de consumo, ocio y trabajo (Vaidhyanathan 2001; Feenberg 2002; Hellwig 2002; Beuscart 2005; Bhattacharjee *et al*. 2006; DeVoss y Porter 2006; Radcliffe 2006; DeVoss y Webb 2008; McKee 2008; Mahanti *et al*. 2011). Tales aportaciones permiten interpretar mejor el impacto de algunos incidentes ocurridos entre 2011 y 2012 -entre los que destaca el cierre de megaupload.com y los dominios asociados por agentes del FBI, a instancias de un juez federal estadounidense-, y ayudan a identificar las deficiencias en los mecanismos vigentes de protección de información personal de usuarios de determinados servicios en línea.

Este y otros casos ponen de manifiesto las escasas garantías jurídicas que el marco regulador actual ofrece para proveedores de servicios de comunicaciones y, en general, para todas las empresas que intentan desarrollar nuevos modelos de negocio en Internet (Moiny 2011). Además, ayudan a comprender las dificultades que persisten para consolidar un marco favorable a la innovación y al desarrollo de infraestructuras tecnológicas que permitan a cualquier empresa prestar servicios en línea a escala global (Choi y Pérez 2007; Kleve *et al*. 2007).

Por otra parte, el desarrollo tecnológico y la mejora en la cobertura de los servicios de banda ancha han permitido la incorporación de cientos de millones de usuarios a nuevas dinámicas de consumo, de ocio e interacción social. El resultado es la generación de un entorno de mercado de magnitud extraordinaria, ampliando a escala global las posibilidades de negocio asociadas con las redes digitales (Hong 2007). No obstante, han sido relativamente pocas las empresas que han sabido rentabilizar esta transformación en las actitudes de los consumidores, consideradas en buena parte una evolución de las observadas en relación con otros servicios de intercambio P2P (*peer to peer*) (Wang y McClung 2012). El retraso en adaptar los modelos de negocio ha sido particularmente evidente en la industria de contenidos y productos audiovisuales, que sigue desaprovechando el potencial de la distribución digital y las posibilidades de acceso a sus contenidos desde múltiples dispositivos (Kleve *et al*. 2007; Bhattacharjee *et al*. 2006).

Las iniciativas legislativas consideradas aquí (SOPA, PIPA, ACTA y CISPA) coinciden en proponer cambios significativos en la gobernanza de Internet, so pretexto de mejorar la seguridad y la protección de la propiedad intelectual. Dadas sus implicaciones democráticas y cívicas, su contenido continúa siendo objeto de intenso debate. Los partidarios de un modelo de capitalismo industrial centrado en la

escasez y el control de la distribución (Perritt 1994) se oponen a quienes confían más en dinámicas de intercambio y cooperación para explotar el potencial de las redes digitales de alcance global. Los primeros han conseguido materializar propuestas sumamente restrictivas de derechos civiles y políticos que abren la puerta a procesos de vigilancia y control sin precedentes. De ser aprobadas en los órganos legislativos sin modificaciones sustanciales, debilitarían seriamente el sistema establecido de garantías para proteger las libertades individuales contra los intentos de infracción injustificada por parte de gobiernos y organizaciones privadas. Incluso las garantías para participar en la vida civil y política de los Estados sin discriminación o represión se verían menoscabadas (Moiny 2011).

4. El cierre de Megaupload.com

El popular servicio de alojamiento e intercambio de archivos Megaupload (http://www.megaupload.com) fue clausurado tras una redada del FBI (Federal Bureau of Investigation) en la madrugada del 19 de enero de 2012. Terminó con la detención de algunos de sus máximos responsables en Auckland (Nueva Zelanda) y sienta un precedente peligroso como vía para resolver conflictos de valores e intereses en la sociedad del conocimiento.

Tras la intervención, megaupload.com muestra solo una imagen donde puede leerse que el nombre de dominio asociado con la web Megaupload.com ha sido intervenido por orden de un juzgado estadounidense y que un jurado federal ha imputado a varios detenidos y entidades por diversos crímenes, entre ellos conspiración para cometer crimen organizado, infracción de las leyes de copyright y blanqueo de dinero (2).

La operación puesta en marcha y coordinada por el FBI implicaba registros en instalaciones ubicadas en Estados Unidos y en ocho países más, con el objetivo de cerrar una veintena de dominios y cerrar o tomar el control sobre los servidores donde se alojaban. El dominio principal, Megaupload.com, registraba un tráfico superior a los 50 millones de visitas diarias, equivalente aproximadamente al 4% del tráfico en Internet.

Se trataba, sin duda, de uno de los servicios más demandados de Internet. Megaupload.com permitía a los usuarios subir archivos (música y películas, fundamentalmente; pero también documentos de texto, programas, etcétera) que otros usuarios podían descargarse. En su modalidad básica -gratuita-, permitía subir archivos de hasta 2 GB y descargas de hasta 1 GB. La modalidad *Premium* -por unos 60 euros anuales- eliminaba el límite de subida, permitía las descargas de hasta 100 GB y combinar varios ficheros. Megaupload contaba además con la plataforma Megavideo, desde la que podían verse series y películas en *streaming*, sin necesidad de descargarlas. En total, la empresa podría haber logrado más de mil millones de visitas (50 millones al día), involucrando a más de 150 millones de usuarios registrados (en torno al 4% del tráfico global en Internet).

El jueves 19 de enero, un día después del gran ‘apagón’ de Internet para protestar por la ley antipiratería conocida como SOPA (*Stop Online Piracy Act*), se hizo público el cierre de Megaupload por el FBI. El FBI intervino la sede central de la empresa, arrestó a cuatro responsables de su mantenimiento y ordenó la detención de tres acusados más por delitos de piratería y blanqueo de capitales. La denuncia, cursada por un jurado de Estados Unidos el 5 de enero de 2012, acusaba a los responsables de la web de blanqueo de capitales y violación de la propiedad intelectual, entre otros delitos:

> “Durante más de cinco años la organización ha operado páginas web que reproducían ilegalmente y distribuían infringiendo las leyes de la propiedad intelectual obras que incluían películas antes de su estreno comercial, música, programas de televisión, libros electrónicos y software de entretenimiento a una escala masiva. (…) Los conspiradores se negaron a cerrar cuentas de usuarios que infringían los derechos de autor”; solo retiraban “selectivamente” los enlaces denunciados y después lo comunicaban “a los poseedores de derechos” (Fuente:

http://www.rtve.es/noticias/20120119/fbi-cierra-megaupload-mayores-webs-intercambio-archivos-internet/490924.shtml (acceso: 15/10/2012)).

Las reacciones tras la intervención del FBI alcanzaron gran visibilidad mediática y dieron origen a un intenso debate. Entre las más extremas, las del grupo *Anonymous*, anunciando que lanzaría el mayor ataque DDoS (*denegación de servicio*) jamás visto. Consiguieron dejar inoperativos sitios web pertenecientes a *Universal Music*, a *Recording Industry Association of America* (RIAA), a *Motion Picture Association of America* (MPAA) y al *Departamento de Justicia* (DOJ) (Merlo 2012).

Precisamente esta renuencia a colaborar con las autoridades y entidades de gestión de derechos de autor es una de las cosas que más valoraban los usuarios de Megaupload. La demanda contra los administradores incluye cinco cargos: conspiración para cometer infracciones de los derechos de autor, conspiración para lavado de dinero, dos cargos por infracción criminal de los derechos de autor y otro cargo por conspiración para cometer extorsión, al entender que los acusados se comportaban como una banda criminal.

Los cuatro arrestados fueron Kim Schmitz (alias Kim Dotcom), ciudadano de Finlandia y de Alemania, fundador de Megaupload Limited y presunto jefe de la "mega conspiración", según el FBI; Fin Batato, ciudadano alemán y jefe de publicidad comercial y de ventas; Mathias Ortmann, alemán y jefe técnico de la compañía; y Bram van der Kolk. También se presentaron cargos contra 3 colaboradores: Julius Bencko, ciudadano de Eslovaquia y director gráfico; Sven Echternach, alemán y director de desarrollo de negocio; Adrus Nomm, de Estonia y jefe de programación. Las cuentas bancarias de los administradores fueron registradas y se examinaron los servidores de Megaupload para recoger evidencias de la difusión de contenido supuestamente pirateado (Fuente: http://cultura.elpais.com/cultura/2012/01/19/actualidad/1327003171_243063.html (acceso: 15/10/2012)).

Según las autoridades norteamericanas, la estimación de pérdidas para la industria audiovisual de todo el entramado de dominios y servicios asociados con Megaupload podría alcanzar los 500 millones de dólares. Los beneficios para los propietarios de Megaupload, por cuotas de usuarios *premium* y publicidad, rozarían los 175 millones de dólares. La acusación de "blanqueo de capital" se sustenta en el hecho de que Megaupload pagaba a los usuarios mediante un "programa de recompensas por subir contenidos", un dinero presuntamente no declarado. Tras los sucesivos registros en Estados Unidos y ocho países más, el FBI congeló bienes asociados a la empresa y sus gerentes por valor de 38 millones de euros. En los días siguientes se filtraron numerosas noticias sobre el estilo de vida ostentoso de Kim Schmitz en su residencia de Nueva Zelanda.

5. Consecuencias del cierre de Megaupload

Los más afectados por la neutralización de la red de servidores intervenidos fueron las páginas de enlaces, cuyo negocio radicaba en publicitar contenidos enlazados a los archivos existentes en la plataforma Megaupload (un total de 18 dominios, entre ellos Megavideo, Megaclick, Megaworld, Megalive, Megapix, Megacar, Megafund, Megakey, Megamovie, etc.). Evitaban así el consumo de ancho de banda que supondría hospedarlos por sí mismos (y la posible atribución de responsabilidad). Además, se beneficiaban de la segunda mejor plataforma mundial para alojamiento y descarga de archivos, prácticamente sin competencia en su fiabilidad para la distribución de archivos de vídeo y con el mayor crecimiento de la base de usuarios premium (Mahanti 2011: 1091-1099).

Una actividad fundamental de las webs de enlaces consistía en indexar una cantidad ingente de material con interés potencial para millones de usuarios, gran parte de los cuales modificaron sus patrones de consumo y consolidaron, p.ej., la tendencia creciente a ver contenidos bajo demanda, en streaming. Los capítulos de muchas series disponibles mediante esta red de servidores podían llegar a tener más audiencia por este canal que en su medio de emisión habitual.

El fenómeno no pasó desapercibido a la industria audiovisual. De ser cierta la información publicada por el diario *New Zealand Herald*, ejecutivos de varios estudios de Hollywood (entre ellos, Disney, Warner Bros, Fox y Turner Broadcasting) buscaron acuerdos comerciales con el portal Megaupload, pese a tratarse de empresas que habían materializado en las instancias competentes numerosas quejas por violaciones de sus derechos de autor (Fuente: http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10794827 (acceso: 16/10/2012)).

Las propuestas de colaboración apuntaban a la posibilidad de compartir contenidos y realizar acuerdos de publicidad conjunta. Warner Bros podría haber ido más lejos, contemplando la posibilidad de subir al portal la mayor parte de su contenido. La misma fuente aportó otros datos sorprendentes: La defensa de Kim Schmitz pretendía demostrar que al menos 490 cuentas del portal pertenecían a miembros de la *Asociación del Cine* de Estados Unidos (MPAA) y de la *Asociación de la Industria Discográfica* de Estados Unidos (RIA), a través de las cuales subieron unos 16.455 archivos a Megaupload. Además, pretendían probar que 1.058 miembros del portal pertenecían a instituciones oficiales estadounidenses, entre ellas el FBI, la NASA y los tribunales estadounidenses; y que 15.634 cuentas de militares estadounidenses nutrieron con 340.893 archivos la red de servidores a Megaupload.

Puesto que muchos usuarios utilizaban Megaupload de manera legal como sitio alternativo para guardar copia secundaria o principal de sus datos, el cierre inesperado les privó del acceso a su propia información personal o profesional, sin que por el momento hayan encontrado una alternativa razonable que les garantice su recuperación (Cfr. “Kyle Goodwin Motion For Return of Property”, en https://www.eff.org/node/70871 (acceso: 17/10/2012)).

En lugar de ayudar a los usuarios que pagaban por el uso legal de unos servicios que recibían conforme a las cláusulas de un contrato comercial válido, y que resultaron objetivamente perjudicados por la intervención que interrumpió el funcionamiento de la red de servidores, los funcionarios estadounidenses encargados del caso anunciaron que habían terminado su examen de los servidores de Megaupload y que las empresas propietarias de los equipos -*Carpathia hosting* y *Cogent, en Estados Unidos/Canadá; LeaseWeb, en Países Bajos*- tenían total libertad para eliminar el contenido. Al parecer, estas empresas acordaron un plazo para que los gestores de Megaupload intentaran de buena fe proporcionar a los usuarios acceso a sus datos (Cfr. https://www.eff.org/cases/megaupload-data-seizure (acceso: 17/10/2012)).

Cualquiera que sea el desenlace procesal del caso, este episodio ilustra la importancia de elegir con precaución a cualquier proveedor de servicios en la nube (*cloud*), y las condiciones del contrato de prestación de servicios que aceptan los usuarios de Dropbox, Box.net, Google Drive o CX.com, por mencionar algunos de los más populares (3). En particular, resulta importante comprobar qué amparo prevén en caso de cierre legal o quiebra de la compañía proveedora. Tampoco puede descartarse que la información depositada en ellos pueda desaparecer o ser intercambiada con terceros, razón por la que conviene conocer las garantías contra tales supuestos y los procedimientos de indemnización que las empresas contemplan si se dan esas circunstancias.

6. Una industria tradicional de distribución de contenidos anquilosada y reacia a la competencia

6.1. Una oferta limitada

El contexto donde se consolida la oferta de Megaupload venía caracterizado por la escasa innovación en los canales y plataformas de distribución de contenidos multimedia. Las únicas excepciones con modelos de negocio relativamente exitosos (*Spotify*, para la música; *Netflix*, para películas y series; *iTunes*, para música y aplicaciones; etc.) tenían/tienen ciertas ventajas y numerosos inconvenientes. La facilidad en el acceso a contenidos no siempre va acompañada de una oferta suficientemente extensa y variada. El

coste de la suscripción básica se ha ido incrementando rápidamente y la disponibilidad del servicio con frecuencia queda limitada a ciertos países (Estados Unidos, Canadá y Reino Unido, en bastantes casos). Los propietarios de derechos reciben una remuneración muy escasa por el disfrute de sus obras. Y persisten las dificultades técnicas para sortear el acceso a los mismos contenidos mediante procedimientos no demasiado complejos.

Por otra parte, Internet permite a los usuarios comparar los precios de un mismo producto vendido en países diferentes. Si incluimos en el cálculo un factor de corrección en función del poder adquisitivo (salario medio) de cada país, el mismo álbum en CD *The Final Frontier*, del grupo Iron Maiden, cuesta en España 12.57 € (de media); en Francia, 14,37 €; en Alemania, 7.88 €; y en el Reino Unido, 4.95€ (los gastos de producción pueden estimarse cubiertos en la horquilla de 4-7€). El CD *At the edge of time*, de Blind Guardian, cuesta en España 15.53€; en Francia, 12.41€; en Alemania, 8.94€; y en Reino Unido, 6.91€ (4). Se trata de diferencias de precio considerables, que para muchos consumidores resultan arbitrarias e injustificadas. Esta situación ha llevado a las instancias antimonopolio de la Unión Europea a la apertura de expedientes por presunto acuerdo para subir artificialmente los precios (Crombie 2001).

6.2. Abuso de posición dominante

En relación con los libros electrónicos se han podido constatar abusos flagrantes de posición dominante y de conspiración para pactar al alza su precio, motivo por el que fueron condenadas en Estados Unidos Apple y varias editoriales (Macmillan, Penguin, Hachette, HarperCollins y Simon & Schuster, entre otras). Este tipo de prácticas han costado decenas de millones de dólares a los usuarios estadounidenses, y prueban la existencia de una inequívoca conspiraron entre las empresas involucradas para imponer en la venta de libros lo que se conoce como un *modelo de agencia*:

> "Se comunicaron entre ellos de forma habitual (…) para intercambiar información sensible y darse garantías de cooperación para lograr los fines de la conspiración. (…) Bajo ese modelo, los editores controlan el precio de venta al público designando a los minoristas como 'agentes' que no tienen en realidad la facultad de alterar el precio de venta que imponen los editores. En consecuencia, los editores podrían poner fin a la libre competencia entre minoristas y aumentar los precios que los consumidores pagan por los libros electrónicos. (…) Millones de libros electrónicos que se hubieran vendido a 9,99 dólares o otros precios bajos acabaron vendiéndose por otros precios marcados por los Acuerdos de Agencia de Apple, por lo general 12,99 o 14,99 dólares" Fuente: http://cultura.elpais.com/cultura/2012/04/11/actualidad/1334163962_714199.html (acceso: 16/10/2012) (5).

Si tenemos en cuenta que la demanda presentada en los juzgados de Nueva York (6) propone como inicio de los hechos el mes de septiembre de 2008, poco antes de la proliferación a escala mundial de lectores electrónicos de todo tipo y de dispositivos como tabletas y teléfonos móviles inteligentes -que desplazaron rápidamente los hábitos de lectura hacia el soporte electrónico-, se entenderá mejor el alcance económico de este tipo de prácticas comerciales anticompetitivas y el perjuicio para los consumidores. Walter Isaacson, en su biografía de Steve Jobs, aporta elementos sumamente clarificadores al respecto:

> "Con el iPod, Jobs había transformado el negocio de la música. Con el iPad y su *App Store*, comenzó a transformar todos los medios de comunicación, desde las editoriales al periodismo, la televisión y las películas. Los libros eran un objetivo evidente, puesto que el *Kindle* de Amazon había demostrado que existía una demanda de libros electrónicos. Así que Apple creó la *iBooks Store*, que vendía libros electrónicos del mismo modo que la *iTunes Store* vendía canciones. Hubo, sin embargo, una ligera diferencia en el modelo de negocio. Para iTunes, Jobs había insistido en que todas las canciones se vendieran a un precio bajo,

> inicialmente a 99 centavos. Jeff Bezos, de Amazon, había intentado adoptar un enfoque similar con los *ebooks*, insistiendo en venderlos por un máximo de 9,99 dólares. Jobs entró y ofreció a los editores lo que se había negado a ofrecer a las compañías discográficas: Pondrían el precio que quisieran para sus mercancías en la *iBooks Store*, y Apple tendría un 30%. En un principio eso se tradujo en precios más altos que en Amazon" (Isaacson 2011: 505. Trad. mía).

Jobs se sentía más capaz de innovar en el negocio de la distribución de música por Internet que en la venta de libros. Pero tenía claro que nadie pagaría más por los ebooks de Apple, y en el evento de lanzamiento del *iPad* confirmó que "el precio será el mismo". El propio Steve Jobs reconoce los hechos, según recoge Isaacson en su biografía:

> "Amazon se equivocó. Pagaba el precio al por mayor de algunos libros, pero comenzaba a venderlos por debajo de costo, a 9,99 dólares. Una medida que los editores odiaban - pensaron que menoscabaría su capacidad de vender libros de tapa dura a 28 dólares. Así que, antes de que Apple irrumpiera en escena, algunos libreros habían comenzado a retirar sus libros de Amazon. De modo que le dijimos a los editores: 'Iremos hacia un modelo de agencia, donde vosotros establecéis el precio, y nosotros obtenemos nuestro 30%; y sí, el cliente paga un poco más, pero eso es lo que queréis de todos modos.' No obstante, exigimos una garantía de que si alguien vende los libros más baratos que nosotros, entonces podremos venderlos también al precio más bajo. Así que los editores se fueron a Amazon y le dijeron: 'Usted va a firmar un contrato de agencia o no le daremos los libros'" (Isaacson 2011: 505-506. Trad. mía).

7. Nuevos patrones de consumo y el modelo de negocio al que apuntaba Megaupload

7.1. La importancia de los tiempos de respuesta

Para comprender mejor la escasa flexibilidad en los cauces convencionales de distribución de contenidos resulta útil conocer los tiempos de respuesta a la aparición de nuevas demandas o tendencias de consumo. Puede servir de ejemplo el retraso de varios años de Amazon en abrir su tienda de eBooks en español y comercializar fuera de Estados Unidos sus tabletas y *eReaders*. El portal de Amazon en español (Amazon.es) se puso en marcha el 14 de septiembre de 2011; pero su primer centro logístico en España, localizado en San Fernando de Henares, no entró en funcionamiento hasta mayo de 2012 (7). Mientras tanto, ningún otro servicio alternativo de ámbito español o comunitario podía ofrecer un catálogo tan amplio de productos, tiempos de respuesta y precios similares.

7.2. Ventajas de la distribución de contenidos por Internet

Aparte de facilitar el acceso desde múltiples dispositivos a los archivos de los propios usuarios en la nube y a todo tipo de contenidos en formato digital, la infraestructura tecnológica desarrollada por Megaupload puso de manifiesto que eran viables modelos de negocio a escala mundial con características sumamente interesantes. Entre ellas, la posibilidad de remunerar por derechos de autor directamente a los propietarios de los contenidos, puesto que resultaba sencillo establecer la correlación directa entre remuneración y número de escuchas o visualizaciones. Un sistema que, para los titulares de derechos de autor, podría gozar de mayor credibilidad que los cálculos basados en estudios segmentados, subcontratados a empresas privadas con evidentes conflictos de intereses -en España, p.ej., CEDRO; o la tristemente famosa *Sociedad General de Autores y Editores* (SGAE) (8).

La creación de contenidos pensados para su distribución por Internet permite costes de producción y

distribución considerablemente más bajos, y posibilita análisis y estudios de mercado más sencillos. Internet se ha convertido en la gran herramienta que permite garantizar con una efectividad sin precedentes el derecho universal de acceso a la cultura y al conocimiento, bien a través de suscripciones gratuitas con algunas limitaciones (por lo general, mediante inserción de publicidad o la desactivación de algunas funciones en las aplicaciones o servicios) o mediante suscripciones de pago que eliminan estas limitaciones y ofrecen ventajas adicionales.

7.3. Cambios en los hábitos de consumo e impacto cultural

Quizás el mayor impacto de los servicios ofertados por Megaupload haya sido la aparición y consolidación de nuevas pautas de consumo. Como se ha visto en otras ocasiones (en relación con servicios como Napster, Skype y Whatsapp, p.ej.), los usuarios de internet han respaldado cualquier tecnología que permita herramientas eficaces de comunicación y un acceso sencillo y completo a productos de interés cultural o de ocio (Choi y Pérez 2007). Si la tecnología lo permite, harán lo posible por tener acceso a ellos en cualquier marco jurídico (Stiegler 2008; Mahanti *et al*. 2011).

Bajo una perspectiva estrictamente comercial, el aspecto más relevante del fenómeno es el significado cultural que adquiere y su impacto para fomentar nuevas dinámicas de mercado articuladas sobre nuevos valores, en claro contraste con los que inspiraron la normativa vigente sobre *copyright* y propiedad intelectual (DeVoss, Porter 2006). La doctrina legal acumulada en los primeros años de funcionamiento de servicios de intercambio de archivos como *Napster* y *Grokster* está cargada de confusiones, lagunas de conocimiento técnico y errores conceptuales básicos que determinaron en muchos casos atribuciones de responsabilidad sumamente cuestionables (Saxby 2000; Hayes 2001; Radcliffe 2006; Moiny 2011).

En muchas de esas sentencias puede observarse cómo opera una conceptualización convencional de la creatividad artística, literaria o musical, que vincula el progreso y el desarrollo de una sociedad más a la propiedad que a las redes de cooperación, intercambio y uso justo (*fair use*) de las obras o productos culturales (Lessig 2004; McKee 2008; Vaidhyanathan 2001).

Pero aunque la industria musical y audiovisual acumule numerosas sentencias favorables en la persecución del intercambio de material protegido por derechos de autor, las numerosas cuestiones abiertas y la complejidad que añade el ritmo acelerado de desarrollo tecnológico (tras el cierre de *Napster*, pronto aparecieron varios servicios de intercambio P2P descentralizados como *KaZaA*, *Morpheus*, *LimeWire, BitTorrent*, etc.) obligará a estas compañías a dedicar cantidades ingentes de dinero para defender sus intereses en un contexto de cambio cultural tan acelerado como el actual. En algunos casos, las consecuencias de esas sentencias se volvieron precisamente contra las compañías más innovadoras en los canales de distribución de sus propios contenidos y dispositivos, como señalan Choi y Pérez en relación con *Sony*.

7.4. Aparición de nuevas comunidades sociotécnicas

Una consideración detenida de los forzamientos tecnológicos, culturales y de mercado sugiere que el punto de equilibrio en los intereses contrapuestos solo podrá alcanzarse mediante estrategias que aprovechen sabiamente las nuevas demandas, y doten a las empresas de la capacidad de adaptarse a tendencias bien consolidadas en las *comunidades sociotécnicas* y en sus patrones de cooperación y consumo -en la práctica, irreversibles- para proporcionar este tipo de servicios a través de un cauce legal (Beuscart 2005; Bhattacharjee *et al*. 2006).

Los grandes sellos de música y los principales productores audiovisuales forman un conglomerado de

intereses tan complejo que, en la práctica, resultan muy poco eficientes en el cumplimiento de sus objetivos comerciales prioritarios y siempre tentados para buscar múltiples maneras de conspirar para presionar a las personas o instancias que pueden garantizarles un marco regulador favorable (Sheridan 2007) (9).

El deterioro en el modelo de negocio de las grandes compañías discográficas ha ido en paralelo a su incapacidad para comprender las razones del éxito de pequeñas compañías innovadoras y su proceso de adaptación a la evolución en los patrones de consumo de los consumidores, hasta conseguir captar el interés de grandes grupos que compartían una misma cultura sociotécnica. La empresa *BitTorrent*, fundada en 2002 por Bram Cohen, revolucionó el modelo vigente de intercambio P2P con el lanzamiento de una tecnología novedosa que permite descargar archivos de múltiples usuarios cogiendo pequeñas partes de cada uno. A partir de entonces fue posible para la mayoría de los usuarios descargar películas y archivos de vídeo de gran tamaño en un período relativamente corto de tiempo.

La comunidad de desarrolladores *Linux* pronto supo sacar provecho de la tecnología BitTorrent para distribuir las nuevas versiones de su sistema operativo. Con ella, *Red Hat* fue capaz de transferir 21,15 terabytes de datos -equivalente a todos los libros de la Biblioteca del Congreso estadounidense- en un plazo de 3 días y con un coste total de 99$ en servicios de alojamiento. De haberlo hecho con la tecnología convencional, habría tenido que pagar entre 60.000 y 90.000 dólares por el consumo de ancho de banda (Choi y Pérez 2007: 174-175).

7.5. La primera generación de ***nativos digitales***

Las redes y aplicaciones de intercambio P2P no garantizaban siempre la disponibilidad o permanencia de contenidos tan heterogéneos como los demandados por comunidades de usuarios cada vez mayores y más especializadas, ni los suministraban a una velocidad razonable o mediante herramientas de indexación y búsqueda eficaces.

Fueron perdiendo protagonismo con el auge de servicios similares a Megaupload (*RapidShare*, *zSHARE*, *MediaFire* y *Hotfile*, p.ej., aunque las características técnicas de Megaupload eran particularmente apreciadas por los usuarios, como analizan con detalle Mahanti *et al*. 2011). Tras un tiempo breve de familiaridad con estos servicios podían apreciarse cambios de comportamiento significativos en el consumo de productos de ocio, en las dinámicas de cooperación y en la gestión de información personal, dando origen a una cultura de trabajo y a estilos de ocio sustentados en valores diferentes

El alojamiento en la nube -muy similar al tipo de servicios que prestaba Megaupload- se considera ahora una tecnología estratégica en la productividad empresarial. Y millones de usuarios acostumbrados a viajar y trabajar en contextos muy diversos pero siempre conectados no entienden su trabajo cotidiano sin la libertad y flexibilidad que les proporciona el no depender de un único soporte físico para acceder a la información que les importa. Los canales de distribución tradicionales responden al contexto tecnológico de décadas pasadas, son caros, poco confortables y asociados a pautas de consumo de masas y estilos de organización que generan dependencias y limitaciones incompatibles con la horizontalidad y la disponibilidad para cooperar en comunidades o grupos sociotécnicos muy diversificados (Sano-Franchini 2010).

El anquilosamiento en el modelo de negocio de la industria tradicional de contenidos no es simplemente un efecto de la asimetría entre desarrollo cultural y tecnológico -bien analizada por teóricos como Bernard Stiegler (Stiegler 1998, 2008)-, sino la expresión de una incapacidad mayor para detectar el impacto comercial de las nuevas dinámicas culturales inspiradas por desarrollos tecnológicos que satisfacen de manera genuina las necesidades de millones de usuarios (Choi y Pérez 2007: 173-178).

Las grandes compañías discográficas cuentan con el respaldo financiero de entramados empresariales formidables, lo que les otorga capacidad para influir en las instancias gubernamentales donde se gestan y modifican las leyes de derechos de autor. Pero suelen estar más pendientes de sus intereses corporativos que de analizar bajo enfoques innovadores la evolución en los patrones de consumo de sus clientes y los valores que inspiran las nuevas dinámicas culturales.

Para los *nativos digitales*, las pautas y estilos de consumo han cambiado radicalmente durante el proceso de convergencia de medios hacia el soporte digital. Una vez consumada, el resultado es la aparición de esquemas culturales mucho más flexibles para entender la creatividad literaria, musical y audiovisual en general, muy dependientes de los continuos desarrollos tecnológicos y de las aplicaciones para explotar la integración de texto, gráficos, animación, audio, vídeo y otros elementos que, a su vez, generan nuevas necesidades y nuevos hábitos lúdico-creativos o formas de expresión (DeVoss, Webb 2008).

7.6. Reacción punitiva sin estrategias de negocio innovadoras

Por supuesto, esta nueva cultura digital conlleva sus propios desafíos éticos y sociales, y origina debates e interpretaciones conflictivas de fenómenos que, en un nuevo contexto tecnológico, se vuelven ambivalentes o imposibles de encajar en el marco jurídico previo (McKee 2008). El aluvión de demandas que las compañías discográficas presentaron contra todo tipo de usuarios que descargaban música a través de las redes P2P fue pronto interpretado como un modo de demonizar a sus propios clientes, cuya afición por la música había proporcionado beneficios enormes a los legítimos propietarios de derechos de autor durante décadas.

En lugar de modificar sus estrategias de mercadotecnia para adaptarse al nuevo contexto tecnológico y cultural, la industria discográfica reaccionó aferrándose a un modelo de negocio obsoleto, cada vez menos relevante en la era digital (Sano-Franchini 2010: 205). Con ello perdió también la oportunidad de analizar qué ocurría en las redes P2P y de establecer correlaciones sumamente interesantes entre las inversiones en publicidad radiofónica para algunos de sus productos -para mantenerlos un tiempo en las listas de éxitos-, las campañas de mercadotecnia y el número de descargas de los mismos (Bhattacharjee *et al*. 2006).

La asociación que mejor representaba sus intereses (RIAA: *Recording Industry Association of America*), adoptó la estrategia de amedrentar a cualquier usuario de aplicaciones para intercambio de archivos, ya se tratara de “niños, abuelos, madres solteras, abuelas fallecidas o de gente común que no hizo otra cosa que descargar algunas canciones y dejarlas en una carpeta compartida -algo convertido ya en norma cultural de la generación del *iPod*” (Sheridan 2007, citado por Sano-Franchini 2010: 205 -trad. mía-).

Para los usuarios pertenecientes a este nuevo grupo sociotécnico, los intentos de resistencia a los cambios culturales producidos en su peculiar proceso de alfabetización tecnológica (Selber, 2004) resultaban simplemente inútiles (en línea con las tesis de Stiegler, 1998). No se trata de *inmigrantes digitales* -incorporados tardíamente, con mayor o menor entusiasmo, a las posibilidades y estilos de trabajo del soporte digital-, sino de *nativos digitales* -individuos que crecieron familiarizados con el lenguaje digital de las computadoras, los videojuegos e Internet (Prensky 2001). La nueva generación asume de forma natural que “la música disponible libremente y en grandes cantidades es la nueva norma cultural, y la industria no ha dado a los consumidores otra alternativa razonable” (Sheridan 2007).

8. Asociación entre propiedad intelectual y ciberseguridad como pretexto para la restricción de derechos y libertades

La pretensión de mantener en la distribución por Internet los mismos márgenes de negocio que a través de cauces tradicionales ha llevado a muchas entidades de gestión de derechos de autor a actuaciones recaudatorias que rozan lo absurdo. En el contexto de la educación superior, las pretensiones de algunas sociedades privadas que gestionan los derechos de autor se han materializado en estrategias tan voraces que obstaculizarían seriamente la docencia universitaria a través de plataformas de teleformación, p.ej. (como denunció la Conferencia de Rectores de las Universidades Españolas -CRUE- en abril de 2012). Se trata precisamente de las instituciones que más invierten en costear el acceso de sus decenas de miles de usuarios a contenidos en formato convencional y electrónico, pero que soportan un crecimiento imparable de los costes de suscripción a recursos electrónicos como publicaciones, bases de datos y monografías (superior a los 130 millones de euros anuales, destinados básicamente a pagar derechos de autor) (10).

Para muchos, es un ejemplo más de reacción equivocada a dinámicas difíciles de encajar en el marco jurídico que regulaba la propiedad intelectual y los derechos de autor en la primera mitad del siglo XX -en el que parece anclada la industria tradicional de contenidos (Lessig 2004; DeVoss y Webb 2008).

8.1. Las pretensiones de SOPA y PIPA

Ese marco regulador tiende a volverse extraordinariamente complejo y ambiguo cuando se pone en relación con restricciones y cautelas adicionales, derivadas de las inquietudes de los Estados en materia de ciberseguridad y espionaje industrial. En esta línea han ido numerosas iniciativas legislativas recientes, contra las que reiteradamente han advertido organizaciones no gubernamentales como la *Electronic Frontier Foundation* (EEF), la *Fundación Mozilla*, la plataforma *WordPress* y la organización *Fight for the Future,* entre varias más agrupadas en la plataforma *American Censorship Day* (11).

Protect IP Act (PIPA), propuesta para su tramitación en el Senado estadounidense (12), y *Stop Online Piracy Act* (SOPA), propuesta para su tramitación en el Congreso (13), coinciden en su pretensión de legalizar la posibilidad de cerrar cualquier sitio web, dentro o fuera de Estados Unidos, sospechoso de alojar contenidos protegidos por las leyes de *copyright*.

Se trata de normas respaldadas fundamentalmente por la industria de Hollywood y una veintena de congresistas (republicanos en su mayoría). Pero han sido rechazadas de manera clara por pesos pesados en Internet (entre ellos, *Google*, *Facebook*, *AOL*, *eBay*, *Twitter* y *Yahoo*) y fueron objeto de firme repulsa por más de cien juristas de todo el país, cuya opinión, expresada en una carta (*An open letter to the House of Representatives*, Nov. 15, 2011) (14) enfatizaba la peligrosa ambigüedad de facultar a cualquier instancia de la Administración para cerrar sitios con “alta probabilidad” de alojar contenidos protegidos. También la editora de la revista *Nature* -por mencionar a un actor de perfil más discreto en el debate- manifestó su desacuerdo.

La mejora de la eficacia en las acciones orientadas a prevenir eventuales violaciones de los derechos de propiedad intelectual no debe conseguirse suprimiendo garantías para un proceso justo, como ocurriría si la mera sospecha puede servir de motivo principal para cerrar una web. Así redactadas, estas normas habrían dado el máximo respaldo institucional a ciertas instancias de la administración estadounidense para arrogarse *de facto* jurisdicción internacional en la lucha contra la piratería y la falsificación (una pretensión inimaginable e inaceptable para los congresistas y senadores que impulsaron PIPA y SOPA, si procediera de cualquier otro país).

Según el experto español Enrique Dans, la reacción coordinada a estas iniciativas -que motivó un *apagón* sin precedentes de los principales portales de Internet- es fundamental para transmitir que Internet es “muchísimo más importante que los problemas de una industria del entretenimiento que se niega a adaptarse a los tiempos. (…) Jamás en toda la historia de la humanidad, ha habido ni un solo caso en el que una tecnología detuviese su evolución por las quejas de aquellos cuyas actividades se

veían afectadas por ella" (Cfr. http://www.publico.es/culturas/417601/mas-de-60-000-paginas-secundaron-el-apagon-de-internet-en-eeuu (acceso: 19/10/2012)).

8.2. Ley Sinde

Dans establece un paralelismo claro entre *SOPA/PIPA* y la *Ley Sinde* en España: "Tanto SOPA/PIPA como la ley Sinde-Wert se dedican a cerrar páginas sin tutela judicial efectiva, a crear una justicia paralela a la medida de discográficas y entidades de gestión y a desarrollar mecanismos de censura. En ambos casos el ataque a los derechos fundamentales y a la libertad de expresión es total" (Cfr. http://www.publico.es/culturas/417601/mas-de-60-000-paginas-secundaron-el-apagon-de-internet-en-eeuu (acceso: 19/10/2012)).

Hoy se conoce bien la presión considerable ejercida por varios miembros de la legación de la embajada estadounidense para poner a prueba los mecanismos jurídicos que garantizan el derecho a la privacidad de las comunicaciones en España y la evolución de las acciones legales contra algunos sitios que proporcionaban enlaces para descarga de contenidos. Lo hicieron contando con la colaboración de personal de las asociaciones privadas españolas que gestionan los derechos de autor (de la SGAE, sobre todo) (15).

Resulta llamativo que la propia embajada advirtiera del lastre que puede suponer el desprestigio social de entidades como la SGAE -ilustrado con profusión de detalles- para cualquier intento de reforma del marco jurídico vigente. Por su parte, los técnicos de la SGAE advierten a los interlocutores estadounidenses de las dificultades para encajar en el marco jurídico español algunas de las acciones que proponen, por lo que consideran "que desde un punto de vista legal debería ser menos costoso bloquear el acceso de usuarios a sitios operados desde fuera de España" (Cfr. http://www.elpais.com/articulo/espana/EE/UU/investigo/webs/espanolas/elpepuesp/20101221elpepunac_32/Tes (acceso: 19/10/2012)).

Pero el interés del asunto radica en observar con qué sutileza y entusiasmo se afanan estas organizaciones privadas -que presuntamente defienden los intereses de los autores y editores, pero dan la impresión de hacerlo con menor aprecio por los derechos que amparan al resto de ciudadanos- para encontrar algún modo de cortar a los internautas "sospechosos de traficar con material protegido" el servicio de conexión a Internet. Incluso se ofrecen "para que los dueños de los derechos puedan proporcionar detectores de direcciones IP sospechosas sin saber el nombre de la persona tras la dirección".

La falta de garantías procesales mínimas ya era evidente, tras varias sentencias desfavorables a iniciativas similares emprendidas por las gestoras francesas de derechos de autor (Moiny 2011: 352-355). Pese a las dudas, SGAE y otras entidades españolas confiaban en esa vía para que las operadoras y proveedores de conexión a Internet pudieran "limitar o eliminar" el servicio por el que pagan sus suscriptores sin violar las leyes españolas sobre privacidad (16).

Como era previsible, muchas de las acciones legales instadas por la SGAE y sometidas a escrutinio por el personal de la embajada estadounidense terminaron en nada. A ello contribuyó una circular de la *Fiscalía General del Estado*, de mayo de 2006, en la que se determinaba que, *no pudiéndose demostrar el ánimo de lucro, el intercambio de ficheros vía P2P no es delito*. Y contra lo dispuesto en ella han ido precisamente las presiones de Estados Unidos al gobierno español, hasta materializarse en el articulado de la ley Sinde-Wert. Paradójicamente, una ley aprobada después de que las iniciativas que la inspiraron -PIPA y SOPA- fueran paralizadas o declaradas incompatibles con la constitución de los Estados Unidos (17).

8.3. ACTA

Medidas de orientación fundamentalmente punitiva contempla otra norma, el *Anti-Counterfeiting Trade Agreement* (ACTA, Dec. 3, 2010) (18) que, destinada en su primer borrador de 2007 a ser un documento comercial, se orienta más bien a establecer un marco internacional armonizado que penalice la piratería y la falsificación. Entre otras razones, por los riesgos para la salud y la seguridad que suponen los equipos de uso médico o los productos de consumo defectuosos. El Acuerdo viene motivado por el propósito de luchar contra las mafias que se lucran con este tipo de actividades, evitar las pérdidas para la industria y la disminución en la recaudación de impuestos aparejada, más que por la pretensión de incentivar la innovación tecnológica en algunos modelos de negocio.

En la práctica, sus promotores han optado por la estrategia de "discreción y liderazgo" para intentar vincular a los países de mayor peso en la industria del software y de la producción científica, cultural y audiovisual (la masa crítica estaría constituida por Australia, Canadá, la Unión Europea, Japón, Corea del Sur, México, Marruecos, Nueva Zelanda, Singapur, Suiza y Estados Unidos). Los promotores -un conglomerado de agentes públicos y privados- manifiestan su total disponibilidad para "ofrecer apoyo técnico" a los países en desarrollo (que suelen contar con instrumentos reguladores en materia de propiedad intelectual menos exigentes).

Se trata, una vez más, de hacer lo posible para sortear el siempre complicado proceso de debate público sobre cuestiones de inevitable trascendencia económica, política y social. Pese a que la Comisión Europea se mostró dispuesta a sumarse al ACTA, el pleno del Parlamento Europeo lo rechazó el 3 de julio de 2012 (478 votos en contra, 39 a favor y 165 abstenciones). En las semanas previas a la votación, una intensa campaña de movilización social consiguió hacer llegar a representantes europeos 2,8 millones de firmas (19).

Individualmente, el 26 de enero de 2012 lo firmaron una veintena de embajadores de países europeos en Tokio (España, entre ellos). Se opusieron Holanda, Chipre, Eslovaquia, Estonia y Alemania (20), aduciendo que ACTA obligaría a los proveedores de Internet a vigilar los contenidos que alojan o circulan por sus redes. Además de menoscabar la libertad de expresión, el Acuerdo autoriza a los titulares de derechos a obtener información sobre los infractores en la Red -forzando a los operadores a colaborar.

El incremento de la inseguridad jurídica de todos los internautas resulta obvio, pues ACTA convierte a los proveedores de servicios de telecomunicaciones en una especie de "policía privada del *copyright*", a los que además responsabiliza de las acciones de sus clientes.

Aunque los Estados no están obligados a incorporar a su ordenamiento jurídico las sanciones penales que propone ACTA (cárcel incluida), la clave para entender el rechazo del que ha sido objeto por actores con intereses muy diversos (entre otras, las asociaciones de consumidores, asociaciones de internautas y entidades como *RedTel*, la *Asociación Española de Operadores de Telecomunicaciones*) tiene mucho que ver con la ambigüedad y vaguedad con que se redactan y justifican sus medidas más polémicas (21). También ha contribuido a ello la falta de transparencia y de calidad democrática en el proceso elegido para su aprobación, evitando el debate público y optando por influir a las personas e instituciones con mayor capacidad de liderazgo en la toma de decisiones.

Tras analizar un borrador del ACTA que circulaba por abril de 2010, la asociación española *RedTel* se extrañó por no encontrar *ninguna mención a crear oportunidades de negocio*. Una carencia que sería explicable si su objetivo fuese combatir la piratería de bienes físicos -donde ya existen cauces comerciales legales para el mismo tipo de bienes- pero que dirigido contra la *piratería de productos en soporte digital* pasa por alto una diferencia fundamental: la escasa oferta legal de contenidos.

Similar sesgo punitivo y ausencia de propuestas para nuevos modelos de negocio se aprecia en el articulado de la *Ley Sinde*, cuyo reglamento de aplicación incluye la *Ley española de Economía sostenible* (22). Se trata de una norma inequívocamente condicionada por la presión de los lobbies de la

industria audiovisual y de las distribuidoras estadounidenses, como se pudo conocer a través de la información confidencial que facilitaron los 115 cables de *WikiLeaks* sobre el tema (23).

8.4. CETA

Entre julio y octubre de 2012, diversas fuentes han filtrado los detalles de un borrador de acuerdo entre Canadá y la Unión Europea, el *Comprehensive Economic and Trade Agreement between Canada and the European Union* (24). CETA es un acuerdo comercial diseñado para fortalecer las relaciones económicas entre Canadá y la UE a través del *libre* comercio y del aumento de las inversiones. Incluye casi al pie de la letra las disposiciones más polémicas analizadas en el ACTA en relación con el papel de los Proveedores de Servicios de Internet (ISP) y el inicio de actuaciones contra los internautas a partir de meras sospechas (los aspectos que motivaron el rechazo del Parlamento Europeo al ACTA).

Las negociaciones para la aprobación de CETA se están llevando con mayor sigilo que las del ACTA. El objetivo sigue siendo introducir las disposiciones del ACTA que no pudieron pasar los filtros del debate parlamentario, en línea con otros acuerdos comerciales (KORUS: *US Korea Free Trade Agreement* (25); TPP: *Trans-Pacific Partnership* (26); TRIPS: *Agreement on Trade Related Aspects of Intellectual Property Rights* (27)) que la industria del entretenimiento ha respaldado porque ampliaba o reforzaba el alcance de las cláusulas sobre propiedad intelectual.

En lugar de evitar infracciones contra los derechos de autor, muchos vaticinan que esta involución del marco jurídico comprometerá seriamente la seguridad para navegar por Internet, inhibirá la libertad de expresión en la red y retrasará el crecimiento en sectores tecnológicos con un peso significativo y creciente en el PIB de los países más desarrollados. En última instancia, los intereses que sus promotores pretenden defender no podrán ser satisfechos sin menoscabar seriamente los derechos civiles y políticos del conjunto de los ciudadanos, dentro y fuera del ciberespacio (28).

8.5. CISPA

La *Cyber Intelligence Sharing and Protection Act* (CISPA), o proyecto de ley H.R. 3523 de 2011, fue promovida por políticos republicanos y demócratas del *House Permanent Select Committee on Intelligence* (una instancia con varios subcomités: *Intelligence Community Management*, *Technical and Tactical Intelligence* y *Terrorism, Human Intelligence, Analysis and Counterintelligence*, entre otros) (29). El 26 de abril de 2012, obtuvo el respaldo de la Cámara de Representantes, pero está pendiente de los trámites en el Senado y de la firma del Presidente.

Se trata de una norma de calado, con objetivos mucho más amplios que los contemplados en las propuestas anteriormente comentadas para extender el alcance de los derechos de propiedad intelectual. CISPA persigue combinar intereses públicos y privados en acciones de gran alcance, haciendo de la propiedad intelectual una cuestión de seguridad nacional. Además, pretende recabar la colaboración de las empresas de ciberseguridad y de otros agentes privados, dotándoles de amplia inmunidad contra abusos potenciales (30).

Para ello, atribuye a los *proveedores de servicios de ciberseguridad* competencias considerablemente amplias, facultándoles para identificar y obtener información sobre amenazas de ciberseguridad y compartirla con otras instancias, incluyendo el gobierno federal, el ejército o las agencias de espionaje (31).

Destaca, en particular, el papel que otorga a las “entidades protegidas” y “autoprotegidas” (organizaciones o empresas -no un persona física- contratadas por un proveedor de servicios de

ciberseguridad que prestan a terceros (o a sí mismas) servicios con fines de seguridad cibernética (32). Les dota de un margen de inmunidad a todas luces excesivo, dada la ambigüedad del tipo de acciones en que pueden verse involucradas y la diversidad de procedimientos compatibles con la consecución de sus fines (33).

La *Fundación Fronteras Electrónicas* (EFF) critica la ausencia de garantías para evitar que las entidades públicas y privadas involucradas en la prevención del cibercrimen bajo la cobertura de H.R. 3523 hagan un uso de la información personal obtenida para otros fines (34). Probablemente esto explica el prematuro respaldo que CISPA ha recibido de grandes empresas como Facebook, Microsoft, IBM, Intel, Oracle y Symantec, entre otras muchas. A cambio de participar voluntariamente en el intercambio de datos, obtendrían con esta ley una inmunidad jurídica sin precedentes: podrán compartir el contenido de los mensajes de sus usuarios con las agencias de inteligencia, siempre que consideren que su contenido supone un riesgo para la seguridad informática del país (35).

Los objetivos de estas entidades en la prevención de posibles ataques informáticos (un “Pearl Harbour informático”, en la retórica de algunos políticos republicanos) difícilmente podrían alcanzarse sin vulnerar derechos básicos en materia de privacidad, secreto de las comunicaciones, libertad de expresión y otros derechos civiles. Entre los apartados más polémicos de CISPA está la definición que propone de *amenaza para la ciberseguridad*; y la inclusión de las acciones contrarias a los derechos de propiedad intelectual en una categoría muy amplia, la de “riesgo para los sistemas o redes de entidades públicas y privadas” (36).

La *American Civil Liberties Union* (ACLU) y algunos representantes demócratas opuestos a la norma coinciden en señalar que la ausencia de protecciones específicas para los ciudadanos supone una amenaza para la democracia estadounidense mayor que la que pueda suponer un ataque informático (37).

Conclusiones

El debate sobre la protección de los derechos de autor y la propiedad intelectual en Internet muestra las dificultades para encontrar un punto de equilibrio entre los intereses de las grandes compañías productoras de contenido audiovisual y los derechos civiles que amparan a los internautas. La evolución del marco normativo estatal en muchos países y de los acuerdos internacionales se ha visto distorsionada por la presión constante de las asociaciones privadas que representan los intereses de las compañías discográficas (RIAA, SGAE, etc.) para reforzar su sesgo punitivo, en detrimento claro de los derechos, libertades e intereses genuinos de millones de usuarios de la Red.

Con ello, las productoras y distribuidoras de contenidos han perdido importantes oportunidades de negocio derivadas de la evolución de los patrones de consumo entre los nativos digitales y de múltiples desarrollos tecnológicos innovadores, que algunas empresas han explotado con éxito, como sugiere un análisis detenido del *fenómeno Megaupload*.

Pero la conceptualización reciente de los delitos contra la propiedad intelectual en términos de amenazas a la ciberseguridad introduce componentes mucho más inquietantes en el debate. Supone una amenaza sin precedentes para la continuidad de una Internet libre del espionaje constante de los Estados o de organizaciones privadas sobre las acciones de sus usuarios.

Las iniciativas legislativas aquí consideradas (SOPA, PIPA, ACTA, CISPA, etc.) coinciden en abrir un amplio margen de inseguridad jurídica que permitiría a muchas compañías abusar de su posición dominante en la prestación de servicios críticos en la Internet de hoy; y ser eximidas de la responsabilidad por compartir información personal de sus clientes y usuarios con servicios de espionaje, ejércitos, policía y otras instancias públicas o privadas.

Por su capacidad para influir en el derecho interno de los países más desarrollados, los intereses que subyacen a tales propuestas pretenden abrir la vía para que cualquier Estado, autoritario o democrático, pueda presionar de manera inaceptable a los proveedores de servicios de Internet, interceptar comunicaciones, bloquear aplicaciones e interrumpir servicios que han resultado decisivos para el progreso democrático y el fortalecimiento de los derechos civiles en muchos países.

La dinámica de innovación tecnológica vertiginosa que propicia Internet dificultad la creación de un marco estable de valores y cultura de trabajo en las organizaciones. Leyes como SOPA, PIPA, ACTA y CISPA se inspiran en la concepción convencional (neoclásica) del valor, orientado al mercado. Desde este enfoque, cuesta distinguir (a) un *sentido restringido de la confianza*, como una característica relacional que debe fomentarse porque facilita el crecimiento económico; y (b) un *sentido más amplio*, a saber: la confianza de la ciudadanía en las organizaciones con las que se relaciona, y que implica cierta conciencia de la cultura y los valores corporativos que asumen, así como ciertas expectativas acerca de la capacidad ética de estas organizaciones para reconocer y resolver los dilemas éticos (Willmott 1998).

En la época de Kant eran notables los progresos en la percepción pública de pertenencia a una comunidad de alcance mundial. Afirmó que “la violación del derecho en un punto de la tierra repercute en todos los demás” (Kant 1998: 30). Y su crítica al “comportamiento inhospitalario” la dirigió contra los Estados que, dotados de un sistema jurídico desarrollado, consideraron prioritarios sus intereses comerciales e hicieron de su “visita” a varios continentes una cruel campaña de conquista y expolio.

En nuestro tiempo, se libra un conflicto encarnizado “entre una visión de Internet como mero canal para llevar productos al mercado” y “una visión de Internet como espacio público o hábitat cultural” (DeVoss y Porter 2006: 183). Internet se ha convertido en la arena donde la incapacidad para distinguir entre capital ético al servicio exclusivamente de fines comerciales y capital ético al servicio de propósitos cívicos y democráticos más amplios determina la calidad democrática de los Estados.

En la práctica, sus promotores han optado por la estrategia de “discreción y liderazgo” para intentar vincular a los países de mayor peso en la industria del software y de la producción científica, cultural y audiovisual (la masa crítica estaría constituida por Australia, Canadá, la Unión Europea, Japón, Corea del Sur, México, Marruecos, Nueva Zelanda, Singapur, Suiza y Estados Unidos). Los promotores -un conglomerado de agentes públicos y privados- manifiestan su total disponibilidad para “ofrecer apoyo técnico” a los países en desarrollo (que suelen contar con instrumentos reguladores en materia de propiedad intelectual menos exigentes).

Notas

1. RSF hizo pública su preocupación tras conocer que la empresa canadiense *Research In Motion* (RIM), fabricante de los dispositivos Blackberry, facilitó a las autoridades británicas información personal de los usuarios de su servicio de mensajería (más seguro y difícil de interceptar), tras los disturbios en Londres. La misma empresa había cedido en otras ocasiones a la presión de Estados represivos (Emiratos Árabes Unidos y Arabia Saudí, entre otros) que le exigieron aplicar herramientas de filtraje a ciertos sitios web o impedir el uso de servicios encriptados. Fuente: http://www.rsf-es.org/news/reino-unido-preocupante-colaboracion-de-blackberry-con-scotland-yard/ (acceso: 21/10/2012).

2. El 23 de enero de 2012, la URL http://www.megaupload.com solo mostraba una imagen con este contenido: “This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. District Court. A federal grand jury has indicted several individuals and entities allegedly involved in the operation of Megaupload.com and related websites charging them with the

following federal crimes: Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)), Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371), Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and Criminal Copyright Infringement (18 U.S.C §§ 2, 2319; 17 U.S.C. § 506)". Cfr. http://www.megaupload.com/banner.jpg (acceso: 23/01/2012).

3. Otras alternativas que ofrecen, además, cifrado de archivos: *iDrive*, *Comodo Online Storage*, *Wuala*, *CloudSafe*, *TeamDrive*, *JustCloud* y *SafeSync*.

4. Fuente: http://www.animaadversa.es/discos/el-precio-de-la-cultura-en-espana/1121/ (acceso: 16/10/2012). Las diferencias de precio de los CDs en Europa habían sido ya objeto de varios procesos de indagación, ante la sospecha de que obedecían a razones arbitrarias (cfr. Crombie 2001).

5. Más detalles sobre el asunto en:
http://www.macstories.net/stories/understanding-the-agency-model-and-the-dojs-allegations-against-apple-and-those-publishers/
http://uk.reuters.com/article/2012/04/11/us-apple-ebooks-idUKBRE8391JW20120411
http://publishingtrendsetter.com/industryinsight/simple-explanation-agency-model/ (acceso: 16/10/2012).

6. Cfr. http://online.wsj.com/public/resources/documents/ebooks04112012b.pdf (acceso: 16/10/2012).

7. Fuente: http://www.amazon.es/gp/feature.html?ie=UTF8&docId=1000641843 (acceso: 16/10/2012).

8. Cfr.
http://www.elpais.com/articulo/espana/EE/UU/investigo/webs/espanolas/elpepuesp/20101221elpepunac_32/Tes
(acceso: 20/10/2012).

9. Sheridan hace una descripción interesante del ambiente, las interacciones y otros detalles que le llamaron la atención en su primera visita a un gran estudio de grabación.

10. Cfr. http://www.nacionred.com/lobbies-pi/cedro-quiere-cobrar-5-euros-por-alumno-por-derechos-de-autor y http://www.elmundo.es/elmundo/2012/04/16/cultura/1334570372.html (acceso: 16/10/2012).

11. Cfr. http://www.europapress.es/portaltic/internet/noticia-dia-ley-sopa-apago-internet-20120118121407.html
https://www.eff.org/search/site/sopa
https://action.eff.org/o/9042/p/dia/action/public/?action_KEY=8173 https://www.eff.org/search/site/pipa
https://www.eff.org/search/site/cispa
https://www.eff.org/search/site/acta (acceso: 16/10/2012).

12. Cfr. http://www.leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf (acceso: 16/10/2012).

13. Cfr. http://www.govtrack.us/congress/bills/112/hr3261 (acceso: 16/10/2012).

14. Cfr. http://politechbot.com/docs/sopa.law.professor.letter.111511.pdf (acceso: 16/10/2012).

15. Cfr.
http://www.elpais.com/articulo/espana/EE/UU/investigo/webs/espanolas/elpepuesp/20101221elpepunac_32/Tes
(acceso: 19/10/2012).

16. Cfr.
http://www.elpais.com/articulo/espana/EE/UU/investigo/webs/espanolas/elpepuesp/20101221elpepunac_32/Tes
(acceso: 19/10/2012).

17. Cfr. http://www.adslzone.net/article7729-por-que-eeuu-frena-la-ley-sopa-pero-fuerza-a-espana-a-aplicar-la-ley-sinde.html (acceso: 20/10/2012).

18. Cfr. http://www.dfat.gov.au/trade/acta/Final-ACTA-text-following-legal-verification.pdf https://www.eff.org/sites/default/files/filenode/EFF_PK_v_USTR/foia-ustr-acta-response1-doc10.pdf (acceso: 16/10/2012).

19. Cfr. http://tecnologia.elpais.com/tecnologia/2012/07/04/actualidad/1341384852_955656.html (acceso: 18/10/2012).

20. Fue firmado por Austria, Bélgica, Bulgaria, República Checa, Dinamarca, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Polonia, Portugal, Rumania, Eslovenia, España, Suecia y el Reino Unido. Cfr. http://tecnologia.elpais.com/tecnologia/2012/01/26/actualidad/1327601242_933321.html (acceso: 20/10/2012).

21. Cfr. http://www.nacionred.com/legislacion-pi/hoy-es-el-dia-en-que-la-union-europea-podria-ratificar-el-acta (acceso: 20/10/2012).

22. Cfr. http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf (acceso: 16/10/2012).

23. “The Minister reacted enthusiastically to our offer of expert engagement, saying it would be valuable for GOS officials to hear what has worked and what has not worked to reduce illicit downloads” Cfr. http://www.elpais.com/articulo/espana/Cable/reunion/Gonzalez-Sinde/numero/embajada/EE/UU/elpepuesp/20101220elpepunac_23/Tes
Más detalles:
http://www.elpais.com/articulo/espana/EE/UU/ejecuto/plan/conseguir/ley/antidescargas/elpepuesp/20101203elpepunac_52/Tes

http://www.elpais.com/documentossecretos/tema/pirateria_en_espana/ (acceso: 16/10/2012).

24. http://www.laquadrature.net/en/confirmed-acta-like-outrageous-criminal-sanctions-in-ceta http://opennet.net/blog/2012/07/leaked-ceta-draft-provokes-acta-comparisons-transparency-worries (acceso: 20/10/2012).

25. http://www.eastasiaforum.org/2010/11/18/obama-will-leave-korea-without-korus-heart-but-no-seoul/ (acceso: 20/10/2012).

26. http://infojustice.org/wp-content/uploads/2011/04/Koo-TPP-Section-by-Section-Analysis-April-2011.pdf (acceso: 20/10/2012).

27. http://www.wto.org/english/tratop_e/trips_e/trips_e.htm (acceso: 20/10/2012).

28. Cfr. https://www.eff.org/deeplinks/2011/12/2011-review-developments-acta (acceso: 20/10/2012).

29. Cfr. http://www.govtrack.us/congress/bills/112/hr3523 (acceso: 20/10/2012).

30. ‘Sec. 1104. (a) Intelligence Community Sharing of Cyber Threat Intelligence With Private Sector and Utilities-
‘(1) IN GENERAL- The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities and to encourage the sharing of such intelligence.
‘(3) SECURITY CLEARANCE APPROVALS-
‘(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.

31. ‘(b) Use of Cybersecurity Systems and Sharing of Cyber Threat Information-
‘(1) IN GENERAL-

‘(A) CYBERSECURITY PROVIDERS-
‘(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and
‘(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.

32. ‘(11) PROTECTED ENTITY- The term ‘protected entity’ means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.
‘(12) SELF-PROTECTED ENTITY- The term ‘self-protected entity’ means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

33. ‘(4) EXEMPTION FROM LIABILITY- No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith–
‘(A) for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or
‘(B) for decisions made based on cyber threat information identified, obtained, or shared under this section.

34. Cfr. https://www.eff.org/pages/no-digital-big-brother-keep-military-out-your-email (acceso: 20/10/2012).

35. Cfr. http://alt1040.com/2012/04/cispa-la-nueva-sopa-va-muy-en-serio-lista-de-las-grandes-companias-que-apoyan-la-legislacion (acceso: 20/10/2012).

36. ‘(5) CYBER THREAT INTELLIGENCE-
‘(A) IN GENERAL- The term ‘cyber threat intelligence’ means intelligence in the possession of an element of the intelligence community directly pertaining to–
‘(i) a vulnerability of a system or network of a government or private entity;
‘(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or any information stored on, processed on, or transiting such a system or network;
‘(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity; or
‘(iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity.
Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

37. Cfr. http://www.aclu.org/stop-cyber-spying; y http://sociedad.elpais.com/sociedad/2012/04/27/vidayartes/1335555403_669308.html (acceso: 21/10/2012).

Bibliografía

Bhattacharjee, Sudip (y otros)
2006 “Whatever happened to payola? An empirical analysis of online music sharing”, *Decision Support*

Systems, 42/1 (Oct.): 104-120.

Beuscart, Jean-Samuel
2005 “Napster users between community and clientele: The formation and regulation of a sociotechnical group”, *Sociologie du Travail*, 47 (Dec.): e1-e16.

Choi, David (y Arturo Pérez)
2007 “Online piracy, innovation, and legitimate business models”, *Technovation*, 27/4 (April): 168-178.

Crombie, Lynn
2001 “Brussels inquiry into price of CDs”, en http://edition.cnn.com/2001/WORLD/europe/01/26/commission.cd/index.html

DeVoss, Dànielle Nicole (y James E. Porter)
2006 “Why Napster matters to writing: Filesharing as a new ethic of digital delivery.” *Computers and Composition* 23:2 (January): 178-210.

DeVoss, Dànielle Nicole (y Suzanne Webb)
2008 “Media Convergence: Grand Theft Audio: Negotiating Copyright as Composers”, *Computers and Composition*, Vol. 25/1: 79-103.

Feenberg, Andrew
2002 *Transforming technology: A critical theory revisited*. Oxford, Oxford University Press.

Hayes, David L.
2001 “Advanced copyright issues on the Internet, PART V”, *Computer Law & Security Report*, 17/1: 219-232.

Hellwig, E.
2002 “Memo to the Record Companies: Downloading Can’t Be Stopped”, *Business 2.0* (Mar. 6).

Hong, Seung-Hyun
2007 “The recent growth of the internet and changes in household-level demand for entertainment”, *Information Economics and Policy* 19/3-4 (October): 304-318.

Isaacson, Walter
2011 *Steve Jobs*. New York, Simon & Schuster.

Kant, Immanuel
1998 *Sobre la paz perpetua*. Trad. de Joaquín Abellán. Madrid, Tecnos, 6ª edic. (orig.: *Zum ewigen Frieden. Ein philosophischer Entwurf*. 1795).

Kleve, Pieter (y Richard De Mulder, Kees van Noortwijk)
2007 “Information technology in intellectual property law – Problem solving or window dressing?”, *Computer Law & Security Review* 23/5 (January): 427-435.

Lessig, Lawrence
2004 *Free culture: How big media uses technology and the law to lock down culture and control creativity*. New York, The Penguin Press.

Mahanti, Aniket (y otros)
2011 “Characterizing the file hosting ecosystem: A view from the edge”, *Performance Evaluation*, 68: 11 (Nov.): 1085-1102.

McKee, Heidi A.

2008 “Ethical and legal issues for writing researchers in an age of media convergence”, *Computers and Composition*, Vol. 25/1: 104-122.

Merlo, Alessio
2012 “Hacktivists hit out at Symantec, police and anti-piracy groups”, *Network Security,* nº 2 (Feb. 2012): 1-2.

Moiny, Jean-Philippe
2011 “Are Internet protocol addresses personal data? The fight against online copyright infringement”, *Computer Law & Security Review* 27/4 (August): 348-361.

Perritt, Henry H.
1994 “Protecting intellectual property rights on the information superhighway: A review of *Protecting intellectual property rights on the information superhighway*, by Joseph L. Ebersole (Washington, DC, Information Industry Association, 1994)”, *The Journal of Academic Librarianship*, Vol. 20/5-6.

Prensky, Marc
2001 “Digital natives, digital immigrants”, *On the Horizon*, 9 (5): 1-6. Disponible en: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (acceso: 18/10/2012).

Pryor, Andrew (y otros)
2008 “Buy or burn?: Empirical tests of models of crime using data from a general population”, *The Social Science Journal*, 45/1 (March): 95-106.

Radcliffe, Mark F.
2006 “Grokster: The new law of third party liability for copyright infringement under United States law”, *Computer Law & Security Review*, 22/2 (Jan.): 137-149.

RSF (Reporters Without Borders)
2012 *Enemies of the Internet. Report 2012*. Disponible en: http://issuu.com/rsf_webmaster/docs/rapport-internet2012_ang?mode=window&backgroundColor=%23222222 (acceso: 15/10/2012).

Sano-Franchini, Jennifer Lee
2010 “Intellectual Property and the Cultures of BitTorrent Communities”, *Computers and Composition*, 27/3 (Sept.): 202-210.

Saxby, Stephen
2000 “News and comment on recent developments from around the world: Recording industry launches several law suits to protect music copyrights on the Web”, *Computer Law & Security Review*, Vol. 16/5 (Oct.): 352-353.

Selber, Stuart A.
2004 *Multiliteracies for a digital age*. Carbondale, Southern Illinois University Press.

Sheridan, Rob
2007 “When pigs fly: The death of Oink, the birth of dissent, and a brief history of record industry suicide. demonbaby”, en: http://www.demonbaby.com/blog/2007/10/when-pigs-fly-death-of-oink-birth-of.html (acceso: 18/10/2012).

Stiegler, Bernard
1998 *Technics and time, 1: The fault of Epimetheus*. (Richard Beardsworth & George Collins, Trans.). Stanford, CA, Stanford University Press.

2008 *Technics and time, 2: Disorientation*. (Stephen Barker, Trans.). Stanford, CA, Stanford University Press.

Vaidhyanathan, Siva
2001 *Copyrights and copywrongs: The rise of intellectual property and how it threatens creativity*. New York, New York University Press.

Wang, Xiao (y Steven R. McClung)
2012 "The immorality of illegal downloading: The role of anticipated guilt and general emotions", *Computers in Human Behavior*, 28/1 (January): 153-159.

Willmott, Hugh
1998 "Towards a new ethics? The contributions of poststructuralism and posthumanism", en M. Parker (ed.), *Ethics & organization*. London, Sage: 76-121.

Zentner, Alejandro
2006 "Measuring the Effect of File Sharing on Music Purchases", *Journal of Law and Economics*, Vol. 49/1 (April): 63-9