RESPONSABILIDAD DE LOS INTERMEDIARIOS DE INTERNET EN EL DERECHO DE LA UE

Liability of internet intermediaries under EU law

ABRAHAM BARRERO ORTEGA
Universidad de Sevilla
abraham@us.es

Cómo citar/Citation
Barrero Ortega, A. (2021).
Responsabilidad de los intermediarios de internet en el derecho de la UE.
Revista Española de Derecho Constitucional, 123, 107-132.
doi: https://doi.org/10.18042/cepc/redc.123.04

Resumen

El presente trabajo analiza la responsabilidad jurídica de los intermediarios de internet (ISP) en el derecho de la Unión Europea. Responsabilidad por los contenidos ilícitos o infractores de sus usuarios. Se trata de discernir si los intermediarios deben responder por posibles ilícitos que los usuarios de sus servicios pueden causar a terceros con motivo del alojamiento y difusión de contenidos a través de la red. El régimen jurídico general de la responsabilidad de los intermediarios viene diseñado en la Directiva 2000/31/CE, sobre el comercio electrónico. Más recientemente, otras normas comunitarias han venido a perfilar o completar ese régimen de la responsabilidad en aspectos particulares o, mejor dicho, respecto a determinados contenidos.

Palabras clave

Prestadores de servicio; intermediarios; internet; responsabilidad; Tribunal de Justicia de la Unión Europea.

Abstract

This paper analyses the legal liability of Internet intermediaries under European Union law. Liability of intermediaries for the illegal content of their users. It is necessary to determine whether intermediaries should be held responsible for possible unlawful acts that the users of their services may cause to third parties when hosting and disseminating content through the network. The general legal regime for the liability of intermediaries is laid down in Directive 2000/31/EC, on electronic commerce. More recently, other Community rules have supplemented this liability regime in particular areas or, rather, for certain content.

Keywords

Service providers; intermediaries; internet; liability; Court of Justice of the European Union.

SUMARIO

I. DE QUÉ HABLAMOS CUANDO HABLAMOS DE RESPONSABILIDAD JURÍDICA DE LOS INTERMEDIARIOS DE INTERNET

La responsabilidad de los intermediarios en internet (en adelante, ISP[1]) por los contenidos de los usuarios de su servicio viene suscitando en las últimas décadas un intenso debate socioeconómico que, obviamente, tiene implicaciones

[1] Los ISP, que comenzaron a surgir a finales de los ochenta y principios de los noventa, son las empresas que proporcionan a los usuarios el acceso a internet y servicios relacionados. Más específicamente, pueden incluirse, entre otras, en las siguientes categorías:

a) Los operadores de redes: proveen la infraestructura para el acceso a la transmisión de internet entre un punto y otro. Por ejemplo, los operadores que trabajan con los *routers*, *switches*, cables, etc.
b) Los proveedores de acceso a internet: pueden ir desde aquellos que simplemente proveen acceso a la navegación y un correo electrónico hasta aquellos que ofrecen a los usuarios infraestructuras para el manejo de sus páginas web. Así, compañías como AT&T, BT, Claro, Une, T-Mobile, Orange, etc.
c) Los proveedores de servicios de alojamiento de la información o *hosting*: permiten que los usuarios almacenen o guarden la información que deseen en sus servidores. En esta categoría, podemos encontrar los servicios en la nube, como YouTube, DropBox, SkyDrive, etc. Los usuarios pueden almacenar diferentes tipos de información, como material audiovisual, textos, fotografías, archivos musicales, etc.
d) Los operadores de salas de chat, grupos de noticias, blogs o *bulletin boards system*, BBS: fueron muy populares en el comienzo de internet, pues utilizaban un sistema de difusión mediante el intercambio de mensajes de texto.

jurídicas (Riordan, 2016: 3-13). A día de hoy es un debate abierto, debido a la aparición de nuevos tipos de ISP que no encajan en los parámetros de la legislación fraguada a finales del siglo xx.

El debate gira en torno a la responsabilidad de los intermediarios por los contenidos ilícitos de sus usuarios, discutiéndose si es preciso sancionar en todo caso su responsabilidad, si, por el contrario, debe establecerse un régimen de exención de responsabilidad o si conviene definir un régimen ecléctico que combine el interés de los perjudicados o víctimas en obtener reparación de los daños padecidos con el libre funcionamiento de internet. El debate ofrece también la oportunidad de exigir (o no) a estos intermediarios la colaboración con los perjudicados y con las autoridades en la identificación de los usuarios infractores y también en la ejecución de las resoluciones judiciales o administrativas contra esos usuarios.

El debate es complejo por cuanto confluyen diferentes derechos, bienes y valores de relevancia constitucional. De un lado, está el interés de los perjudicados en obtener del legislador adecuada protección de sus derechos e intereses; especialmente el derecho del honor, a la intimidad y a la propia imagen, así como los derechos de propiedad industrial (marcas, patentes, diseños industriales, etc.) y propiedad intelectual (derechos de autor y derechos conexos). De otro lado, están las libertades de expresión e información en internet y, más en general, las libertades comunicativas a través de la tecnología informática. Tampoco cabe ignorar los incentivos a la innovación tecnológica y el interés general en el correcto funcionamiento de internet. Establecer un régimen severo de responsabilidad podría acarrear un desincentivo a la inversión en nuevas aplicaciones que mejoren el funcionamiento de la red, que, a corto o medio plazo, podría bloquear seriamente la arquitectura y el funcionamiento de internet en detrimento de los intereses de millones de personas y empresas (Frosio, 2017).

Precisamente, uno de los objetivos de la Unión Europea (en adelante, UE) es la construcción de un mercado único en el que los agentes económicos operen bajo unas mismas reglas de juego, sin obstáculos transfronterizos, restricciones

e) Los proveedores de acceso logístico o motores de búsqueda: proveen a los usuarios herramientas en la red para facilitar la búsqueda de las diferentes páginas de internet, entre los cuales están Google, Yahoo!, etc.

f) Los proveedores de servicios de redes sociales: permiten a los usuarios la interacción con otros usuarios para intercambiar distintos contenidos que se alojan en las plataformas del prestador. Las redes sociales se convierten en un espacio virtual retroalimentado en el que los usuarios consumen, pero también aportan información. Así, Facebook, Twitter, LinkedIn, etc.

al comercio o burocracia enervante. A tal fin responde la Directiva 2000/31/CE, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. La comúnmente denominada Directiva sobre el comercio electrónico.

No es dable exigir que los ISP tengan conocimiento de todas las actividades que los usuarios realizan a través de sus redes, servicios o plataformas. Lo que se debate es qué grado de responsabilidad podría caberles en caso de que, de algún modo, tuvieran conocimiento de la ilicitud o contribuyeran a magnificar el daño. La responsabilidad de los intermediarios queda circunscrita, pues, a los contenidos ilícitos que ofrecen o facilitan; se habla así de responsabilidad *frente a contenidos*. No se trata solo de que los ISP deban responder por incumplimientos contractuales o por los daños y perjuicios infligidos a terceros con motivo de la prestación del servicio, sino también de decidir si deben responder por posibles infracciones que los usuarios de sus servicios pueden causar a terceros con motivo del alojamiento y difusión de contenidos a través de la red (Riordan, 2016: 3-13).

¿Respecto a qué contenidos cabría apreciar esa responsabilidad? Los ejemplos más comunes son las infracciones de la propiedad industrial[2], de la propiedad intelectual o derechos de autor[3], la vulneración de derechos fundamentales como el derecho al honor, a la intimidad, a la propia imagen[4], o a la protección de datos[5]. Asimismo, la violación de otros bienes y valores de relevancia constitucional como la dignidad de grupos de individuos (*hate speech*)[6], la protección de la juventud y de la infancia (pornografía infantil)[7] o —cuestión vidriosa— la dimensión institucional de la libertad de información (desinformación o *fake news*) (Pauner Chulvi, 2018). Las conductas delictivas vinculadas a las tecnologías o ciberdelincuencia plantean igualmente retos novedosos frente a los cuales urge un posicionamiento legal[8].

---

2 STJUE de 12 de julio de 2011, *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd*, C-324/09.

3 STJUE de 27 de marzo de 2014, *UPC Telekabel*, C-314/12.

4 STJUE de 3 de octubre de 2019, *Eva Glawischnig-Piesczek c. Facebook Ireland*, C-18/18.

5 STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*, C-131/12.

6 STEDH, Gran Sala, de 16 de junio de 2015, *Delfi AS c. Estonia*.

7 Recomendación (UE) 2018/334 de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea.

8 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la

Las posibles infracciones pueden ser constitutivas de delitos o, en atención a su menor gravedad, hechos o actos contrarios a las normas que originan la responsabilidad civil extracontractual. La responsabilidad administrativa es la que deriva de una infracción o contravención tipificada en la ley y de la que se debe responder ante una autoridad administrativa que, generalmente, ejerce funciones de control, vigilancia o inspección.

Los ordenamientos jurídicos parten de un principio general de no responsabilidad o inmunidad de los ISP, siempre que se den una serie de condiciones prestablecidas (los «puertos seguros») para cada tipo de servicio de intermediación; condiciones orientadas a discernir adecuadamente los intereses en juego en cada actividad de intermediación, pues no puede medirse de igual forma la mera transmisión de datos por internet que proporcionar espacio de alojamiento en servidores para poner esa información a disposición del público desde los servidores del intermediario, almacenar temporalmente información en memoria caché u ofrecer servicios automáticos de búsqueda y directorios de enlaces a informaciones (Arroyo Amayuelas, 2020).

En caso de que no concurran las condiciones que justifican *a priori* la exención de responsabilidad, los ISP pueden ser responsables de los actos o contenidos infractores de los usuarios. Pero no puede decirse que esa responsabilidad se produzca en todo caso, objetiva o automáticamente. Además, esa posible responsabilidad no necesariamente ha de ser una responsabilidad *stricto sensu*, es decir, una responsabilidad (civil, administrativa o penal) que recaiga directamente sobre el patrimonio del intermediario, sino que dicha responsabilidad puede traducirse, según los casos, en la obligación de advertir o de cesar en la prestación del servicio al usuario. El ISP puede verse obligado a resarcir él mismo o a colaborar para neutralizar el daño o agravio (Urban, Karaganis y Schofield, 2016).

Basta una mirada rápida al derecho comparado para constatar que existen diferentes modelos y pautas de regulación de la responsabilidad de los prestadores de servicios en internet, desde ordenamientos que adoptan una legislación general, horizontal o inespecífica, aplicable a cualesquiera actividades o contenidos, hasta otros que optan por una regulación vertical o específica, para cada clase de actividades o contenidos (datos personales, propiedad industrial, derechos de autor, etc.) (Riordan, 2016: 100 y ss.).

En cuanto a las pautas de atribución de responsabilidad, cabría distinguir entre regímenes jurídicos que contemplan la exención completa y regímenes

certificación de la ciberseguridad de las tecnologías de la información y la comunicación, y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad).

jurídicos que se decantan por la exención parcial. Las soluciones jurídicas van desde la inmunidad total o absoluta a la inmunidad condicionada. El prestador del servicio o no es responsable o lo es solo bajo determinadas circunstancias (Garrote Fernández-Díez, 2014). Como quiera que sea, lo más habitual suele ser que una misma legislación, horizontal o vertical, incluya criterios mixtos de imputación de responsabilidad, con mezcla de supuestos de inmunidad absoluta y otros de inmunidad condicionada.

Obviamente, el alcance de la inmunidad depende de la cualidad de cada tipo de servicio de intermediación. Y es que no es lo mismo hacer circular que alojar o hacer accesible en la red un contenido editado y generado por un usuario. No es lo mismo prestar un servicio de acceso a internet que prestar un servicio de alojamiento, de envío de correo electrónico o de búsqueda de información. Dependiendo de la naturaleza de cada servicio prestado, se establecen una serie de requisitos para la exención de la responsabilidad del ISP. Si esos requisitos no se cumplen, el ISP será responsable (Kleinschmidt, 2010).

Más exactamente, en el primer modelo (inmunidad total), el ISP no es responsable de los contenidos subidos por terceros, puesto que es considerado simple mediador. La consideración del ISP como mero prestador de un servicio de intermediación refuerza su posición como no responsable de la actividad que los usuarios realizan entre sí dentro de la red o de la plataforma. El ISP es un proveedor neutral que media entre dos personas, el usuario que genera el contenido y el usuario que accede a él. Es decir, un intercesor pasivo o inactivo, que deja que las cosas ocurran sin intervenir (Garrote Fernández-Díez, 2014).

En el segundo modelo (inmunidad condicionada), el intermediario se encuentra eximido de responsabilidad siempre y cuando cumpla con ciertas condiciones, tales como retirar o bloquear el contenido ilegal una vez que sea notificado de ello («notificación y retirada») o simplemente notificar al usuario infractor («notificación y notificación»). Por notificación se entiende la resolución dictada por un órgano competente (judicial y, excepcionalmente, administrativo) que declare la ilicitud del contenido y ordene su retirada o que se imposibilite el acceso a este (Garrote Fernández-Díez, 2014).

En algunos países, el procedimiento de «notificación y retirada» puede ser incoado por el titular del derecho o bien jurídico infringido, de modo que es el perjudicado el que identifica el contenido ilícito y lo comunica directamente al ISP. El perjudicado no puede limitarse a indicar al ISP la existencia de contenido ilícito en general, sino que debe identificarlo de modo específico y preciso (Urban, Karaganis, y Schofield, 2016). Es una vía, por así decir, privada de resolución del conflicto, al margen de que ulteriormente el conflicto, si no hay acuerdo, pueda llegar a la autoridad competente.

En ausencia de resolución que ponga en conocimiento del intermediario notificado la ilicitud de los contenidos o actividades, la responsabilidad puede derivar del requisito del «conocimiento real u objetivo» de esa ilicitud por parte del ISP. El ISP no ha sido notificado, pero lo cierto es que conocía otros hechos o tenía otra información acreditativa del contenido infractor (Garrote Fernández-Díez, 2014).

En este segundo modelo resulta crucial diferenciar aquellas plataformas puramente intermediarias y neutrales de aquellas otras que ejercen control sobre el servicio subyacente. Así, si su actividad va más allá de la pura puesta a disposición de información o de la puesta en contacto de usuarios, y si con ello ordenan o controlan de alguna forma la actividad de los participantes, deben ser tratadas como algo distinto que los intermediarios puros. Esto implicará que las exclusiones de responsabilidad que la legislación establece para la labor de intermediación pura no podrían aplicarse. La clave está, pues, en trazar la línea de cuánto control es relevante a efectos de decidir si una plataforma pierde o no la inmunidad prevista para los simples mediadores (Riordan, 2016: 32 y ss.).

En aquellos ordenamientos jurídicos donde no existe legislación alguna (imprevisión legislativa), se ha recurrido a la doctrina de la responsabilidad civil (excepcionalmente penal) para resolver casos particulares, lo que obliga al juez a examinar y ponderar cuidadosamente en cada controversia los derechos, bienes y valores en conflicto y, como se acaba de indicar, la posición y actitud del intermediario. El silencio del legislador ha sido suplido por un «activismo judicial» a través de la aplicación de la obligación genérica de reparar el daño causado por la plataforma a otro (Garrote Fernández-Díez, 2014).

Sea como fuere, ningún ordenamiento ha adoptado un régimen de responsabilidad objetiva (es decir, aquel que considera responsable al intermediario con independencia de toda culpa por los contenidos expresados por clientes o usuarios a través de sus servicios). En la mayoría de los países se ha recurrido a la responsabilidad subjetiva, lo que implica —reitero— analizar *ad casum* el comportamiento del ISP para determinar si conocía la ilicitud y ha tomado las precauciones necesarias para neutralizar el daño. Se examina, pues, si el intermediario actúa con negligencia o con culpabilidad y si, antes de que se produzca el daño, ya tenía algún conocimiento de la ilicitud de los datos o contenidos (Synodinou, 2015). Los ISP no están obligados a responder por cualquier daño por el solo hecho de desarrollar una actividad riesgosa dentro de la sociedad de información, pero sí cuando obren descuidada, negligente o imprudentemente, es decir, cuando no retiren o bloqueen contenidos habiendo sido notificados de la ilicitud de estos o cuando, aun no habiendo sido notificados, tuvieran «conocimiento real u objetivo» de la ilicitud.

La responsabilidad de los ISP, en definitiva, no será apreciada por el mero hecho de que un proveedor de contenidos o cualquier particular realice conductas que son punibles utilizando los servicios y recursos técnicos provistos por el intermediario (lo que nos llevaría a una responsabilidad objetiva, por el mero riesgo que supone su actividad), sino por sus propias actuaciones en relación con tales conductas y, en concreto, la diligencia mostrada en evitarlas o impedirlas una vez descubiertas.

En estas coordenadas, y puestos a matizar con mayor precisión las consideraciones generales que anteceden, el presente trabajo se centra a renglón seguido en el régimen de responsabilidad de los ISP en el derecho vigente de la UE (II), sin perjuicio de oportunas consideraciones *de lege ferenda* (III). Como es sabido, la Comisaría del Mercado Interior tiene abierta, desde el pasado junio, consulta pública de cara a la revisión de la Directiva sobre comercio electrónico.

II. LA REGULACIÓN EN EL MARCO DE LA UE

La regulación de la responsabilidad de los ISP en el marco de la UE podría definirse como una regulación compleja, integrada por diversos elementos normativos, debido a la modalidad jurídica empleada hasta la fecha por el legislador europeo. Es sabido, en efecto, que, a través de la directiva comunitaria, los países que conforman la UE reciben indicaciones y guías sobre una serie de aspectos normativos a los cuales deben adecuarse. No obstante, teniendo en cuenta la pluralidad y diversidad de estructuras jurídicas de cada uno de ellos, los medios concretos a través de los cuales debe alcanzarse el objetivo quedan en manos de cada Estado (Bellido Barrionuevo, 2003).

En tal sentido, el régimen jurídico de la responsabilidad de los ISP en internet diseñado en la Directiva 2000/31/CE, sobre el comercio electrónico, y completado en las medidas nacionales de transposición, está marcado por una gran flexibilidad.

Téngase en cuenta, además, que otras normas comunitarias han venido a perfilar o completar el régimen de la responsabilidad previsto en la Directiva sobre el comercio electrónico en aspectos particulares o, si se quiere, respecto a determinados contenidos. Así, recientemente, la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital, y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (Directiva sobre los derechos autor y derechos afines). *Lex specialis derogat generali*.

A grandes rasgos, la Directiva 2000/31/CE aborda el régimen de responsabilidad de los ISP desde una perspectiva horizontal o inespecífica (arts. 12 a 15). Regula, en efecto, una responsabilidad general de los prestadores de servicios de la sociedad de la información, incluidos los servicios de intermediación, de carácter civil administrativo o penal, y frente a cualquier contenido ilícito o infractor. No obstante, la directiva establece un régimen diferenciado de responsabilidad para estos que varía en función de las actividades que cada uno desempeña dentro del tráfico electrónico de internet (Salvador Coderch y Ruiz García, 2001).

El legislador europeo no sienta ninguna presunción de conocimiento de la ilicitud de los contenidos, sino que, al igual que ocurre en EE. UU., se parte de un principio general de exención de responsabilidad o inmunidad, «puerto seguro» o *safe harbor* (Garrote Fernández-Díez, 2014). Ahora bien, la inmunidad está sujeta a una serie de condicionamientos que, de no darse, podrían determinar la responsabilidad del prestador.

1. PRESTADORES DE SERVICIOS O INTERMEDIARIOS

La Directiva sobre el comercio electrónico define los servicios de la sociedad de la información como aquellos que se prestan a distancia, por vía electrónica, a petición individual del destinatario, y, normalmente, a cambio de una remuneración[9]. Estos servicios comprenden los prestados a través de internet siempre que representen una actividad económica para el prestador.

Un tipo específico de servicios de la sociedad de la información son los de carácter intermediario o servicios de intermediación (ISP). La directiva no proporciona una definición general, pero prevé tres categorías de servicios intermedios: a) la mera transmisión (*mere conduit*): servicio consistente en transmitir información a través de una red de comunicaciones o en facilitar el acceso a esta; b) la memoria tampón (*caching*): servicio de almacenamiento de datos de manera temporal que prestan algunos operadores de redes para asegurar la transmisión, y c) el alojamiento de datos (*hosting*): servicio que provee a los usuarios un sistema para poder almacenar información.

[9] La nota de que el servicio se preste normalmente a cambio de una remuneración no significa que necesariamente deba existir un pago por parte del receptor del servicio. Lo decisivo es que el servicio debe constituir una actividad de naturaleza económica para el prestador. Por tanto, son también servicios de la sociedad de la información los que se prestan gratuitamente y obtienen sus ingresos por otras vías, especialmente a través de la publicidad.

Los ISP facilitan las transacciones entre usuarios de internet. Brindan acceso, hosteo, transmiten e indexan contenidos, productos y servicios originados por los usuarios. Estos intermediarios pueden encontrarse en la capa física de internet (por ejemplo, proveedores de servicios de conectividad) o en la capa de aplicaciones (tales como las plataformas que alojan contenidos, brindan servicios de almacenamiento, redes sociales, los intermediarios de venta de productos, etc.)[10].

2. EXENCIÓN DE RESPONSABILIDAD O «PUERTO SEGURO»

La Directiva sobre el comercio electrónico exime a los ISP de responsabilidad si a) desempeñan un papel *neutro* o *pasivo* en relación con los contenidos transmitidos y/o albergados y si b) actúan «con prontitud» para retirar o impedir el acceso a los contenidos tan pronto como tengan «conocimiento efectivo» de la infracción o del carácter ilícito del contenido (arts. 12, 13 y 14). Rol neutro y diligencia ante el conocimiento efectivo.

Las exenciones de responsabilidad solo se aplican a aquellos supuestos en que el ISP se limita al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros es transmitida (*mere conduit*) o almacenada temporalmente (*caching*), con el fin de hacer que la transmisión sea más eficiente. Esa actividad es de naturaleza meramente técnica, automática y pasiva, lo que implica que el prestador de servicio no tiene control sobre los contenidos. «El servicio de facilitación del acceso no debe ir más allá del procedimiento técnico, automático y pasivo que garantice la ejecución de la transmisión de datos, sin implicaciones adicionales» (STJUE de 15 de septiembre de 2016, *Tobias Mc Fadden*, C-484/14).

El intermediario no tiene participación alguna en el contenido de los datos transmitidos. Esto requiere, obviamente, que no modifique los datos que transmite. No hay modificación cuando el prestador del servicio realice manipulaciones de carácter técnico durante la transmisión, ya que no alteran la integridad de los datos. Un prestador de servicios que colabore deliberadamente con uno de los destinatarios de su servicio a fin de cometer ilícitos

[10] A diferencia del ordenamiento estadounidense, la Directiva sobre el comercio electrónico no alude a los prestadores de servicios que faciliten instrumentos de búsqueda o enlaces (*links*) a contenidos o actividades de terceros. Ahora bien, la directiva no impide a los Estados miembros que, al transponerla a sus ordenamientos internos, regulen de forma expresa la responsabilidad de los proveedores de servicios de búsqueda y directorios de enlaces (Carbajo Cascón, 2014).

rebasa las actividades de mero transporte (mera transmisión) o de almacenamiento automático y temporal (memoria tampón) y no puede beneficiarse de la inmunidad.

El TJUE ha sentado algunas pautas para determinar cuándo nos encontramos ante un servicio de mera intermediación. Así, es necesario examinar si el papel desempeñado por el prestador es neutro, esto es, si su comportamiento es solo técnico, automático y pasivo. La mera circunstancia de que el servicio sea remunerado, o, incluso, de que dé información general a sus clientes, no puede implicar que se excluya a Google de las exenciones de responsabilidad, ni tampoco la concordancia de la palabra clave seleccionada y del término de búsqueda introducido por un internauta basta por sí misma para que se considere que Google tiene conocimiento o control de los datos introducidos en su sistema por los anunciantes y grabados en su servidor. Sin embargo, sí es revelador el papel que desempeña Google en la redacción del mensaje comercial que acompaña al enlace promocional o en el establecimiento o la selección de palabras clave (STJUE de 23 de marzo de 2010, *Google France y Google*, C-236/8 a C-238/8).

Para el caso de la venta de productos en internet por medio de proveedores del servicio de subastas electrónicas y portales que explotan un mercado electrónico, el mero hecho de que el operador almacene en su servidor ofertas de venta, determine las condiciones de su servicio, sea remunerado por este y dé información general a sus clientes no puede implicar que ostente el control de esos contenidos. Por el contrario, cuando este operador presta una asistencia consistente en optimizar la presentación de las ofertas de venta en cuestión o en promover tales ofertas, no ha ocupado una posición neutra entre el cliente vendedor y los potenciales compradores, sino que ha desempeñado un papel activo que le permite adquirir conocimiento o control de los datos (SSTJUE de 12 de julio de 2011, *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal [UK] Ltd*, C-324/09, y de 7 de agosto de 2018, *Coöperatieve VerenigingSNB-REACT U.A. y Deepak Mehta*, C-521/17).

Asimismo, no ocupa una posición neutra una sociedad editora de prensa que dispone de una página de internet en la que se publica la versión digital de un periódico y que, además, obtiene una remuneración de los ingresos generados por la publicidad comercial difundida en esa página, con independencia de que el acceso a dicha página sea gratuito o de pago (STJUE de 11 de septiembre de 2014, *Sotiris Papasawas*, C-291/13).

A tenor de esta jurisprudencia, la determinación de si el servicio prestado puede o no ser considerado neutro corresponde, en último término, al órgano judicial nacional, atendiendo a si la actividad del prestador de servicios tiene naturaleza «meramente técnica», lo que implica que «no ejerce control».

En cambio, para beneficiarse de la exención de responsabilidad, el prestador de un servicio consistente en el almacenamiento de datos, hospedaje o alojamiento web (*hosting*) habrá de actuar con diligencia y por iniciativa propia para retirar los datos o contenidos o impedir el acceso a ellos en cuanto tenga «conocimiento efectivo» o real de su ilicitud. La retirada o la actuación encaminada a impedir el acceso a estos habrá de llevarse a cabo respetando las libertades de expresión e información y los procedimientos establecidos a tal fin en el ámbito nacional.

La noción de «conocimiento efectivo» ha ido, poco a poco, ampliándose jurisprudencialmente en atención a los avances de la tecnología y, sobre todo, al propósito de involucrar más a los prestadores de servicios en el control de las infracciones.

En una primera fase, el conocimiento efectivo se vinculaba a una resolución de un órgano competente (judicial o administrativo) que declarase la lesión o el daño. Desde el instante en que el prestador tuviera conocimiento de esa resolución, debía adoptar las medidas oportunas para la retirada o el bloqueo.

Sin embargo, con el paso del tiempo, el TJUE y los tribunales nacionales han venido aceptando diferentes medios a través de los cuales un prestador puede adquirir «conocimiento efectivo», como puede ser la petición de retirada dirigida al prestador por el perjudicado o por las fuerzas y cuerpos de seguridad.

Al margen de medios externos que le vienen dados al prestador, el conocimiento efectivo puede deducirse de otros hechos o circunstancias aptos para posibilitar, por inferencias lógicas, una efectiva aprehensión de la realidad ilícita (STJUE de 12 de julio de 2011, *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal [UK] Ltd*, C-324/09). Así, la jurisprudencia habla de «intromisiones notorias», públicas y sabidas por todos.

Alguna jurisprudencia ha llegado incluso a fijar una presunción *iuris tantum* a favor de la existencia del conocimiento en algunos concretos supuestos como los vínculos o enlaces proporcionados con ánimo de lucro (STJUE de 8 de septiembre de 2016, *GS Media BV*, C-160/15).

En cualquier caso, las exenciones de responsabilidad descritas no afectan a la posibilidad de que se exija al ISP poner fin a una infracción o impedirla, incluso suprimiendo los datos ilícitos o impidiendo el acceso a ellos (Husovec, 2013). La Directiva sobre el comercio electrónico no se opone a que un juez o tribunal o una autoridad administrativa de un Estado miembro puedan obligar a un prestador a retirar los datos que almacene o a bloquear el acceso a aquellos (arts. 12.2, 13.2 y 14.3).

Ahora bien, estos requerimientos deben ser efectivos, proporcionados, disuasorios y no crear obstáculos innecesarios al comercio legítimo (STJUE

de 12 de julio de 2011, *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal [UK] Ltd*, C-324/09).

En los supuestos en que se ordene administrativa o judicialmente el bloqueo, tanto los proveedores de servicios de internet como los buscadores deben proceder de inmediato a la retirada o al bloqueo y, además, asumir los costes económicos. La colaboración de los ISP es imprescindible y la orden de retirada o bloqueo es una medida restrictiva de la libertad de empresa, pero proporcionada al logro de los fines que la justifican —art. 18.1 de la Directiva del comercio electrónico— (STJUE de 27 de marzo de 2014, *UPC Telekabel*, C-314/12).

Las exenciones de responsabilidad de los ISP no excluyen, en suma, la posibilidad de que el perjudicado entable, conforme al ordenamiento de cada Estado miembro, una acción de cesación de contenidos ilícitos. Dichas acciones pueden dirigirse a los tribunales o a las autoridades administrativas y, aunque el prestador no sea responsable, puede verse obligado a colaborar en la cesación o reparación del perjuicio o daño infligido (STJUE de 11 de septiembre de 2014, *Sotiris Papasavvas*, C-291/13).

3. EL PRINCIPIO DE NO SUPERVISIÓN Y EL DEBER DE COLABORACIÓN

El ISP no responderá en ningún caso por el incumplimiento de una genérica obligación de supervisión de contenidos, que no puede exigírsele *a priori*. La directiva prohíbe, en efecto, a los Estados imponer el filtrado o control *ex ante* (art. 15.1).

Imponer a un proveedor de servicios la obligación de supervisar o monitorizar activamente la totalidad de sus contenidos (en este caso, por el simple riesgo de ser sancionado si algo infringe los derechos de autor) es una medida desproporcionada, tanto por la inversión tecnológica que supone como por el riesgo de lesión de los derechos fundamentales de los usuarios. Una obligación que no respeta el «justo equilibrio» entre la protección de cualesquiera bienes jurídicos y los derechos fundamentales a expresarse libremente y a recibir y emitir información (SSTJUE de 16 de febrero de 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA [SABAM] y Netlog NV*, C-360/10, de 8 de septiembre de 2016, *GS Media BV y Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker*, C-160/15, y de 7 de agosto de 2018, *Land Nordrhein-Westfalen y Dirk Renckhoff*, C-161/17, entre otras).

La jurisprudencia europea, sin embargo, ha ido modulando en determinadas circunstancias el principio general de no supervisión/no filtrado para

supuestos de, por así decir, control *a posteriori* —tras la constatación judicial o administrativa del contenido infractor—.

La directiva del comercio electrónico ampara que se obligue a un prestador de servicios de alojamiento de datos como Facebook a suprimir comentarios idénticos y, en determinadas condiciones, similares a un comentario declarado judicialmente ilícito (contrario al honor). Lo novedoso es que se sienta la obligación del intermediario de detectar y retirar no solo las expresiones exactamente iguales a las declaradas difamatorias, sino también las similares, de modo que el intermediario debe detectar por su cuenta tales contenidos (STJUE de 3 de octubre de 2019, *Eva Glawischnig-Piesczek c. Facebook Ireland*, C-18/18).

Cuestión diferente es que los operadores de transmisión de datos actúen *motu proprio*, implementando programas de filtrado que detectan expresiones en la información que pueden indicar la existencia de contenidos ilícitos para proceder a su bloqueo siquiera preventivo. Actuación precautoria que puede derivarse de la adhesión a códigos de buena conducta o códigos de práctica (art. 15.2). La autorregulación, o autocontrol, puede resultar provechosa.

Nótese que la directiva no regula de forma expresa (a diferencia de lo que sucede en la legislación estadounidense) la obligación de los intermediarios de implementar un sistema de «denuncia y retirada» (*notice & takedown*) de contenidos ilícitos a disposición del perjudicado. El legislador europeo, debido al carácter horizontal de la regulación (frente a la DMCA americana, centrada en la infracción de derechos de propiedad intelectual), ha preferido dejar al legislador nacional o a la autorregulación de los ISP la posibilidad de emplear sistemas de estas características, sin establecer exigencias de ningún tipo sobre el procedimiento que seguir y sobre la influencia de tales sistemas a la hora de enjuiciar la existencia o no de «conocimiento efectivo» en el ISP (STEDH, Gran Sala, de 16 de junio de 2015, *Delfi AS c. Estonia*). Se deja a la libre voluntad del legislador nacional o a los códigos internos de conducta generales o sectoriales la introducción de sistemas de denuncia y retirada.

En sentido análogo, la directiva faculta a los Estados miembros para establecer obligaciones tendentes a que los ISP comuniquen con prontitud a las autoridades públicas 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 estas, información que les permita identificar a los destinatarios de su servicio. En la adopción y en el cumplimiento de estas obligaciones, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento nacional para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información.

La directiva no impone un deber general de colaboración de los prestadores de servicios de intermediación para la identificación de los usuarios que cometen ilícitos a través de su servicio o sistema, sino que vuelve a dejar la decisión final a los Estados miembros.

El Derecho de la UE no obliga a los Estados miembros a imponer en su legislación interna el deber de comunicar datos personales con objeto de garantizar la protección efectiva frente a contenidos ilícitos en el marco de un procedimiento civil, aunque admite que puede ser una opción legítima. El derecho a la intimidad y a la privacidad de las comunicaciones no está por encima del derecho de propiedad (intelectual) y, en consecuencia, en la búsqueda de un justo equilibrio entre ambos, la normativa comunitaria no excluye la facultad de los Estados para implementar mecanismos legales que impongan a los prestadores de servicios de acceso la obligación de comunicar esos datos (STJUE, Gran Sala, de 29 de enero de 2008, *Promusicae c. Telefónica*, C-275/06).

El TEDH ha ido algo más allá y ha dado la razón a los jueces nacionales que habían condenado a un sitio web por los comentarios ofensivos y anónimos alojados en la web. Las webs, en las circunstancias del caso, debieron poner filtros para evitar mensajes insultantes e identificar a los infractores. Al no hacerlo, incurrieron en responsabilidad *in vigilando* (STEDH, Gran Sala, de 16 de junio de 2015, *Delfi AS c. Estonia*).

4. EL RÉGIMEN ESPECIAL PARA LOS DERECHOS DE AUTOR: EL FILTRADO COMO MEDIDA EFECTIVA

Ante el imparable menoscabo de los derechos de autor en el ciberespacio, la reciente Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital, exige que los servicios de almacenamiento y puesta en común de contenidos en línea hagan «los mayores esfuerzos» (art. 17.4) para garantizar que las subidas de contenidos por los usuarios de sus sistemas no supongan una infracción de *copyright*. De no lograrse este objetivo, entonces los servicios serían responsables de las infracciones. Tal obligación requiere aparentemente que esos servicios empleen tecnologías de supervisión y filtrado, lo que va más allá de lo exigido por la Directiva sobre el comercio electrónico. Es cierto que el precepto no impone directamente el uso de esas tecnologías, pero puede interpretarse razonablemente en el sentido de que tiene la intención de lograr dicho resultado.

Los ISP tienen que controlar las prácticas de sus usuarios y utilizar tecnologías de supervisión para evitar que los materiales infractores se carguen y

almacenen en sus sistemas. Algunos proveedores de servicios de internet deben asumir mayores responsabilidades para ayudar a prevenir las infracciones. El art. 17 se dirige específicamente a los proveedores de servicios digitales que permiten compartir contenidos en línea (véanse YouTube, Vimeo, Dailymotion, etc.) y que ostentan una posición dominante en el mercado. Si uno de los objetivos principales del servicio es proporcionar acceso a grandes cantidades de contenidos protegidos por derechos de autor cargados por los usuarios y organiza y promueve dichas subidas con fines lucrativos, entonces dicho servicio perderá la inmunidad otorgada por las reglas de puerto seguro.

El art. 17 establece, en efecto, que el proveedor de servicios de uso compartido de contenidos en línea no será responsable de las infracciones perpetradas por sus usuarios cuando: a) obtenga una autorización de los titulares de los derechos —mediante acuerdo de licencia— (art. 17.1); b) demuestre, aun sin autorización, que ha hecho «los mayores esfuerzos» para impedir la disponibilidad de las obras mediante la aplicación de medidas efectivas y proporcionadas —siempre que los titulares de derechos hayan suministrado al servicio la información pertinente y necesaria para la aplicación de tales medidas— (art. 17.4), y c) cuando, tras la notificación de la infracción, haya actuado «de modo expeditivo» para suprimir o inhabilitar el acceso a estas obras u otros objetos protegidos y demuestre que ha hecho «los mayores esfuerzos» para impedir su futura disponibilidad a través de las medidas mencionadas en la letra anterior (art. 17.4). En suma, o licencia o, si no, máxima diligencia en la retirada.

III. *DE LEGE FERENDA*

En los últimos años, en la UE se viene abriendo paso una nueva tendencia legislativa y jurisprudencial orientada a exigir una labor más activa de los ISP para la adecuada protección de un buen número de derechos e intereses legítimos. Se quiere involucrar más a los intermediarios de internet en el respeto a estos bienes jurídicos y, por ende, en el control de los contenidos ilícitos o infractores. Se quiere que sean más responsables.

Ello plantea un interesantísimo debate de política legislativa. El desafío es mayúsculo: diseñar un marco legal que permita mantener un ecosistema dinámico, diverso y abierto a la innovación para que puedan seguir sumándose nuevas voces y emprendimientos a internet, que promueva derechos fundamentales, como la libertad de expresión y el acceso a la información en tiempos digitales, pero que, al mismo tiempo, proteja adecuadamente otros derechos, bienes y valores, como el honor, la intimidad, la propia imagen, la

propiedad industrial, la propiedad intelectual, la protección de los menores, el acceso transparente a la información veraz o el interés de la justicia en la prevención y represión del delito.

1. EN TORNO A LA CONVENIENCIA DE PONER AL DÍA LA DIRECTIVA SOBRE EL COMERCIO ELECTRÓNICO

Hay unanimidad entre la doctrina a la hora de insistir en la necesidad de poner al día la Directiva sobre el comercio electrónico. Una normativa que tiene veinte años y que debe atender a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de contenidos como consecuencia del funcionamiento del mercado interior, los desafíos planteados por la rápida evolución tecnológica y la globalización, lo que ha ocasionado que internet se haya convertido en una realidad omnipresente en nuestra vida tanto personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. El aumento de los flujos de contenidos tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también riesgos, pues las actividades, los datos y la información sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su uso y destino.

En los últimos años, como se ha visto, se ha intensificado el debate político-legislativo tendente a optimizar el régimen de responsabilidad de los ISP. Todo este bagaje normativo y jurisprudencial debiera conducir a una próxima reforma del marco general de la responsabilidad previsto en la Directiva 2000/31, sobre el comercio electrónico.

2. IMPRESCINDIBILIDAD DEL CONTROL JUDICIAL DE CONTENIDOS

Hay, asimismo, consenso doctrinal en torno a lo que cabría denominar la imprescindibilidad del control judicial de los contenidos (Teruel Lozano, 2016).

Idealmente, la revisión judicial es la mayor garantía para las libertades de expresión e información —y otros derechos fundamentales en juego— y la modalidad de control más respetuosa con la posición de intermediación, neutral o pasiva, de los ISP. Es también la solución más coherente siguiendo la

lógica de la Directiva sobre el comercio electrónico, que prohíbe la supervisión o monitorización generalizada de los contenidos en internet, precisamente en aras del «justo equilibrio» entre las libertades de expresión e información y otros posibles bienes jurídicos. El ISP es sujeto privado, no es autoridad, y no debe, en principio, controlar.

Es, por lo demás, un control indispensable e indisponible para los Estados miembros que deriva del reconocimiento del derecho a la tutela judicial efectiva tanto en el derecho de la UE (art. 47 CDFUE) como en las constituciones nacionales. Toda persona tiene derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso pueda producirse indefensión. Y entre esas personas, también ISP y usuarios de internet.

3. EL CONTROL ADMINISTRATIVO COMO OPCIÓN EN AUGE Y ¿RECOMENDABLE?

Hoy existe en todo el mundo una tendencia normativa creciente orientada a aumentar el control sobre los ISP, incluyendo la atribución a autoridades administrativas de cada vez más facultades de supervisión. Estas autoridades independientes tienen una larga tradición en el campo de la protección de los datos personales (art. 8 CDFUE), si bien hoy la variedad de órganos (judiciales y administrativos) a la que se puede acudir para recabar protección frente a un contenido ilícito se extiende a otros muchos ámbitos (Rallo Lombarte, 2002).

La legitimidad del control administrativo de contenidos descansa, primero, en que sea una ley formal la que autorice al poder público, y, segundo, en que las resoluciones sean motivadas (*op. cit.*). No todo es libertad de expresión o de información en internet y, por tanto, no toda restricción de acceso a los contenidos de la red requiere de la garantía judicial. No obstante, no es descartable que en la oferta de bienes y servicios en internet las resoluciones administrativas puedan afectar a derechos fundamentales. De ahí que deba asegurarse la revisión judicial de la decisión administrativa.

El control administrativo no suele producirse de oficio, sino previa solicitud del titular de derechos; solicitud que no podrá ser genérica o alusiva a un catálogo de servicios o contra un sitio web, sino que tendrá que especificar contenidos infractores.

No existe restricción constitucional, al menos a nivel de los textos internacionales, a que la Administración pueda controlar los excesos en el ejercicio de las libertades de expresión e información. A nivel nacional habría que fijarse en

aquellos Estados que, más allá de la prohibición de censura previa, recogen también la prohibición del secuestro administrativo de comunicaciones, proyectándose este no solo como una prohibición de secuestro preventivo, sino como una más amplia prohibición de intervención de la Administración en este ámbito.

Si la respuesta europea pudiera ser distinta en atención a las peculiaridades constitucionales de cada Estado miembro, estaríamos ante una cuestión de difícil armonización legislativa. Resultaría, pues, discutible que, en una futura revisión de la Directiva sobre el comercio electrónico, se incluyera el control administrativo como estándar común.

Estándar común que, a mi entender, debiera estar integrado más bien por las dos garantías siguientes: 1) que el control del órgano competente (preferiblemente judicial) sea el resultado (incluso como medida cautelar) de un proceso legalmente establecido para tutelar los bienes y derechos que pudieran verse lesionados, y 2) que el control se ejerza sobre unos contenidos determinados y concretamente identificados, sin sistemas genéricos de filtrado.

4. ¿CORRESPONSABILIZAR A LOS PRESTADORES DE SERVICIOS DEL CONTROL?

Otras propuestas *de lege ferenda* son más polémicas, empezando por la ampliación de la responsabilidad de los ISP en el control de contenidos. Así, se ha sugerido fomentar el uso de mecanismos automatizados de búsqueda activa de contenidos infractores, aun dejando claro que, en ningún caso, se puede infringir la prohibición de la obligación general de supervisión que sienta la Directiva sobre el comercio electrónico (art. 15.1).

El inconveniente es que incentivar la monitorización o el filtrado por los ISP puede comprometer seriamente las libertades de expresión e información de los usuarios. En tal sentido, alguna doctrina ha denunciado la creciente intervención privada de las grandes tecnológicas en el libre flujo de internet, con un impacto negativo en la libre comunicación, mediante restricciones *directas* (remoción o bloqueo) o *indirectas* (priorización o reducción de alcance) de contenidos (Teruel Lozano, 2014; 2016).

Si los ISP, en tanto solo ofrezcan servicios técnicos y no intervengan de ninguna manera en los contenidos, no son responsables, por esa misma lógica no debieran erigirse en «órganos competentes» llamados a decidir qué contenidos pueden circular (De Gregorio, 2018).

Como se ha dicho, hay que revisar la concepción tradicional de la prohibición de censura previa, clásicamente concebida como garantía frente a cualquier medida limitativa de la elaboración o difusión de una obra, especialmente al hacerla depender del previo examen oficial de su contenido. Esto es, convendría

alumbrar una definición más amplia de censura que abarque cualquier limitación (pública o privada) de las libertades de expresión e información (García Morales, 2013). En principio, ello conduciría a una descalificación de los sistemas de filtrado y bloqueo, aunque, excepcionalmente, se podrían admitir en el marco de una concreta orden dictada por un órgano competente.

En cualquier caso, resulta inaplazable aprobar una adecuada regulación (autocontrol, autoetiquetado, supervisión de la autoridad independiente, etc.) de estos filtros que ya utilizan algunos servidores y buscadores, exigiéndose, ante todo, transparencia y pluralidad para evitar formas privadas de censura.

En cuanto a los sistemas de denuncia y retirada, parece razonable exigir que la notificación sea lo suficientemente precisa y razonada como para que el ISP pueda tomar una decisión fundada al respecto. La identificación del denunciante no debiera ser obligatoria para iniciar el procedimiento, aunque es recomendable su inclusión con el fin de facilitar un procedimiento con garantías. El ISP debiera informar tanto al denunciante como al titular del contenido supuestamente ilícito de las medidas que va a llevar a cabo. El ISP debiera instaurar un procedimiento de «contranotificación» que permitiera al titular del contenido supuestamente infractor formular alegaciones. La «contranotificación» no se exigiría en casos de manifiesta ilicitud del contenido o, aún más, grave ilicitud penal con peligro para la vida o la seguridad de las personas. En otros supuestos relacionados con la prevención del delito, cabría que la autoridad competente eximiera al ISP de la obligación de notificar al supuesto infractor por motivos de orden público o, en puridad, de seguridad pública.

Los ISP debieran publicar cuáles son sus procedimientos de notificación y retirada y cómo se implementan. El objetivo es, de nuevo, lograr una regulación cuidadosa que respete las libertades de expresión e información y acote el control privado. Está bien que a través de la autorregulación los ISP se involucren en el control. Pero la autorregulación tiene límites, máxime cuando hay derechos fundamentales en juego. El legislador democrático está facultado para prever medidas correctoras ante posibles abusos de posición dominante (Teruel Lozano, 2014). Convendría, en suma, combinar autorregulación y ley, actuando esta *ex ante* para definir el marco general del autocontrol y *ex post* para evitar desvíos.

5. ¿UN NUEVO ESTÁNDAR SOBRE EL «CONOCIMIENTO EFECTIVO» DE LA ILICITUD?

La Directiva sobre el comercio electrónico exime de responsabilidad al ISP que no tiene «conocimiento efectivo» de la ilicitud del contenido. La

norma europea impone este requisito, pero no aclara de qué forma el ISP puede conocer realmente. Algunas leyes nacionales han intentado clarificar tal noción[11]. En este contexto, se comprende que el conocimiento efectivo, en cuanto estándar jurisprudencial, haya evolucionado notablemente en atención a la variedad de casos a la que se han enfrentado tanto el TJUE como los jueces y tribunales nacionales.

En un primer momento, se interpretó que un ISP tenía responsabilidad cuando un órgano competente (judicial o, excepcionalmente, administrativo) declarase la ilicitud del contenido y el intermediario, tras conocer la resolución, no lo retirara. Ello obligaba a la «judicialización» de toda reclamación, y, en principio, el ISP no debía retirar (porque no era responsable) hasta que un juez u órgano administrativo decretase la ilicitud, lo que podía durar años (Groussot, 2008).

Esta interpretación podía tener sentido en una internet de finales del siglo pasado, pero se comprobó poco práctica con la irrupción de la denominada «web semántica» o «web 2.0», en la que los usuarios son no solo consumidores, sino también originadores de contenidos. Se cayó, pues, en la cuenta de que la solución debería pasar por no limitar la responsabilidad a la constatación judicial o administrativa de la infracción, sino valorar otros posibles medios de conocimiento efectivo.

Así, los jueces han venido aceptando diferentes medios a través de los cuales un ISP puede adquirir conocimiento real, como la solicitud de retirada o bloqueo del perjudicado o de las fuerzas y cuerpos de seguridad del Estado. En cuanto el ISP conozca que la información subida por un usuario infringe derechos de terceros, debe eliminarla o bloquearla si no quiere ser corresponsable de la infracción (Capodiferro, 2017).

Pero ¿qué ocurre cuando el prestador ha desarrollado una plataforma que facilita la infracción? ¿Cuándo adquiere conocimiento en tales circunstancias? Determinadas tecnologías son completamente neutras, como un servidor de alojamiento de datos o un buscador de internet; sin embargo, hay plataformas diseñadas específicamente para facilitar u optimizar una conducta infractora (Angelopoulos, 2015).

Estos interrogantes fueron despejados por el TJUE, en 2011, con ocasión del famoso caso *L´Oreal v. eBay*. El TJUE estimó que un ISP no podía acogerse al «puerto seguro» cuando había tenido un papel activo en la conducta lesiva, en especial prestando asistencia a la presentación de ofertas (en este caso, infringiendo derechos de marcas por la venta de falsificaciones). Además, el

[11] Así, los arts. 15 y 16 de la Ley española 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

TJUE consideró que los jueces nacionales podían adoptar, a la luz de las circunstancias de cada controversia concreta, medidas contra los ISP destinadas a evitar que se repitieran *pro futuro* las lesiones.

Por esas mismas fechas, algunos altos tribunales nacionales se pronunciaron sobre la cuestión de qué sucede cuando el perjudicado no identifica con detalle qué contenidos lesionan sus derechos. ¿Cómo puede entonces el ISP conocer la infracción? Así, el Tribunal Supremo español aclaró que, cuando los contenidos infractores son notorios, un ISP no puede alegar falta de conocimiento efectivo[12].

Ante este aumento paulatino del grado de responsabilidad de los ISP, los titulares de derechos de propiedad intelectual demandaron el establecimiento de la obligación general de supervisión a través de filtros, algo que el TJUE consideró, en 2012, contrario al derecho de la Unión (STJUE de 16 de febrero de 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA [SABAM] c. Netlog NV*, C-360/10).

Tras casi dos décadas de aplicación y desarrollo de este estándar de responsabilidad de los servicios en línea, con abundante jurisprudencia comunitaria y nacional, el Parlamento Europeo estimó necesaria su revisión, aunque solo aplicable a la violación de derechos de propiedad intelectual. En efecto, en la Directiva sobre los derechos de autor y derechos afines de 2019, el ya analizado y polémico art. 17 establece que los servicios usados por los usuarios para cargar contenido no podrán acogerse al régimen de exención de responsabilidad operativo durante años, debiendo adquirir una licencia para llevar a cabo esa puesta a disposición o, alternativamente, realizar sus mejores esfuerzos para garantizar la indisponibilidad de las obras protegidas (Curto, 2019).

Una vez que esta directiva se haya implementado en los Estados miembros, servicios como YouTube o Instagram serán responsables por la explotación de contenido ajeno cargado por sus usuarios si carecen de una licencia, si no disponen de medios y protocolos para evitar dicha disponibilidad o si, tras recibir una notificación, no actúan de forma diligente y realizan los mejores esfuerzos para evitar que dicho contenido se vuelva a poner a disposición.

Es evidente que este nuevo estándar de responsabilidad supone un paso más en la involucración de los ISP en el control de las conductas ilícitas (STEDH, Gran Sala, de 16 de junio de 2015, *Delfi AS c. Estonia*). Un paso más que probablemente se acabe extendiendo a otros derechos e intereses legítimos y que, en último término, implica el establecimiento de una suerte de responsabilidad proactiva (*accountability*), similar a la prevista en el Reglamento general de protección de datos de 2016.

[12] STS de 10 de febrero de 2011.

La internet actual poco se parece a la que existía en el año 2000, tanto por las tecnologías ahora disponibles para transmitir información como por las técnicas para evitar la puesta a disposición de contenidos ilícitos. El reto, en el contexto de una posible revisión de la Directiva sobre el comercio electrónico, radica en la correcta delimitación de un nuevo estándar sobre «el conocimiento efectivo» de la ilicitud y su aplicación por los tribunales que asegure el difícil equilibrio entre la evolución de la tecnología y el respeto de los derechos e intereses legítimos ajenos.

6. ¿DIFERENCIAR ENTRE PRESTADORES DE SERVICIOS?

Por último, se ha sugerido que el régimen de la responsabilidad de los ISP debería prever diferencias de trato o asimetrías, teniendo en cuenta la realidad del mercado interior. Habría que valorar si conviene, y es conforme al ordenamiento de la UE, diferenciar entre, de un lado, la responsabilidad de las grandes plataformas de internet, y, de otro, la responsabilidad de las *start-up* o empresas emergentes, pequeñas empresas e iniciativas cooperativas, educativas y sin ánimo de lucro. Es decir, endurecer, con más obligaciones, el régimen de la responsabilidad de las grandes plataformas, pero sin frenar u obstaculizar la innovación, competencia y desarrollo de las empresas emergentes sin ánimo de lucro, que deben poder seguir surgiendo y existiendo en internet dentro de un marco regulador más favorable (Riordan, 2016: 315 y ss.). En tal sentido, el concepto de *smart regulation* propone racionalizar la elaboración de las leyes y defiende que no se trata de regular más, sino de hacerlo de manera más inteligente, considerando siempre la importancia de mantener un entorno económico atractivo y flexible para la actividad del sector privado, distinguiendo en función de las concretas necesidades de los distintos agentes económicos que en él intervienen (García García, 2019).

Desde una óptica más jurídica, la igualdad en la ley es un derecho fundamental de toda persona —física o jurídica— respecto de cualquier relación jurídica, que vincula a los poderes públicos que aprueban normas, a los creadores del derecho de la UE, reconocido ampliamente en las constituciones de los Estados miembros, en la Carta de Derechos Fundamentales de la UE (art. 20) y que el TJUE ha catalogado como un principio basilar del derecho europeo (por todas, SSTJUE de 13 de noviembre de 1984, *Racke*, 283/83, de 17 de abril de 1997, *EARL*, C-15/95, y de 13 de abril de 2000, *Karlsson*, C-292/97).

El derecho a la igualdad en la ley postula, como regla, la generalidad de la ley, pero no es incompatible con el trato diferenciado siempre que tal diferencia tenga un fundamento objetivo y razonable. Desde el punto de vista de

las consecuencias jurídicas del trato diferenciado, la igualdad en la ley implica también una exigencia de proporcionalidad, de manera que a una diferencia fáctica trivial no se le atribuyan grandes consecuencias jurídicas. Esta doble exigencia, razonabilidad y proporcionalidad *stricto sensu* del trato diferenciado, evidencia que la obligación correlativa del derecho a la igualdad es la interdicción de la arbitrariedad (STJUE de 13 de noviembre de 1984, *Racke*, 283/83).

En consecuencia, no sería, a mi juicio, contrario a la igualdad en la ley que el legislador europeo, y en concreto la Directiva sobre el comercio electrónico, ponderase y distinguiera, al hilo de la responsabilidad de los ISP, entre las grandes plataformas y las plataformas emergentes o pequeñas. Es más, el legislador europeo ya viene caminando desde hace algún tiempo en esta dirección. La Directiva sobre los derechos de autor y derechos afines (art. 17) es la mejor y más reciente prueba de ello[13].

Bibliografía

Angelopoulos, C. (2015). Sketching the outline of a ghost: the fair balance between copyright and fundamental rights in intermediary third party liability. *Info*, 17, 72-96. Disponible en: https://doi.org/10.1108/info-05-2015-0028

Arroyo Amayuelas, E. (2020). La responsabilidad de los intermediarios en internet. ¿Puertos seguros a prueba de futuro? *Cuadernos de Derecho Transnacional*, 12, 808-837. Disponible en: https://doi.org/10.20318/cdt.2020.5225

Bellido Barrionuevo, M. (2003). *La directiva comunitaria*. Madrid: Dykinson.

Capodiferro Cubero, D. (2017). La libertad de información frente a Internet. *Revista de Derecho Político*, 100, 701-737. Disponible en: https://doi.org/10.5944/rdp.100.2017.20715

Carbajo Cascón, F. (2014). Delimitación de la responsabilidad de los servicios de intermediación de la sociedad de la información (I). *Iustitia*, 12, 245-278. Disponible en: https://doi.org/10.15332/iust.v0i12.1499

Curto, N. (2019). EU Directive on Copyright in the Digital Single Market and ISP Liability: What's Next at International Level? *Journal of law, technology & the internet*, 11 (3), 84-110. Disponible en: https://doi.org/10.2139/ssrn.3434061

[13] Entre la legislación nacional más reciente, la alemana *NetzDG* o Ley de protección en redes sociales, de 1 de septiembre de 2017. Esta ley fija un límite temporal sumamente ajustado para la retirada de contenidos (24 horas para contenidos manifiestamente ilícitos, 7 días para otros casos) y la imposición de unas sanciones en absoluto nimias (hasta 50 millones de euros en los casos más graves), y, sobre todo, circunscribe su ámbito de aplicación a redes sociales con más de dos millones de usuarios registrados en Alemania.

De Gregorio, G. (2018). Freedom of Expression and ISP Liability in the European Digital Single Market. *European Competition and Regulatory Law Review*, 2, 203-215. Disponible en: https://doi.org/10.21552/core/2018/3/7

Frosio, G. (2017). Reforming Intermediary Liability in the Platform Economy: a European Digital Single Market Strategy. *Northestern University Law Review*, 112 (19) 19-46. Disponible en: https://doi.org/10.2139/ssrn.3009155

García García, M. J. (2019). Smart regulation law-making and participatory democracy: consultation in the European Union. *Revista Catalana de Dret Públic*, 59, 85-96.

García Morales, M. J. (2013). La prohibición de la censura en la era digital. *Teoría y Realidad Constitucional*, 31, 237-276. Disponible en: https://doi.org/10.5944/trc.31.2013.10308

Garrote Fernández-Díez, I. (2014). *La responsabilidad de los intermediarios en Internet en materia de propiedad intelectual. Un estudio de derecho comparado*. Madrid: Tecnos.

Groussot, X. (2008). Music production in Spain (Promusicae) vs. Telefónica de España SAU - Rock the KaZaA: another clash of fundamental rights. *Common Market Law Review*, 45 (6), 1745-1766.

Husovec, M. (2013). Injunctions against innocent third parties: case of website blocking. *Journal of Intellectual Property. Information Technology and Electronic Commerce Law*, 4 (2), 116-129.

Kleinschmidt, B. (2010). An International Comparison of ISP's Liabilities for Unlawful Third Party Content. *International Journal of Law and Information Technology*, 18, 332-355. Disponible en: https://doi.org/10.1093/ijlit/eaq009

Pauner Chulvi, C. (2018). Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red. *Teoría y Realidad Constitucional*, 41, 297-318. Disponible en: https://doi.org/10.5944/trc.41.2018.22123

Rallo Lombarte, A. (2002). *La constitucionalidad de las autoridades independientes*. Madrid: Tecnos.

Riordan, J. (2016). *The liability of internet intermediaries*. Oxford: Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780198719779.001.0001

Salvador Coderch, P. y Ruiz García, J. A. (2001). Directiva sobre comercio electrónico: control de contenidos. *Indret: Revista para el Análisis del Derecho*, 1.

Synodinou, T. (2015). Intermediaries' liability for online copyright infringement in the EU: evolutions and confusions. *Computer Law & Security Review*, 31(1), 57-67. Disponible en: https://doi.org/10.1016/j.clsr.2014.11.010

Teruel Lozano, G. (2014). Libertad de expresión y censura en internet. *Estudios Deusto*, 62, 41-72. Disponible en: https://doi.org/10.18543/ed-62(2)-2014pp41-72

—— (2016). Perspectivas de los derechos fundamentales en la sociedad digital. *Fundamentos: Cuadernos monográficos de teoría del Estado, Derecho público e Historia Constitucional*, 9, 217-243.

Urban, J. M., Karaganis, J. y Schofield, B. (2016). *Notice and Takedown in Everyday Practice*, *The American Assembly*. New York: Columbia University. Disponible en: https://doi.org/10.31235/osf.io/59m86