IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios

Raquel Xalabarder Plantada

Resumen

A raíz de su posición de intermediarios necesarios, los ISP (*Internet service providers*) «contribuyen» de alguna manera a las infracciones que se cometen en Internet y, por lo tanto, a partir de las reglas generales de atribución de responsabilidad, podrían ser declarados responsables por las infracciones cometidas por sus clientes y usuarios. En este artículo se examina el régimen de exención de responsabilidad que, a modo de compromiso entre los ISP y los titulares de los contenidos, se contiene en la Digital Millennium Copyright Act norteamericana de 1998 y en la Directiva 2000/31/CE, de 8 de junio del 2000, de Comercio Electrónico, que en España fue implementada por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Examinaremos las diferencias y las coincidencias en la atribución de responsabilidad a los ISP por la prestación de servicios de acceso y mera transmisión, de *hosting* y de *caching*, así como la jurisprudencia en los distintos países europeos, pero también el caso de Estados Unidos, país que ha ido llenando los huecos dejados por el legislador en temas tan fundamentales como la responsabilidad de los ISP por las páginas con contenidos infractores accesibles a través de motores de búsqueda y por los enlaces a material infractor contenidos en las páginas que ellos almacenan.

Palabras clave

Internet, infracciones, responsabilidad, *Internet service providers*, DMCA, DCE, LSSICE

Tema

Propiedad intelectual

Abstract

As necessary intermediaries, ISP (*Internet Service Providers*) somehow "contribute" to the infringements committed by users over the Internet and might, consequently –in accordance with general rules on liability–, be deemed liable for any infringements committed by their clients and users. This article will examine the exemptions from liability adopted as a compromise between ISP and content owners, in the U.S. *Digital Millennium Copyright Act* of 1998 and the European *Directive 2000/31/CE, of June 8th 2000, on electronic commerce,* which has been implemented into Spanish law by *Law 34/2002, of April 11th, on Services of the Information Society and Electronic Commerce.* We will examine the differences and coincidences in the allocation of liability on ISP for providing services of access and transmission, of hosting and caching, as well as case law from European countries and the USA, which has been "filling the gaps" left by the legislator concerning issues as important as ISP liability for infringing contents accessed through search engines and for links to infringing contents available on web pages hosted by them.

Keywords

Internet, infringement, liability, Internet Service Providers, DMCA, DCE, LSSICE

Topic

Intellectual property

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

Debido a su posición de intermediarios necesarios, los ISP «contribuyen» de alguna manera a la comisión de la infracción y, por lo tanto, en base a las reglas generales de atribución de responsabilidad, podrían ser declarados responsables. La batalla para establecer un régimen especial de responsabilidad para los ISP empezó ya en 1995 en Estados Unidos, en el seno de la *National Information Infrastructure –NII*[1] (donde se concluyó que era «*cuanto menos, prematuro*» excluir o reducir la responsabilidad de los ISP por las infracciones de propiedad intelectual que sus usuarios cometieran) y continuó en la arena internacional, con ocasión de la aprobación de los *«Tratados Internet» de la OMPI* de 1996[2] (donde los ISP volvieron a defender sus intereses, consiguiendo evitar que se les declarara responsables por las infracciones de propiedad intelectual cometidas en Internet). Al final, se alcanzó un compromiso incorporado, por primera vez, en la *Digital Millennium Copyright Act* norteamericana, de 28 de Octubre de 1998[3] (en adelante, **DMCA**), y dos años después en la Directiva 2000/31/CE, de 8 de junio de 2000, de comercio electrónico[4] (en adelante, **DCE**). En España, la DCE fue implementada por la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico[5] (en adelante, **LSSICE**).

En este artículo, examinaremos y compararemos las soluciones legislativas y jurisprudenciales adoptadas en ambos lados del Atlántico, para eximir de responsabilidad a los ISP por las infracciones (de todo tipo) cometidas por sus usuarios.

1. Algunos comentarios previos en relación con ambos regímenes

Una diferencia fundamental entre ambos sistemas norteamericano y europeo es la llamada **aproximación vertical frente a horizontal**. Mientras que la DMCA sólo exime a los ISP de responsabilidad por las infracciones de propiedad intelectual, la DCE les exime de responsabilidad por infracciones de cualquier tipo. El motivo de la aproximación horizontal de la DCE se explica porque la divergencia normativa y jurisprudencial nacional en materia de responsabilidad de los ISP podría *«entorpecer el correcto funcionamiento del mercado interior al*

1. Libro blanco sobre *«Propiedad intelectual y la Infraestructura de Información Nacional»*: http://www.uspto.gov/web/offices/com/doc/ipnii/.
2. En el marco de la conferencia diplomática de la OMPI que debatía (tras cinco años de reuniones) diversas actualizaciones puntuales (técnicas) del lenguaje del Convenio de Berna para la protección de las obras literarias y artísticas, y del Convenio de Roma para la protección de los llamados «derechos conexos». Los llamados «Tratados Internet» de la OMPI se pueden consultar en su página web: http://www.wipo.org; Concretamente, el Tratado OMPI Derecho de Autor: http://www.wipo.int/treaties/es/ip/wct/index.html y el Tratado OMPI sobre Interpretación o Ejecución y Fonogramas: http://www.wipo.int/treaties/es/ip/wppt/index.html.
3. La DMCA está disponible en el web de la Copyright Office: http://www.copyright.gov.
4. *Vid.* http://www.europa.eu.int/comm/internal_market/en/ecommerce/index.htm. En el momento de preparar este artículo, la DCE ya ha sido implementada en Austria (Ley 152/2001 de 21 Diciembre 2001), Bélgica (Leyes de 11 de marzo de 2003), Dinamarca (Ley 227/2002 de 22 abril 2002), Finlandia (Ley 458/2002 de 5 junio 2002), Francia (Ley 719/2000 de 1 agosto 2000 y Ley 575/2004 de 21 junio 2004), Grecia (Decreto 131/2003 de 16 mayo 2003), Islandia (Ley 30/2002 de 16 abril 2002), Irlanda (Reglamento 68/2003 de 24 febrero 2003), Italia (Decreto 70/2003 de 9 abril 2003), Luxemburgo (Ley de 14 agosto 2000), Noruega (Ley de 23 mayo 2003 y Ley de 20 febrero 2004), Portugal (Decreto 7/2004 de 7 enero 2004), España (Ley 24/2002 de 11 julio 2002, LSSICE), Suecia (Ley de 6 junio 2002), el Reino Unido (Reglamento 2013/2002 de 21 agosto 2002) y Holanda (Ley de mayo 2004, que implementa la DCE, a través de modificaciones puntuales de diversas leyes y reglamentos).
5. Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE); modificada por la Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones (LGT).
Vid. http://www.setsi.mcyt.es/legisla/internet/ley34_02/sumario.htm.

obstaculizar el desarrollo de servicios transfronterizos y producir distorsiones de la competencia» (cons.40). En Estados Unidos, otras leyes sectoriales vienen a «completar» la exención parcial de responsabilidad de los ISP que hace la DMCA (por ser una ley de modificación de la *Copyright Act*). En este sentido, hay que mencionar la *Telecommunications Decency Act* de 1996,[6] cuya cláusula del «buen samaritano» (*Good Samaritan*) permite la exención de responsabilidad de algunos ISP por las actuaciones de sus usuarios en Internet. Aunque inicialmente estaba prevista para la responsabilidad por «*third party speech*» (difamaciones, afirmaciones falsas, etc. cometidas por usuarios de Internet), su alcance se ha ido expandiendo hasta cubrir la responsabilidad por todo tipo de infracciones civiles, salvo en los ámbitos expresamente excluidos –en concreto, la propiedad intelectual y las materias de competencia federal, especialmente las reguladas por leyes federales contra la obscenidad y la pornografía infantil. De todas maneras, la aproximación horizontal de la DCE sigue siendo más amplia que la norteamericana. Un ISP podría quedar exento de responsabilidad por infracción de una marca en la UE, pero no en Estados Unidos. Por ejemplo, Mindspring, un ISP que almacenaba una página web que anunciaba relojes de imitación, fue declarado responsable por tal infracción, ya que ni la TDA ni la DMCA eran aplicables para eximir de responsabilidad al ISP por la infracción de marca –*vid.* Gucci *vs.* Hall, 135 F.Supp. 2d 409 (S.D.N.Y. 2001). En Europa, Mindspring hubiera quedado fácilmente eximido de tal responsabilidad, con el simple cumplimiento de las condiciones del «*safe-harbor*» de alojamiento de datos («*hosting*») del art.14 DCE y correspondientes leyes nacionales (por ejemplo, *vid.* art.16 LSSICE).

La segunda consideración importante, al comparar ambos sistemas, es que mientras que la DMCS sólo cubre la **exención de la responsabilidad por «daños y perjuicios»** (es decir, la compensación económica), la DCE exime de cualquier tipo de responsabilidad. Como tendremos ocasión de ver, esta diferencia explica alguna de las especificidades de la DCE, en comparación con la DMCA, y además será motivo de posibles interpretaciones contradictorias (o cuanto menos, diferentes) a nivel nacional, lo cual no favorece el camino hacia la pretendida harmonización.

Tanto la DMCA como la DCE se basan en una lista de escenarios, conocidos como *safe-harbors* en los que –si se cumplen unas condiciones concretas– el ISP no será responsable por la infracción cometida por su usuario. En principio, el simple incumplimiento de alguna de estas condiciones impide al ISP beneficiarse de la exención, pero no necesariamente le asigna responsabilidad por la infracción. **El régimen de safe-harbors sólo sirve como un primer «filtro»**: la responsabilidad de cada ISP se establecerá de acuerdo con las reglas generales de responsabilidad, ya sea mediante la doctrina de la responsabilidad secundaria (*secondary liability*)[7] en Estados Unidos, o como colaborador necesario o responsable civil por hecho ajeno en los países de tradición roma-

6. Telecommunications Decency Act de 1996: http://www.fcc.gov/telecom.html; *vid.* sec.230(c): *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*

7. En Estados Unidos, dos son las doctrinas para establecer la existencia de «responsabilidad secundaria» (es decir, por hecho ajeno) por infracciones de la propiedad intelectual: *vicarious liability* y *contributory infringement*. En base a la doctrina establecida en Shapiro, Bernstein & Co. *vs.* H.L. Green Co., 316 F.2d 204 (2c Dir 1963), se acepta que existe responsabilidad (*vicarious liability*) por una infracción de la propiedad intelectual cometida por un tercero, cuando se cumplan dos requisitos: la capacidad (y derecho) de supervisar la actividad infractora y la existencia de un interés económico en la misma. Así pues, la decisión de si existe o no *vicarious liability* se centrará en el examen del grado de supervisión que el ISP tiene (no necesariamente, ejerce) sobre la actividad infractora y del beneficio económico que obtiene de ella (ya sea directo o indirecto).
La doctrina jurisprudencial del *contributory infringement* aparece posteriormente como una adaptación de la doctrina del *vicarious liability*: quien, con conocimiento de la actividad infractora, induce, causa o contribuye materialmente a la conducta infractora de un tercero, puede ser declarado responsable como infractor «contribuyente» –*vid. Gershwin vs. Columbia*, 443 F.2d 1159 (2d Cir. 1971). Desde entonces, se considera que existe *contributory infringement* cuando se conoce y se facilita la producción de la infracción por parte de tercero. Así pues, las cuestiones que se plantean al decidir si existe o no *contributory infringement* se centran, además de en la definición de «contribuir» a la infracción, en el examen del grado de conocimiento que el ISP tiene de la actividad infractora (¿específico o general? ¿anterior o posterior a la infracción? ¿puede el ISP «cerrar los ojos» ante la infracción? etc.).
En el famoso caso «Betamax», *Sony vs. Universal*, 464 U.S. 417 (1984), la *Supreme Court* examinó ambas doctrinas antes de concluir que no existía responsabilidad alguna por parte de Sony por la fabricación de aparatos grabadores/reproductores de vídeo, que podían ser utilizados para copiar películas sin autorización de los titulares de derechos.

nista.[8] Sin embargo, se trata éste de un tema poco pacífico y deberemos esperar a que los diversos legisladores nacionales, o los tribunales nacionales, se manifiesten al respecto. Lo que queda claro es que tanto en la DCE como en la DMCA, es necesario que exista una infracción «de base» por parte del tercero (usuario).

Por otro lado, ninguno de ambos regímenes de exención de responsabilidad afectan ni impiden la adopción por parte de los tribunales, o autoridades administrativas correspondientes, de **órdenes que exijan la terminación o eviten la comisión de una infracción**, incluidas la supresión de información ilegal o el desmantelamiento del acceso a la misma.[9] Más aún, si un ISP desobedece una de estas órdenes no podrá beneficiarse de la exención de responsabilidad correspondiente.

2. Supuestos de exención de responsabilidad de los ISP (*safe-harbors*)

La DCE establece **tres *safe-harbors*: de mera transmisión, de memoria tampón (*caching*) y de alojamiento de datos (*hosting*),** en los que la responsabilidad del ISP puede quedar exenta cuando se cumplan con las condiciones específicas que se establecen para cada uno de ellos.

Art. 12. Mera transmisión

1. Los Estados miembros garantizarán que, en el caso de un servicio de la sociedad de la información que consista en transmitir en una red de comunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones, no se pueda considerar al prestador de servicios de este tipo responsable de los datos transmitidos, a condición de que el prestador de servicios:

a) no haya originado él mismo la transmisión;
b) no seleccione al destinatario de la transmisión, y
c) no seleccione ni modifique los datos transmitidos.

2. Las actividades de transmisión y concesión de acceso enumeradas en el apartado 1 engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión.

3. El presente artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida.

Art.13. Memoria tampón («Caching»)

1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, el prestador del servicio no pueda ser considerado responsable del almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos, a condición de que:

8. Para un estudio de derecho comparado sobre la tipología de la responsabilidad (civil y penal) por hecho ajeno en los sistemas del *common law* y los sistemas de tradición romanista, *vid.* K. Koelman, B.P. Hugenholtz, *Online Service Provider Liability for Copyright Infringement*, WIPO Workshop on Service Provider Liability, Geneva (Dec.1999), disponible en: http://www.ivir.nl/publicaties/hugenholtz/wipo99.pdf.

9. *Vid.* arts.12, 13, y 14 DCE: «*El presente artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida*».

a) el prestador de servicios no modifique la información;

b) el prestador de servicios cumpla las condiciones de acceso a la información;

c) el prestador de servicios cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector;

d) el prestador de servicios no interfiera en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información, y

e) el prestador de servicios actúe con prontitud para retirar la información que haya almacenado, o hacer que el acceso a ella sea imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se encontraba inicialmente, de que se ha imposibilitado el acceso a dicha información o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella.

2. El presente artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios poner fin a una infracción o impedirla.

Art. 14. Alojamiento de datos («Hosting»)

1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:

a) el prestador de servicios no tenga conocimiento efectivo de que la actividad o la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que,

b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

2. El apartado 1 no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios.

3. El presente artículo no afectará la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de servicios de poner fin a una infracción o impedirla, ni a la posibilidad de que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos.

A modo de resumen, un ISP se podrá beneficiar de las **exenciones de mera transmisión y de memoria tampón (*caching*)** cuando su participación sea de naturaleza meramente técnica, automática y pasiva, de manera que el ISP no tenga ni conocimiento ni control sobre la información transmitida o almacenada. Ello presupone, entre otras cosas, que el ISP no modifique la información transmitida,[10] que no interfiera con los mecanismos establecidos en origen,[11] y –en el caso del *caching*–[12] que actúe con prontitud para retirar los datos o impedir su acceso cuando tenga conocimiento de que los mismos

10. Tal como recoge el considerando 43 de la DCE, este requisito no abarca las manipulaciones de carácter técnico que tienen lugar en el transcurso de la transmisión, puesto que no alteran la integridad de los datos contenidos en la misma.
11. Por ejemplo, para el cómputo del número de visitas a la página web, o el acceso protegido mediante contraseña o páginas web encriptadas, etc.
12. En este punto, cabe mencionar el Auto de 10 de Noviembre de 2004 del Juzgado de lo Mercantil n.º 2 de Madrid, en relación con una medida cautelar solicitada para obligar a Bitmailer, S.L. a cesar en la provisión del servicio de acceso a Internet a la empresa NetProvider S.A., operadora de la página web http://www.weblisten.com. El Juzgado concluye que, a diferencia de los supuestos previstos para el «*hosting*» (art. 16 LSSICE) y el «*caching*» (art. 15 LSSICE), el art. 14 LSSICE (acceso y mera transmisión) no obliga a los proveedores de acceso a Internet a la cesación o a la retirada de contenidos, propiamente. En este caso, los demandantes no aportaron pruebas suficientes para fundamentar que Bitmailer prestara, además de los servicios de acceso y mera transmisión, alguno de ambos servicios («*hosting*» o «*caching*») para NetProvider, y el Juzgado denegó la medida cautelar solicitada.

han sido retirados o su acceso ha sido deshabilitado en origen, o de que un tribunal o autoridad administrativa haya ordenado su retirada o acceso. Estos *safe-harbors* han sido transpuestos en los arts.14 a 16 de la LSSICE.[13]

Basta decir que tanto los escenarios, como las condiciones específicas establecidas para cada uno de ellos, son paralelos a los *safe-harbors* de la sec.512 DMCA.[14]

Para la **exención por almacenamiento (*hosting*)**, se establece un doble nivel de ausencia de conocimiento, por parte del ISP, acerca de la ilicitud de la información almacenada: «**conocimiento efectivo**» y «**conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito».** La DMCA (sec.512) también recoge este doble nivel de conocimiento, como **actual *knowledge* y *awareness***, respectivamente, siendo conocido este último como el ***red-flag-test***: la ilicitud debe ser «aparente». La simple existencia de circunstancias «sospechosas» de que ocurre un ilícito no es suficiente para responsabilizar al ISP. De esta manera se refuerza el principio de que el ISP no tiene obligación de supervisar ni controlar las páginas y acciones de sus usuarios, ni siquiera cuando existan circunstancias «sospechosas». Al final, pues, el nivel de (des)conocimiento exigido para la exención de responsabilidad por daños y perjuicios es el mismo bajo ambos sistemas: ausencia de «conocimiento efectivo» y de ***awareness***. Por supuesto, para poder seguir beneficiándose de la exención por **alojamiento (*hosting*)**, al tener conocimiento efectivo o ***awareness*** de la existencia de un ilícito, el ISP debe actuar con prontitud para eliminar o impedir el acceso a la información o actividad ilícita.

Sin embargo, más allá de la simple responsabilidad por daños y perjuicios, existe una diferencia importante. El art.14 DCE[15] distingue implícitamente, entre «responsabilidad» en general, por un lado, y responsabilidad «en lo que se refiere a una acción por daños y perjuicios», por otro, y las sujeta a un diferente nivel de (des)conocimiento. La vaguedad y falta de concreción jurídica de este artículo deja amplio margen a los Estados miembros al interpretar para qué tipo de responsabilidad se exige la ausencia de conocimiento. Así, por ejemplo, la ley belga exige conocimiento efectivo para las acciones criminales (definiendo como tal cuando la infracción ha sido debida y formalmente notificada al ISP) y *awareness* para las acciones de indemnización (entendiendo por *awareness* cuando la infracción ha sido de alguna manera puesta en conocimiento del ISP o que las circunstancias hacen que la misma sea aparente). En cambio, en España, la ausencia de conocimiento efectivo no sólo se exige para eximir al ISP de todo tipo de responsabilidad, ya sea civil o criminal (*vid.* art.16 LSSICE), sino que además se le añade un segundo requisito: que la ilicitud haya sido establecida por la «autoridad competente» y que el ISP haya sido debidamente notificado.

El panorama promete ser todavía más interesante a medida que la jurisprudencia decida sobre este extremo, y en especial, si se tiene en cuenta que la DCE no sólo no define cuándo existe «conocimiento efectivo» y cuándo existe *awareness*, sino que además permanece en silencio sobre en quién recae la carga de la prueba de tales extremos Por ejemplo, bajo la ley alemana, el titular del derecho debe demostrar que el ISP tenía conocimiento de la ilicitud. En cambio, bajo la DMCA, el ***onus probandi*** recae sobre el ISP: deberá demostrar que no tenía conocimiento de la infracción.[16] A ello se añade que, a dife-

13. *Vid.* http://www.setsi.mcyt.es/legisla/internet/ley34_02/tit2.htm#a14
14. *Vid.* sec.512 USCA: http://www.copyright.gov
15. Es posible aventurar que esta falta de precisión en el lenguaje (en definir qué tipo de responsabilidad queda cubierta por la DCE) se deba a la inseguridad de la UE sobre su propio ámbito de competencia en materia de responsabilidad penal –siendo, tradicionalmente, la legislación penal un área reservada a los Estados miembros.
16. Lo cual, al final, puede conducir a un escenario curioso: que sea más difícil exonerar al ISP de responsabilidad por la infracción de PI –bajo la DMCA, que bajo las reglas generales del *contributory infringement,* según las cuales el ***onus probandi*** recaería en el titular del derecho infringido.

rencia de la DMCA, la DCE no dispone de ningún mecanismo de aviso y retirada que podría aportar medios de prueba en este sentido.

3. Lo que no dice la DCE

A diferencia de la DMCA, la DCE no contiene:

- Ningún *safe harbor* para motores de búsqueda y enlaces;
- Ningún proceso de aviso y retirada (*notice and take down*);
- Ninguna disposición sobre la posibilidad de ordenar al ISP que comunique al titular de los derechos infringidos la información relativa al supuesto infractor (que en la DMCA se conoce como *subpoena injunctions*).

En lugar de una regulación expresa –como hace la DMCA– de un proceso de «detección y retirada», la DCE optó por encargar a los Estados miembros y a la Comisión que fomenten «*la elaboración de códigos de conducta a nivel comunitario, a través de asociaciones u organizaciones comerciales, profesionales o de consumidores*» (*vid.* art.16(1)(a) DCE). La necesidad de regular tales procesos de «detección y retirada», así como la necesidad de introducir una exención de responsabilidad específica para motores de búsqueda e hiperlinks, será objeto de especial consideración en los subsiguientes informes sobre la aplicación de la DCE que la Comisión deberá realizar bianualmente.[17] El primer informe sobre la aplicación de la DCE (*vid.* 2000/31/CE, COM(2003)702 final) niega que exista la necesidad de realizar acción alguna en ninguno de los dos temas, e incluso llega a afirmar que las acciones tomadas hasta el momento por los Estados miembros pongan en peligro el pacífico funcionamiento del mercado interior.[18] Veamos si ello es así.

I. Un somero repaso a la diversidad de acciones y soluciones adoptadas en algunos países miembros no ofrece un panorama tranquilizador.

A. En primer lugar, porque el silencio de la DCE sobre una exención específica para los **motores de búsqueda e *hiperlinks***, no significa que los legisladores nacionales no puedan introducirla a nivel nacional (y establecer las condiciones concretas para beneficiarse de la misma), con lo cual poca harmonización se puede esperar en esta materia. En segundo lugar, porque si bien la mayoría de leyes nacionales de transposición de la DCE han preferido ser prudentes y no incluyen referencia alguna al tema, algunas sí lo hacen, y lo hacen de manera poco uniforme. Así, por ejemplo, la **LSSICE** española en su art.17[19] introduce una cuarta exención específica para motores de búsqueda e *hiperlinks*, directamente «inspirado» de la DMCA. De forma similar, **Portugal** introduce una exención para motores de búsqueda e *hiperlinks* sujeta a las mismas condiciones previstas para la exención de *hosting*. **Hungría** optó por introducir una exención para motores de búsqueda, pero no para los *hiperlinks*. También **Austria y Liechtenstein** (país miembro del Espacio Económico Europeo) han introducido exenciones específicas para los motores de búsqueda y los *hiperlinks*, pero sujetándolas a condiciones distintas: la exención de responsabilidad por motores de búsqueda queda sujeta a las mismas condiciones establecidas para la exención por mera transmisión (art.12 DCE) y la exención de responsabilidad por los *hiperlinks* queda sujeta a las condiciones del *hosting* (art.14 DCE).

En **Francia**, en cambio, la responsabilidad por la provisión de motores de búsqueda y enlaces a páginas con contenido infractor ha sido tratada no por el legislador, sino por el «*Forum des Droits sur Internet*»[20] (una organización compuesta por industria y usuarios) concluyendo que quien introduce un enlace a contenido infractor sólo

17. En este sentido, el art.21(2) DCE establece: «*Al examinar la necesidad de adaptar la presente Directiva, el informe analizará especialmente la necesidad de presentar propuestas relativas a la responsabilidad de los proveedores de hipervínculos y servicios de instrumentos de localización, a los procedimientos de "detección y retirada" y a la imputación de responsabilidad tras la retirada del contenido.*»
18. *Vid.* Primer informe de la Comisión sobre la aplicación de la Directiva 2000/31/CE de comercio electrónico, COM(2003)702 final, #4.6 y #4.7. http://www.europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf
19. *Vid.* http://www.setsi.mcyt.es/legisla/internet/ley34_02/tit2.htm#a17
20. *Vid.* http://www.foruminternet.org/recommandations/

puede ser declarado responsable penal si se demuestra que tenía la intención de cometer una infracción o de participar en la misma y sólo podrá ser declarado civilmente responsable (indemnización por daños y perjuicios) cuando su actuación carezca de la mínima prudencia debida (y establece criterios para determinar cuándo se produce una actuación imprudente).

En otros países, la jurisprudencia se ha adelantado al legislador, con soluciones también dispares. En materia de enlaces, las soluciones jurisprudenciales toman prestados algunos de los criterios recogidos en la exención por *hosting*. Así, por ejemplo, en **Bélgica**, Belgacom Skynet fue declarado responsable por el alojamiento de páginas web que contenían enlaces a ficheros de mp3 ilícitos, argumentando que el ISP debería tener conocimiento del carácter ilícito de tales enlaces y los debería haber deshabilitado diligentemente (*IFPI Belgium vs. SA Belgacom Skynet*, Prés. Comm Bruxelles, 2 Noviembre 1999, y en apelación: Bruselas, 8ª Ch., 13 Febrero 2001); y en otro caso, se declaró que la persona que introduce un enlace a una página web con contenido ilegal (pornografía infantil) comparte la misma responsabilidad penal que el propietario de tal página web. (*Affaire Ministère Public vs. VR*, Trib. Corr. Hasselt , 18ª Ch., 1 Marzo 2002, y en apelación: Amberes, 10ª Ch., 7 Octubre 2003). En **Holanda**, el operador de una página web que contenía enlaces a escritos de grupos radicales (que eran constitutivos de delito) fue obligado a deshabilitar tales enlaces, aplicándole las mismas reglas y condiciones previstas para la exención por *hosting* (*Deutsche Band vs. Indymedia*, Tribunal de Distrito, Ámsterdam, 20 Junio 2002). En **Francia,** si bien el operador de una página web que contenía enlaces a ficheros mp3 ilícitos fue declarado responsable por tal infracción, no se dijo nada respecto a la responsabilidad del ISP que alojaba esa página web (*SACEM vs. VR & VR*, Trib. Corr. Epinal, 24 Octubre 2000); En cambio, *voilà.fr* no fue declarado responsable –sobre la base de las reglas generales de responsabilidad– por los enlaces resultantes de las búsquedas (efectuadas por sus usuarios a través del motor de búsqueda de *voila.fr*) a una página web que contenía fotos ilícitas de un cantante (*LORIE vs. Wanadoo*, TGI Paris, 12 Mayo 2003). Merece la pena, mencionar aquí una sentencia de los **Estados Unidos**, por la cual se declaró la responsabilidad por la introducción de un enlace a una página web ajena con contenido ilícito, ya que el operador del enlace conocía (o tenía motivos para conocer) la naturaleza ilícita del contenido enlazado (*Intellectual Reserve Inc. vs. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999).

En cambio, por lo que respecta al uso de ***metatags*** a través de motores de búsqueda, las soluciones son todavía más impredecibles. Los *metatags* son una palabra incorporada en el código html de una página web que es utilizada por los motores de búsqueda y portales para clasificarla y mostrarla al público. Aunque los *metatags* no son visibles para el usuario «normal», tienen una significación económica fundamental, ya que la clasificación y ordenación de las páginas web resultantes se realiza sobre la base de la cantidad de referencias (a esa palabra) que contenga cada página. En tanto los *metatags* sean palabras comunes, no se presenta problema alguno de infracción de propiedad intelectual o industrial. En cambio, cuando la palabra utilizada como *metatag* sea una marca registrada o un título o nombre de obra protegida, entonces su utilización no autorizada puede ser constitutiva de infracción. Es común utilizar nombres de marcas de productos ajenos para atraer a su página al usuario que realiza una búsqueda de tales productos. Se trata, pues, de identificar si el uso de una marca ajena como *metatag* de la página web propia constituye infracción y cuál es la responsabilidad del ISP que gestiona el motor de búsqueda que hace posible que el *metatag* surta los efectos previstos. En principio, el uso de una marca ajena en relación con productos y servicios en el mercado constituye infracción: la cuestión es, pues, decidir si la incorporación de un *metatag* en un espacio que no es normalmente visible para el usuario, supone utilizar la marca «en relación con productos y servicios en el mercado». Las soluciones jurisprudenciales nacionales son diversas y se debaten (incluso dentro del mismo país) entre concluir a favor de la existencia de infracción por el

simple uso de una marca ajena como *metatag,*[21] o entender que no es propiamente «*uso en el comercio*» y que sólo constituirá infracción cuando se demuestre que se está produciendo confusión en el consumidor (que entienda que la página resultante ofrece productos de la marca deseada –utilizada como *metatag* por la página resultante)[22] o, como máximo, podrá ser considerado un acto de competencia desleal (pero no una infracción de marca).[23] En España todavía no hay jurisprudencia en la materia, siendo viables todas las opciones: infracción de marca, tanto de forma estricta (por el mero uso de la marca ajena como *metatag,* ya que la ley española no exige que la marca sea utilizada «en el comercio» sino en relación con el término más amplio de «tráfico económico» –*vid.* Ley 17/2001, de 7 de diciembre, de Marcas) como por la confusión creada en el consumidor; y acto de competencia desleal por actos de confusión y/o de imitación (arts.6 y 11 Ley 3/1991, de 10 de enero, de Competencia Desleal). Sólo el Tribunal de Justicia de la CE podría pacificar o al menos establecer algunas guías a través de la interpretación de las Directivas 89/104/CEE, de 21 de diciembre, sobre marcas y 97/55/CE, de 6 de octubre, por la que se modifica la Directiva 84/450/CEE de 10 de septiembre, sobre publicidad engañosa.

B. Otra conducta específica, el ***keyword selling,*** está siendo examinada bajo las leyes de competencia desleal y de marcas. A ambos lados del Atlántico, algunos ISP (tales como Excite y Google) venden espacio publicitario en las páginas de resultados de búsquedas (realizadas a través del motor de búsqueda) de marcas específicas; es lo que se denomina *keyword selling*. Cuando el usuario realiza una búsqueda (por ejemplo, un nombre genérico «perfumes» o una marca «Estée Lauder»), en la pantalla aparecen no sólo los enlaces a los resultados de la búsqueda, sino también (en el margen superior o lateral) diversos espacios publicitarios y *banners* de productos de competidores o simplemente de almacenes o negocios que ofrecen tales productos. Es un problema semejante al de la utilización de los *metatags*, pero más «escurridizo» ya que aquí la marca no se utiliza «dentro de» la página del competidor (el competidor no aparece como resultado de la búsqueda), sino anunciado «al margen» de los resultados –de manera que hay menos probabilidades de producir confusión en el consumidor y de entender que se está utilizando la marca ajena «en el comercio». Aun así, los ISP ingresan grandes cantidades (calculadas en función de los clicks realizados) a través de estos espacios,[24] con lo cual, se aprovechan indirectamente del valor comercial de marcas ajenas. Las soluciones jurisprudenciales nacionales varían, una vez más. En **Alemania**, la jurisprudencia se decanta a favor del ISP:[25] el simple funcionamiento del motor de búsqueda no asigna responsabilidad al ISP (ya que no tiene obligación de comprobar si el *keyword* vendido infringe o no una marca), a no ser que el titular de la marca le avise de la existencia de infracción (a través de un anuncio tipo *keyword selling*) y el ISP se niegue a deshabilitarlo. En **Francia**, en cambio, se prefiere la solución opuesta, ya sea como infracción directa de marca por parte del ISP (al fin y al cabo, el ISP participa de forma activa en la selección –o aceptación– de las *keywords*) o como com-

21. *Vid.* por ejemplo, en Francia: *Distrimart*, Cour d'Appel de Paris, 13 Marzo 2002; en Inglaterra: *Road Tech Computer Systems vs. Mandata Ltd.* 2002 ETMR 970 y *Reed Exec. Plc. vs. Reed Business Information Ltd.*, 2002 EWHC 2772; en Alemania: *Antragstellerin vs. Antragsgegnerin*, Tribunal Regional de Munich, 17 HK O 10389/04 (24 Junio 2004); en Dinamarca: *Melitta vs. Coffilter Internationalt*, FS 2433/97 Hillerod fodgeret (17 noviembre 1997); en Bélgica: *Belgacom vs. Intouch Presidential*, Tribunal Comercial de Bruselas (15 diciembre 1999), *BVDA Aeronata Int'l Surveys vs. NV Eurosense Belfotop*, Tribunal de Apelación de Antwerp (9 octubre 2000), *NV Resiplast vs. BVBA Resin*, Tribunal Comercial de Bruselas, (4 febrero 2002).
22. *Vid.*, por ejemplo, en Inglaterra: *Reed Exec. Plc. vs. Reed Business Information Ltd.*, 2004 EWCA 159; en Alemania: OLG Dusseldorf, Beschluss I 20 U 104/03 (17 febrero 2004).
23. Ésta es la postura adoptada en Italia: Genertel vs. Crowe Italia, Tribunale di Roma (18 enero 2001), Technoform Bautec Italia vs. Alfa Solare, Tribunale di Milano (8 febrero 2002), Philips vs. Infostrada, Tribunale di Napoli (28 diciembre 2001 y 15 Mayo 2002), y Cassina vs. Galliani Host Arrendamenti, Tribunale di Monza (16 julio 2002).
24. A modo de ejemplo, Google anunció ingresos por este concepto de 1.256 billones de dólares en el primer cuarto del año 2005.
25. *Vid. Nemetschek vs. Google Deutschland*, 33 O 21461/03 y *Metaspinner Media Gmbh vs. Google Deutschland*, 312 O 887/03; 312 O 324/04.

petencia desleal (por el dinero ingresado «en relación con» la marca ajena).[26] Posiblemente en **España** se llegaría a los mismos resultados que en el país vecino (ya sea como infracción de marca o como acto de competencia desleal, por explotación de la reputación ajena de acuerdo con el art.12 Ley 3/1991 de 10 Enero, de Competencia Desleal), pero por el momento no hay jurisprudencia que nos permita ser más concretos. La falta de uniformidad en el panorama europeo es, pues, lamentable, pero tampoco en los Estados Unidos existe por el momento una respuesta clara en las soluciones jurisprudenciales (ni legislativas).

C. Todavía más impredecible es la responsabilidad por la provisión de servicios de boletines y foros de discusión (***Bulletin Board Services, chats,* etc.**). La Directiva no dice nada al respecto (tampoco lo hace la DMCA), a menos –y en la medida– en que se entienda que tales actos puedan quedar subsumidos bajo las exenciones de *hosting* o de mera transmisión. Existen ya algunos casos resueltos por la jurisprudencia, y aunque la mayoría preceden en el tiempo a la DMCA y la DCE, e incluso a sus leyes nacionales de transposición, nada hace cuestionar la vigencia de sus soluciones. En **Alemania**, AOL-Germany fue declarada responsable por alojar un foro de discusión (*chat*) donde se intercambiaban ficheros mp3 ilícitos (Corte de Apelación de Munich, 8 marzo 2001; 29 U 3282/00) y MSN fue declarado responsable por alojar un foro de discusión (chat) que contenía un foto-collage no autorizado de Steffi Graf (Corte de Apelación de Colonia, 28 Mayo 2002; 15 U 221/01). En **Bélgica,** se concluyó que el operador de un BBS tiene la obligación de asegurar que no se distribuirá material ilegal en el mismo –en tal caso, se trataba de programas de ordenador (*Novell & Min.Pub.Co vs. C.*, Trib. Corr. Hasselt, 16 febrero 1999, y en apelación: Amberes, 9ª Ch., 28 febrero 2002). Y en **Estados Unidos**, MAPHIA fue declarado responsable (sobre la base de la doctrina del *contributory infringement*) por operar un BBS que contenía videojuegos Sega ilegales, y por alentar a sus usuarios al intercambio de copias [*Sega vs. MAPHIA*, 857 F. Supp. 679 (N.D.Cal. 1994), 948 F. Supp. 923 (N.D.Cal.1996)]; a pesar de preceder a la DMCA, el resultado hubiera sido probablemente el mismo, ya que resulta obvio que cuanto menos existía *awareness*, si no conocimiento efectivo, por parte del ISP sobre la ilicitud de las copias disponibles en su BBS.

II. Por lo que respecta a la ausencia de un proceso de aviso y retirada (***notice and take down***), la DCE apuesta por la adopción de «*mecanismos rápidos y fiables que permitan retirar la información ilícita y hacer que sea imposible acceder a ella; convendría que estos mecanismos se elaborasen tomando como base acuerdos voluntarios negociados entre todas las partes implicadas y fomentadas por los Estados miembros*» (cons. 40 DCE). Por el momento, el progreso en este campo es bastante desalentador: los acuerdos voluntarios no son (¿todavía?) realidad y sólo un puñado de leyes nacionales han optado por introducir procesos de detección y retirada, similares al de la DMCA. Así lo han hecho, **Finlandia** y **Hungría** (aunque sólo para las infracciones de propiedad intelectual); **Noruega** consideró inicialmente la introducción de tal proceso pero no llegó a materializarse en la ley finalmente aprobada; mientras que **Francia** y **Bélgica** han optado por la corregulación entre ISPs y gobierno. Una vez más, y teniendo en cuenta la transversalidad de las infracciones que tienen lugar en Internet, no parece que la diversidad de soluciones nacionales sea la mejor manera de afrontar el problema y, como mínimo, permite poner en entredicho la bondad del mensaje de tranquilidad que adopta la Comisión en su Primer informe (*vid. supra*).

III. Finalmente, a diferencia de la sec. 512(h) DMCA, la DCE no obliga a los Estados miembros a disponer de un

26. *Vid.* por ejemplo, *Google vs. Viaticum/Luteciel*, Cour d'Appel de Versailles (marzo 2005); *Louis Vuitton vs. Google*, Paris District Cour (febrero 2005); *Accor vs. Overture*, Tribunal de Grande Instance de Nanterre (enero 2005); *Meridien vs. Google France*, Tribunal de Grande Instance de Nanterre (diciembre 2004).

proceso de ***subpoena*** que obligue a los ISP a identificar a los supuestos infractores. El art.15(2) DCE dispone que «*los Estados miembros* ***podrán*** *establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento*». Merece la pena señalar que se trata tan sólo de una potestad (que no obligación) de los Estados miembros, y que la información se entregará a las autoridades públicas y no directamente al titular de los derechos supuestamente infringidos (tal como establece la sec. 512(h) DMCA). Sólo algunos países han adoptado, como obligación, la identificación de los presuntos infractores por parte de los ISP.[27]

Tampoco la **Directiva 2004/48/CE, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual** avanza demasiado en este sentido.[28] Por un lado, asegura a los titulares de derechos de propiedad intelectual objeto de infracción la posibilidad de obtener de la mayoría de ISP (aquellos que presten a escala comercial servicios utilizados en las actividades infractoras) información para identificar y localizar a los supuestos infractores. Sin embargo, se trata –una vez más– de una potestad (esta vez, a nivel judicial): el Estado miembro tiene la obligación de garantizar que «*las autoridades judiciales competentes* ***puedan*** *ordenar*», con lo cual –en la práctica– la efectividad del «derecho de información» queda únicamente en manos del tribunal que conoce del caso. Además, no olvidemos que este derecho se aplicará «*sin perjuicio de otras disposiciones legales que... (e) rijan la protección de la confidencialidad de las fuentes de información o el tratamiento de los datos personales*», con lo cual el ámbito de decisión del tribunal es doblemente amplio.[29]

La pregunta que sigue es: ¿qué ISP? ¿todos? En el famoso caso norteamericano ***Verizon,***[30] al titular de derechos de propiedad intelectual le fue denegada la *subpoena* prevista en la sec.512 DMCA para obtener de un proveedor de acceso a Internet –*Verizon*, información personal de los usuarios supuestos infractores de sus derechos. Entendió el tribunal que la *subpoena* prevista en la DMCA no es de aplicación a los servicios de mera «provisión de acceso» (ya que no es posible cumplir con el requisito de identificación del material infractor que debe ser eliminado o cuyo acceso debe ser deshabilitado, establecido para la concesión de la *subpoena*).[31] Así pues, queda por ver cómo se resolvería en Europa un caso como el de *Verizon*.

27. En concreto, Austria, Bélgica, Italia y Portugal; Alemania establece una obligación sólo en los procesos penales.

28. *Vid.* http://www.europa.eu.int/eur-lex/pri/es/oj/dat/2004/l_195/l_19520040602es00160025.pdf. El art.8 establece un «derecho de información» a favor del titular de los derechos de propiedad intelectual (y sólo de estos derechos), obligando a los Estados miembros a garantizar que «*en el contexto de los procedimientos relativos a una infracción de un derecho de propiedad intelectual y en respuesta a una petición justificada y proporcionada del demandante, las autoridades judiciales competentes puedan ordenar que faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual el infractor o cualquier persona que ... (c) haya sido hallada prestando a escala comercial servicios utilizados en las actividades infractoras ...*»

29. Por el momento, basta apuntar que se está tramitando en España el Proyecto de Ley de transposición de esta Directiva, presentado en las Cortes el 28 de Octubre de 2005.

30. Vid. RIAA vs. Verizon Internet Services Inc., 2003 U.S.App. Lexis 25735 (19 diciembre 2003). Vid. también L. Guibault, Vous qui téléchargez des oeuvres de l'Internet, pourrait-on savoir qui vous êtes ?, Droit des Technologies de l'Information n.18/2004, p.9-31, en la que la autora vaticina una solución similar bajo el art.15(2) DCE que bajo la lectura Verizon de la sec.512(h) DMCA, en el sentido de que ni los ISP proveedores de acceso ni los de mera transmisión quedan sujetos a la obligación de identificación, sólo los ISP que ofrecen servicios de almacenaje quedarían sujetos a ella (en aquellos Estados miembros que la han incorporado en su legislación).

31. Aunque, añade: «*El Congreso no tenía motivo alguno para prever la aplicación de la sec.512(h) al intercambio de ficheros P2P, ni tampoco diseñó la DMCA con la amplitud necesaria para ir alcanzando las nuevas tecnologías a medida que llegaban. Si el Congreso hubiera sido consciente de la tecnología P2P, o hubiera anticipado su desarrollo, la sec. 512(h) pudiera haber sido redactada de forma más general. Tal como es ahora, y contrariamente a la pretensión de la RIAA, nada en la historia legislativa fundamenta la concesión de una subpoena de la sec.512(h) a un ISP que actúa como transmisor del intercambio de ficheros P2P*». *Vid. RIAA vs. Verizon Internet Services Inc.*, 2003 U.S.App. Lexis 25735 (19 diciembre 2003) #II.C.

4. Los sistemas P2P

Entre los diversos temas relacionados con la responsabilidad de los ISP, merecen especial atención las infracciones de propiedad intelectual que se cometen a través de sistemas *peer-to-peer* que permiten a usuarios de todo el mundo «intercambiar» millones de ficheros (ficheros que, normalmente, contienen obras ajenas protegidas). Todos quienes intervienen en este proceso pueden ser declarados responsables por tales infracciones.

- **Los usuarios**: En principio, la descarga de un fichero puede quedar cubierta por la excepción de copia privada, pero no siempre, ya que las soluciones (el alcance de esta excepción) varían de un país a otro. Así, por ejemplo, en **Alemania**, una reciente modificación del art. 53 de la Ley de Propiedad Intelectual requiere expresamente –para poder ser calificada de «copia privada»– que la copia no haya sido hecha «de una fuente obviamente ilegal», excluyendo así de la excepción de copia privada las copias realizadas mediante sistemas P2P. De forma similar, en **Noruega**, no existe copia privada cuando se ha realizado con la intención de ponerla posteriormente a disposición del público. En cambio, en **Canadá** existe desde 1997 una remuneración por copia privada –que incluye también las copias digitales– y que no requiere que la copia haya sido realizada de una fuente legal, de manera que cubre perfectamente las copias obtenidas mediante sistemas P2P –*vid.* BMG *vs.* John Doe, Corte Federal de Canadá, 2004 FC 488 (31 marzo 2004).[32] Sin embargo, en apelación, –*vid.* BMG Canada Inc. *vs.* John Doe, Corte Federal de Apelación de Canadá, 2005 FCA 193 (19 mayo 2005),[33] se concluyó que el tribunal había cometido un error al decidir que el intercambio de ficheros no constituía infracción de la propiedad intelectual. Y en **Estados Unidos**, la copia reiterada con fines de «intercambio» con otros usuarios no podría ser calificada de *fair use* bajo la sec.107 USCA. En cualquier caso, aparte de que la descarga quede o no amparada por la excepción de copia privada, no hay duda alguna de que se comete una infracción cuando los usuarios ponen los ficheros guardados en su PC a disposición del público (del público que tiene el programa P2P instalado en su PC, claro).

- El **productor del programa informático P2P** también puede ser considerado responsable por los actos ilegales cometidos por los usuarios del mismo. Aunque la tecnología es «normalmente» neutral y las exenciones de responsabilidad previstas para los ISP no serían de aplicación para proteger al productor del software, éste quedará sujeto a las reglas generales de responsabilidad por hecho ajeno, que –como apuntábamos antes– varían en cada país. En **Holanda** se eximió a KaZaA –*vid.* Hoge Raad, 19 diciembre 2003: aunque el informe del abogado general eximía de responsabilidad a KaZaA (ya que el programa también era utilizado para fines no ilícitos), la Corte Suprema decidió el caso en base a un aspecto técnico, y no entró a examinar la cuestión concreta de si KaZaA era responsable por las infracciones de PI de sus usuarios.

En **Estados Unidos**, mientras que *Napster* y *Aimster* fueron declarados responsables (por *vicarious liability* y *contributory infringement*, respectivamente),[34] *Grokster* y *KaZaA* no lo fueron inicialmente, ya que tanto en instancia como en apelación[35] se entendió que ellos no ofrecían el «lugar y instalación» para la comisión de la

32. *Vid.* http://www.canlii.org/ca/cas/fct/2004/2004fc488.html
33. *Vid.* http://decisions.fca-caf.gc.ca/fca/2005/2005fca193.shtml
34. *Vid. A&M Records vs. Napster*, 239 F.3d 1004 (9th Cir 2001) y In re Aimster Copyright Litigation, 2003 U.S.App.Lexis 13229 (7th Cir. 2003).
35. *Vid. Metro-Goldwyn-Mayer Studios Inc. vs. Grokster Ltd.*, 259 F.Supp. 2d 1029 (C.D. Cal. 2003), *affirmed*, 380 F.3d 1154 (9th Cir. 2004)

infracción y que no tenían «derecho o poder de supervisar» las actividades infractoras de sus usuarios. Pero como decíamos, ello fue inicialmente. Sin embargo, el pasado verano, la Supreme Court[36] norteamericana concluyó que Grokster era responsable por las infracciones cometidas por los usuarios de su sistema de software P2P, al afirmar que quien distribuye un producto y promociona su uso para cometer infracciones de la propiedad intelectual es responsable de las infracciones resultantes que cometan los usuarios del mismo. En lugar de revisar –como todo el mundo esperaba– la doctrina establecida en Sony en 1984, y clarificar lo que se entiende por «*capable of commercially significant noninfringing uses*»,[37] la Supreme Court optó por concluir que el Noveno Circuito erró al interpretar que Sony fuera aplicable en este caso. En resumen, Sony continua vigente y simplemente se ha añadido un nuevo test para la responsabilidad por hecho ajeno: el denominado «*inducement*».

- Finalmente, **el ISP** que aloja la página web desde la cual se puede descargar el programa P2P o que proporciona los servicios de acceso y de mera transmisión que permiten el funcionamiento del programa P2P, también podría ser considerado responsable por las infracciones de PI. Aquí son de aplicación las exenciones de responsabilidad previstas a favor de los ISP (de «mera transmisión» o de *hosting*). Por ejemplo, en **Noruega,** se exoneró de responsabilidad a un ISP por ofrecer enlaces a páginas web de software P2P, tales como *KaZaA* y *Morpheus*, pero el tribunal no examinó la cuestión de si el ISP contribuía a la comisión de la infracción de los usuarios al ofrecer enlaces a tales páginas –*vid.* Phonofile AS *vs.* ABC Startsiden, Tribunal de Oslo, 27 de octubre de 2003.

Además de las acciones contra los productores de software P2P y los ISP, la campaña de demandas contra usuarios individuales iniciadas en los últimos años por la industria de contenidos ha sido bastante efectiva en la reducción del número de usuarios de P2P (de 60 millones en el 2002 a 20 millones en el 2004 –o al menos, menos gente se atreve a declararse usuario de tales sistemas), y en especial en la «educación» de la sociedad sobre lo que constituye infracción de la propiedad intelectual. Sin embargo, queda por ver si –y en qué términos– el «intercambio» de ficheros mediante sistemas P2P sobrevive –*vid.* la alternativa propuesta por la Electronic Frontier Foundation en favor de una licencia colectiva remunerada y voluntaria.[38]

En cualquier caso, Grokster ha cerrado por el momento sus puertas, a la espera de poder ofrecer el servicio debidamente licenciado.[39]

5. Jurisdicción y ley aplicable

Pero quizás la piedra angular de toda infracción de la PI en Internet, y la subsiguiente responsabilidad del ISP reside en sede de Derecho Internacional Privado, en temas de **jurisdicción y ley aplicable**. A pesar de declarar expresamente que «*no establece normas adicionales de derecho internacional privado ni afecta a la jurisdicción de los tribunales de justicia*» (*vid.* art.1(4) DCE), la DCE establece un sistema de **«control en origen»** (*vid.* art.3 DCE) que puede acabar teniendo una influencia directa a la hora de establecer qué ley rige la infracción. El «control en origen» significa –entre otras cosas– que la ley del país de establecimiento del ISP decidirá si (y en qué medida) el ISP queda o no exento de responsabilidad por una infracción concreta acaecida en Internet. No sería extraño que el tribunal utilizara esta misma ley, del país de establecimiento del ISP, no sólo para examinar la exis-

36. *Vid. Metro-Goldwyn-Mayer Studios Inc. vs. Grokster Ltd., certiorari granted* 380 F.3d 1154 (2005), *vacated and remanded*, 545 U.S. --- (27 junio 2005).
37. *Vid. Sony vs. Universal*, 464 U.S. 417 (1984)
38. *Vid.* http://www.eff.org/share/compensation.php
39. *Vid.* http://www.grokster.com

tencia o no de responsabilidad del ISP, sino también para examinar la existencia o no de infracción (la cual, en principio, debería ser resuelta de acuerdo con la *lex loci delicti comissi* –cualquiera que sea esta ley en un contexto de redes digitales).

Esta posible prevalencia de la ley del país de establecimiento del ISP puede ser especialmente importante cuando se tiene en consideración los criterios de jurisdicción competente. De acuerdo con el Reglamento (CE) 44/2001[40] (conocido como Reglamento de Bruselas por incorporar el *Convenio de Bruselas de 1968 relativo a la competencia judicial y la ejecución de resoluciones judiciales en materia civil y mercantil*), son competentes tanto los tribunales del país donde se produce el daño (*vid.* art.5.3), como los tribunales del país de residencia del demandado (*vid.* art.2.1). Entonces, si la demanda se plantea ante los tribunales del país de establecimiento del ISP (especialmente, cuando la demanda se ejerza contra ambos, infractor e ISP), la jurisdicción competente y la ley aplicable podrán coincidir fácilmente. En cambio, si la demanda se plantea en un país distinto del de establecimiento del ISP, pero que tenga jurisdicción (ya sea en el país de residencia del infractor demandado, o en cualquier país de acceso o descarga del contenido infractor, o incluso en el país de residencia del titular del derecho infringido –al fin y al cabo, es donde él reside donde se produce el daño–), jurisdicción y ley aplicable no coincidirán tan fácilmente. Y fijémonos que, a diferencia de los Estados Unidos y demás países del ámbito anglosajón (denominados del *Common Law*), los tribunales nacionales europeos –bajo el Reglamento de Bruselas– no pueden recurrir al *forum non conveniens* para rechazar su competencia en favor de otro tribunal mejor situado para enjuiciar el caso. El escenario se complica todavía más si se toma en consideración la doctrina del Tribunal de Justicia de las Comunidades Europeas en el caso ***Shevill***,[41] en el sentido de que no todas las jurisdicciones competentes pueden otorgar indemnización por los daños y perjuicios causados a nivel mundial: sólo la jurisdicción del país donde se origina el acto infractor puede establecer indemnización a nivel global, las restantes jurisdicciones competentes sólo podrán indemnizar por los daños producidos en su territorios respectivos.

Si sumamos una única jurisdicción con competencia global (la del país donde se origina la infracción) y el control en origen para establecer la exención de responsabilidad del ISP (ley del país de establecimiento del ISP), la ley aplicable al fondo del asunto (*lex loci delicti*) queda muy debilitada ante la *lex fori*, y no sería de extrañar que el foro acabe interpretando que el *locus delicti* es justamente el país de establecimiento del ISP (que, por ejemplo, almacena el contenido infractor), de manera que se pueda aplicar una única ley, la nacional (*lex fori*) para juzgar toda la infracción (y, si es el caso, la exención de responsabilidad del ISP) a nivel mundial. De hecho, ya existen sentencias –de países del Common Law– que llegan a la misma conclusión a favor de una única jurisdicción y ley aplicable: la del titular del derecho objeto de infracción.[42] Por supuesto, en un ámbito globalizado como Internet, estas soluciones ponen cuanto menos en entredicho los principios generales de previsibilidad y conexión (y, en fin, de conocimiento del derecho) que tradicionalmente han inspirado los ordenamientos jurídicos nacionales y las normas de derecho internacional privado, ya que convierten a todo usuario en posible infractor de alguna ley, de algún país del mundo. Basta una breve referencia al caso de Andrew Meldrum –periodista del diario inglés *Guardian*– quien fue acusado en Zimbabwe por falsedad y difamación, a raíz de la publicación de su artículo en la página web del diario *Guardian* en el que criticaba al gobierno de aquel país. De acuerdo con el fiscal, los tribunales y leyes de Zimbabwe son competentes/aplicables también a los editores y periodistas extranjeros cuando sus ediciones se pueden descargar

40. REGLAMENTO (CE) 44/2001, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. http://europa.eu.int/eur-lex/pri/es/oj/dat/2001/l_012/l_01220010116es00010023.pdf
41. Sentencia de 7 marzo 1995, *Fiona Shevill et al vs. Presse Alliance S. A.*, 1995 TJCE 415 (asunto C-68/93).

desde Zimbabwe. No me parece que las leyes nacionales, ni siquiera en materia de propiedad intelectual, sean suficientemente homogéneas como para hacer posible que la aplicación de una única ley para enjuiciar la infracción cometida en Internet (a nivel internacional) sea considerada justa.

Cita recomendada

XALABARDER, Raquel (2006). «La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 2. UOC. [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/2/dt/esp/xalabarder.pdf>
ISSN 1699-8154

SOME RIGHTS RESERVED

Esta obra está bajo la licencia Reconocimiento-NoComercial-SinObraDerivada 2.5 de Creative Commons. Así pues, se permite la copia, distribución y comunicación pública siempre y cuando se cite el autor de esta obra y la fuente (Revista IDP) y el uso concreto no tenga finalidad comercial. No se pueden hacer usos comerciales ni obras derivadas. La licencia completa se puede consultar en:
<http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.es>

Raquel Xalabarder Plantada

rxalabarder@uoc.edu

Doctora en Derecho por la Universidad de Barcelona (1997), con la tesis *La protecció internacional de l'obra audiovisual. Qüestions relacionades amb l'autoria*. Especial referència als sistemes jurídics d'Espanya i els Estats Units d'Amèrica. Master of Laws en la Columbia University Law School (1992-1993) y licenciada en Derecho por la Universidad de Barcelona (1983-1988). Actualmente es profesora de los Estudios de Derecho y Ciencia Política de la UOC. Durante el curso 2000-2001 fue *Visiting Scholar* en la Columbia University Law School (Nueva York) con un proyecto de investigación sobre «Propiedad intelectual y enseñanza a distancia», subvencionado por la Comisión Fulbright y la Generalitat de Cataluña.

42. *Vid. Dow Jones vs. Gutnick*: la revista electrónica *Barron's* (editada en Estados Unidos por Dow Jones) publicó un artículo en el que se difamaba a Gutnick, residente en Victoria, Australia. Éste demandó al editor norteamericano ante los tribunales de su residencia en Australia. Dow Jones alegó que puesto que la revista se publica en New Jersey, sede del servidor que almacena la revista digital, son los tribunales de este Estado los más apropiados para conocer del caso. El tribunal de Victoria rechazó tales alegaciones (sentencia de 28 agosto 2001), concluyendo que puesto que la revista era accesible (por subscripción) desde Victoria, la publicación (*download*) tenía lugar en Victoria; y añadió que, incluso en el caso de que el razonamiento de Dow Jones fuera correcto (y el lugar de publicación fuera el de la sede del servidor, *upload*, en New Jersey), siempre se ha entendido que en casos de difamación «tradicional», ésta tiene lugar en cualquiera de los países donde se distribuye el material infractor, y no existe motivo alguno para que esta misma regla de jurisdicción no sea también aplicable a los casos de difamación por Internet. El tribunal australiano concluyó «*Gutnick vive en Victoria, tiene aquí su negocio, ... y es aquí donde quiere reivindicar su reputación, puesto que es aquí donde tiene una reputación*». Dow Jones apeló, pero la High Court of Australia confirmó (sentencia de 10 diciembre 2002) la competencia de los tribunales australianos (y la aplicación de la ley australiana): http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html. Finalmente, en el 2004, viendo que la aplicación de la ley y jurisdicción australiana le impedía ganar el caso, Dow Jones accedió a indemnizar a Gutnick.