

MENSAJES Y MENSAJEROS EN INTERNET: LA RESPONSABILIDAD CIVIL DE LOS PROVEEDORES DE SERVICIOS INTERMEDIARIOS*

Miquel Peguera Poch
Universitat Oberta de Catalunya
mpeguera@campus.uoc.es

I. EL DERECHO DE DAÑOS EN SOCIEDAD DE LA INFORMACIÓN.— II. EL SISTEMA DE EXENCIONES DE RESPONSABILIDAD ESTABLECIDO EN LA DIRECTIVA DE COMERCIO ELECTRÓNICO. 1.- La exención de responsabilidad del prestador de servicios en el caso de mera transmisión de datos y de provisión de acceso. 2.- La exención de responsabilidad en el *caching*. 3.- La exención de responsabilidad en el supuesto de alojamiento de datos. 4.- El alcance de las exenciones. 5.- Las acciones de cesación y/o impedimento de una infracción. 6.- Obligaciones de supervisión y de comunicación.— III. LA FUTURA TRANSPOSICIÓN AL DERECHO INTERNO DEL RÉGIMEN DE EXENCIONES DE RESPONSABILIDAD SEGÚN EL ANTEPROYECTO DE 18 DE ENERO DE 2001.— 1.- Las normas generales sobre responsabilidad. 2.- Las exenciones de responsabilidad. 2.1. Transmisión de datos o provisión de acceso a red. 2.2. Almacenamiento en *caching*. 2.3. Alojamiento o *hosting*. 2.4. Hiperenlaces, directorios y motores de búsqueda. 3.- Límites y obligaciones en la prestación de servicios. 3.1. Restricciones a la libre prestación de servicios. 3.2. Obligaciones de comunicación a las autoridades. 3.3. Obligaciones de supervisión en casos específicos. 3.4. Obligación de poner fin a una infracción o impedir la.

I. EL DERECHO DE DAÑOS EN LA SOCIEDAD DE LA INFORMACIÓN.

La llamada *sociedad de la información* se caracteriza por la consolidación mundial de una nueva esfera de actuación: la de las comunicaciones electrónicas. Hacía este nuevo ámbito se trasladan, o se extienden, muchas de las actividades que hasta ahora estaban enmarcadas en

* El presente trabajo constituye un primer borrador de un estudio más amplio sobre la materia que será objeto de publicación próximamente.

Quien esté interesado en recibir comentarios y noticias sobre Derecho y Sociedad de la Información, elaborados por los Estudios de Derecho de la Universitat Oberta de Catalunya, puede enviar un mensaje al autor de este trabajo <mpeguera@campus.uoc.es> indicando su dirección de correo electrónico y sus preferencias temáticas y será incluido en la base de datos de nuestros próximos boletines informativos.

un escenario físico, compartimentado y lleno de barreras y distancias. El desembarco vertiginoso de los actores sociales, económicos y jurídicos en esta nueva esfera nos sitúa constantemente ante la duda de si las normas que hemos utilizado hasta ahora conservarán su capacidad de ordenar y resolver los conflictos que ya han empezado a originarse. Porque es claro que entre las bondades del ciberespacio no se halla la de hacer desaparecer como por ensalmo los conflictos jurídicos. Los sujetos que interactúan en este espacio virtual (esto es, quienes se relacionan por medio de sistemas electrónicos de comunicación) no pierden (es claro que no pueden perder) su aptitud esencial para ser titulares de derechos y de obligaciones. En todas las relaciones, también en las que es vehiculan por los canales cibernéticos, existen titularidades jurídicas activas y pasivas, ejercicio de derechos y cumplimiento (o incumplimiento) de obligaciones. En dos palabras: dimensión jurídica, tanto estática como dinámica. Y por tanto, hay posibilidad y probabilidad de patologías y conflictos. Entre otros la producción de daños, que determinará el nacimiento de responsabilidades.

Pensemos en ello un momento: ¿qué daños pueden producirse en el ámbito de este contexto de relaciones virtuales? Pueden producirse, por ejemplo, daños derivados del incumplimiento de contratos en el marco del comercio electrónico, o perjuicios por el uso fraudulento de tarjetas de crédito, o por la entrega final de productos defectuosos, o por el uso indebido de datos personales tratados informáticamente, o por ataques a la intimidad mediante el correo electrónico, o por piratería de nombres de dominio, o por acciones ilícitas en materia de propiedad intelectual o industrial, o bien perjuicios derivados de la multitud de engaños y estafas que parece que el anonimato electrónico propicia. También podemos pensar, por ejemplo, en los daños que ocasiona un virus informático que se propaga por todo el mundo a velocidad de vértigo. O en los desastres que se producen cuando en un banco, o en cualquier empresa, resulta de repente que el *software* no responde y el “sistema” provoca el caos y pérdidas millonarias. O bien fijémonos en los perjuicios que pueden resultar de fallos en los mecanismos de seguridad informática, por ejemplo en los sistemas de encriptación. La lista sería inacabable. Entre de otras razones, porque (casi) todo el mundo puede acceder a la red con gran facilidad, y por desgracia es muy fácil provocar daños de gran repercusión económica y también moral. De modo que si por una parte las nuevas tecnologías nos ofrecen una gran cantidad de ventajas, por otra parte multiplican los riesgos y las posibilidades de accidentes, daños y perjuicios.

A la aparición de riesgos hasta ahora desconocidos se suma, además, la complejidad técnica de los conflictos, que deriva de un cambio radical de coordenadas, ya que estos riesgos nuevos se plantean en un escenario que también es nuevo. En un escenario en el que ya no hay fronteras ni largas distancias, y en el que surge la dificultad añadida de tener de buscar soluciones jurídicas globales, habida cuenta de los graves problemas de determinación de la ley aplicable y de la jurisdicción competente.

En todos los momentos históricos marcados por la innovación y el progreso industrial y tecnológico, el sistema de responsabilidad civil, o en sentido más general el derecho de daños, emerge con un protagonismo especial, estableciendo una serie de reglas que son claves para al desarrollo y puesta en marcha de las nuevas actividades y tecnologías (nuevas fuentes de riesgos y de potenciales daños). Son las reglas que determinan qué niveles y tipos de riesgos serán tolerables y de qué manera y quién los habrá de soportar.

La finalidad básica de las reglas de responsabilidad es la de resarcir o reparar económicamente el daño causado, cosa que es fácilmente apreciable si consideramos un supuesto particular y concreto en que se ha producido un daño. Pero los objetivos y la

incidencia del derecho de daños va mucho más allá, porque busca también dar respuestas a una serie de cuestiones esenciales de política jurídica. Así, por ejemplo, a la hora de construir la disciplina de la responsabilidad por daños, el legislador ha de decidir si a la vista del nuevo marco de actividades y riesgos será necesario redefinir con mayor precisión cuáles serán los supuestos resarcibles, y en qué medida, en qué condiciones y con qué requisitos lo serán.

El sistema de responsabilidad civil jugará, pues, el difícil papel de distribuir entre los diferentes sujetos implicados la carga de los costes asociados al desarrollo y a la aplicación de los nuevos progresos. Más precisamente: tendrá que fijar los criterios que permitan determinar a quién corresponderá el deber legal de soportar las consecuencias de los daños y perjuicios derivados de los riesgos inherentes a las nuevas actividades. O -por decirlo de otra manera- tendrá que decidir con el dinero y el sacrificio de quién se va a pagar todo lo que la flamante *sociedad de la información* nos va a costar.

Y deberá establecer también los mecanismos jurídicos oportunos que incentiven a los operadores a adoptar medidas adecuadas de prevención para reducir al máximo el número de accidentes y daños. Pero tendrá que hacerlo conjugando adecuadamente los intereses en presencia. En este sentido, por ejemplo, el derecho daños deberá determinar hasta a qué punto una carga excesiva en términos de responsabilidad por daños podría poner (o no) en peligro la propia consolidación o expansión de los operadores económicos que tienen que hacer realidad la nueva economía. En otras palabras: de qué límites, en términos de responsabilidad, podrá (o no) disfrutar el prestador de un determinado tipo de servicios.

Estamos pensando en particular en los denominados servicios intermediarios de la sociedad de la información. La importancia decisiva de estos servicios para el funcionamiento de la red ha llevado al legislador comunitario a establecer una serie de normas básicas relativas a la responsabilidad de quien presta tales servicios. El objeto del presente trabajo es el de realizar algunas consideraciones acerca de las reglas que en este punto se han dictado en la directiva sobre comercio electrónico¹, y acerca también de los esfuerzos del prelegislador interno para su transposición.

II. EL SISTEMA DE EXENCIONES DE RESPONSABILIDAD ESTABLECIDO EN LA DIRECTIVA DE COMERCIO ELECTRÓNICO.

Conviene señalar que, por una parte, el propósito de la directiva es el de evitar que las divergencias entre los derechos internos de cada Estado miembro en este campo obstaculicen el objetivo del mercado interior, en la medida en que estas divergencias pueden provocar distorsiones de la libre competencia y dificultar los servicios transfronterizos. Por otra parte, y de manera más concreta, la directiva quiere servir para establecer unas bases que faciliten a las partes implicadas llegar a acuerdos voluntarios cara a la elaboración de mecanismos rápidos y fiables para la retirada o bloqueo del acceso en relación a los contenidos ilícitos.

El hecho de que unos datos (mensaje) ilícitos, o que causen un daño, hayan circulado por la red gracias a la intervención de un determinado prestador de servicios intermediarios (mensajero) no implica que éste deba ser responsable de aquellos. En la medida en que la actuación del prestador de servicios se haya limitado a la realización de operaciones

¹ Directiva 2000/31/CE, de 8 de junio de 2000 (DOCE nº 178, de 17 de julio), del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Disponible en formato pdf en: http://www.europa.eu.int/comm/internal_market/en/media/elecomm/com31es.pdf

puramente técnicas, pasivas y automáticas, o en la medida en que observe determinados deberes de diligencia, la directiva establece que quedará exento de responsabilidad, con los requisitos y condiciones que a continuación examinaremos.

La aplicabilidad de las exenciones establecidas, que constituyen una especialidad respecto del régimen general de responsabilidad, dependerá del hecho de que realmente se cumplan los supuestos y las condiciones que para cada caso se señalan, de forma que habrá que atender a la verdadera naturaleza de los actos que estos operadores lleven a cabo y no sólo a la denominación que quieran dar a su actividad.

La directiva trata separadamente: a) la simple transmisión de datos y la prestación del servicio de acceso; b) el almacenamiento automático y provisional de datos denominado *caching*; y c) el alojamiento de datos o *hosting*. (Se trata de actividades *intermediarias* que llevan a cabo los llamados *prestadores de servicios intermediarios de la sociedad de la información*, los cuales, presumiblemente, además de dichas actuaciones realizan muchas otras distintas, que quedarán sujetas al régimen general de responsabilidad).

La directiva de comercio electrónico no establece propiamente una regulación general de la responsabilidad de los prestadores de servicios intermediarios. Lo que hace simplemente es fijar a favor de tales prestadores *unos ámbitos concretos de exención de responsabilidad*. Esto es, prohíbe que cuando hayan prestado un determinado servicio (cumpliendo una serie de requisitos subjetivos y/o objetivos) se les pueda imputar responsabilidades derivadas precisamente de haberlos prestado (con los límites que veremos).

Toda la actividad que se produce en el ciberespacio pasa necesariamente por uno o más de estos prestadores de servicios. Y desde la perspectiva del derecho de daños, esta simple consideración resulta capital para construir la relación obligatoria de reparación, tanto en lo que se refiere al nexo de causalidad como a las cuestiones de culpabilidad.

En cuanto al nexo causal hay que tener presente que, en efecto, cualquier daño concreto producido en o a través de la red habrá tenido como una de sus concausas necesarias (o *sine qua non*) la actuación de un prestador de servicios intermediarios, ya que, ciertamente, si realizamos el ejercicio de hipótesis consistente en eliminar mentalmente la actuación de este prestador llegamos a la conclusión de que el daño concreto verificado no se habría producido, ya que el elemento dañoso no habría podido hacerse presente ni circular en la red. Por tanto, la actuación de este operador habrá sido una de las causas del daño.

Si estimamos, como lo hace la llamada *teoría de la equivalencia de las condiciones*, que todos los factores causales concurrentes implican la responsabilidad de sus agentes, entonces el servicio llevado a cabo por el prestador intermediario habrá constituido un elemento suficiente como para imputarle el deber de resarcir. Ahora bien, una aplicación estricta de la teoría del valor equivalente de las condiciones conduciría, como es bien sabido, a imputaciones de responsabilidad exageradas, de muy difícil justificación. Hay infinidad de acciones y omisiones que, sin que su autor pueda preverlo y ni siquiera sospecharlo, pueden llegar a formar parte, incluso parte necesaria, de la conjunción de circunstancias causales que finalmente produce el daño.

Por ello, con frecuencia se ha entendido que para imputar responsabilidad no basta con que la actuación del agente haya sido un factor causal *sine qua non* en relación con la aparición del resultado dañoso. Será necesario, además, que el daño fuera *previsible*. Esto es, que el agente, en el momento de llevar a cabo su acción u omisión, pudiera prever (tuviera la posibilidad

razonable de prever) los resultados dañosos -considerados abstractamente- que pudieran llegar a derivarse de su actuación. (Unos daños, claro está, que la víctima no tenga obligación jurídica de soportar, ya que de otro modo ésta no podría exigir su resarcimiento). Con la citada exigencia jurisprudencial de la previsibilidad del nexo causal, el agente no tendrá que responder de los daños que superen los límites de lo que era razonable prever, a pesar que su actuación haya constituido uno de los elementos necesarios del conjunto de circunstancias causales, esto es, a pesar de existir relación de causalidad entre su acción/omisión y el daño. Este criterio, no bastante, parece todavía insuficiente para excluir imputaciones de responsabilidad excesivas. Ciertamente puede resultar fácilmente concebible que una determinada acción es de por sí susceptible de contribuir, incluso de forma necesaria, a la producción de un daño; pero puede muy bien ser que dicha contribución previsible sea meramente instrumental o incidental dentro de todo el conjunto de circunstancias causales.

Parece, por tanto, imprescindible, a los efectos de establecer satisfactoriamente la imputación del deber de resarcir, valorar la distinta relevancia de cada una de las acciones u omisiones que han contribuido a la aparición del daño. En este sentido, a veces se formula la distinción entre causas próximas, que comportarían responsabilidad, y causas remotas, que no implicarían el deber de reparar. Se ha dicho también que el agente sólo podrá ser considerado responsable cuando haya desplegado una acción u omisión que constituya causa *adecuada* para la producción del daño, entendiéndose por tal aquella acción u omisión que con gran probabilidad producirá un daño, sin necesidad de particulares alteraciones inesperadas de curso causal. De este modo, sólo quien ha puesto en marcha una causa adecuada deberá responder del daño, y no responderán del mismo los agentes de aquellas otras concausas, que, no obstante ser causas *sine qua non* en el caso concreto, no resultan abstractamente y *ex ante* adecuadas para generar responsabilidad en relación con este tipo de daños. Es así, pues, que no cualquier relación de causalidad es idónea para cubrir el requisito de nexo causal que nuestro sistema exige para imputar responsabilidad, ya que en cada caso habrá que valorar si la causa que se examina es lo adecuada o suficiente para basar esa imputación. (Huelga decir que aun siendo un nexo causal adecuado, la falta de otros requisitos, por ejemplo de orden subjetivo, pueden impedir también que finalmente se atribuya responsabilidad al agente).

Visto lo anterior, conviene advertir que, desde la perspectiva de un operador económico que lleva a cabo una actividad como la de los prestadores de servicios intermediarios de la sociedad de la información (una actividad que, recordémoslo, siempre resultará parte integrante del conjunto de circunstancias que confluyen en la causación de cualquier daño concreto en el ámbito de las comunicaciones electrónicas), resulta excesivamente desincentivadora desde el punto de vista empresarial la incertidumbre jurídica de un sistema que debe juzgar caso por caso si su intervención da lugar o no a responsabilidad.

Existen diversos modos de evitar esta incertidumbre. Uno de ellos es el de *que la ley fije una exención de carácter objetivo para determinadas actividades*. Es decir, que establezca previamente y con carácter general que ciertas actividades, perfectamente delimitadas, a pesar de haber formado parte del conjunto de causas necesarias para la producción de un daño, no puedan considerarse nunca (o por lo menos en relación con determinados tipos de daños) como un elemento causal apropiado, y deban considerarse por tanto inidóneas para cubrir el requisito de nexo causal que se requiere para imputar responsabilidad.

Y es esto exactamente -aunque sin expresarlo de este modo- lo que hace el legislador comunitario en relación a los servicios de mera transmisión de datos y a los de provisión de acceso a una red de comunicaciones, siempre que estos servicios se hayan ajustado verdaderamente a las características materiales que la propia directiva señala.

En cambio, en relación a los otros dos servicios mencionados (el almacenamiento en *caching* y el alojamiento de datos) se establecen, básicamente, *exenciones de carácter subjetivo*. La aplicabilidad de la exención depende aquí de si el agente, además de ajustarse a los requisitos objetivos, ha cubierto o no determinados requisitos de diligencia en la prestación del servicio. Si ha infringido alguno de los deberes de diligencia fijados no podrá beneficiarse de la exención, y por tanto (siempre que concurra el resto de requisitos exigibles, como es obvio), podrá llegar a ser obligado a resarcir los daños. Las actividades de *caching* y de *hosting*, por tanto, no son consideradas por la directiva como materialmente inidóneas en si mismas para satisfacer los requisitos de causalidad apropiada: la directiva no impide que pueda fundarse en ellas una imputación de responsabilidad cuando no se hayan cumplido los deberes de diligencia especificados.

La determinación legal precisa de la diligencia exigible es otra forma de otorgar un margen de seguridad a los operadores. En el sistema general subjetivista del artículo 1.902 del Código Civil, el requisito de la culpa o negligencia es imprescindible para imputar la responsabilidad al agente. Ahora bien, la tarea de dilucidar si éste ha sido o no suficientemente diligente permite un margen muy amplio de discreción judicial. La necesidad de conceder a determinados operadores una seguridad jurídica adecuada ha llevado al legislador comunitario a precisar cual es la diligencia exigible en la prestación de determinados servicios. Cubierta esta diligencia, se obliga a los Estados miembros a garantizar la irresponsabilidad del prestador.

Veamos a continuación de qué modo se fijan estas exenciones de responsabilidad.

1. La exención de responsabilidad del prestador de servicios en el caso de mera transmisión de datos (*mere conduit*) y de provisión de acceso.

De entre las distintas prestaciones características de los proveedores de servicio intermediarios de la sociedad de la información hay dos que son ejemplos paradigmáticos de actuaciones meramente instrumentales. Es el caso del servicio que consiste únicamente en transmitir, en una red de comunicaciones, datos que un tercero suministra y solicita que sean transmitidos; y también el del simple servicio de proporcionar acceso a una red de comunicaciones.

Conviene advertir para evitar posibles confusiones en la lectura de los preceptos de la directiva, que cuando se habla del servicio de transmisión de datos (tanto en el artículo 12 como en el 13) se utiliza la expresión “destinatario del servicio” para designar a la persona que encarga al prestador de servicios que transmita unos datos, y que es por tanto el cliente o “destinatario” de dicho servicio, y no debe confundirse con el destinatario de la transmisión, que lo será quien la recibe. Cuando se hace referencia al servicio de acceso, “destinatario del servicio” es la persona que lo pide, esto es, la que obtiene el acceso. Y en relación al alojamiento, de igual modo, el “destinatario del servicio” es quien solicita alojar los datos o contenidos.

El legislador comunitario ha decidido establecer una exención de responsabilidad de carácter objetivo que será aplicable siempre que los servicios mencionados reúnan los requisitos negativos consistentes en que el prestador de tales servicios:

- no haya originado él mismo la transmisión,
- ni tampoco haya seleccionado al destinatario (de la transmisión),
- ni tampoco haya seleccionado ni modificado los datos de la transmisión.

El primero de estos requisitos [la letra a) del artículo 12.1] puede sorprender a primera vista, pero parece claro que debe entenderse en el sentido de que el prestador de servicios no debe ni

ser el creador del contenido de la transmisión, ni tampoco debe ser él quien tome la iniciativa de realizar una concreta transmisión (esta decisión la toma el “destinatario” del servicio, que es quien suministra los datos y pide que se transmitan). Ciertamente el prestador *participa* en la operación de transmisión, hasta el punto de que precisamente está prestando el servicio de transmisión, pero lo hace a solicitud del destinatario de dicho servicio y en este sentido puede afirmarse que no la origina él².

El proveedor que presta el servicio de transmisión de datos, o el de facilitar el acceso -y por tanto la obtención de datos- en una red, y más concretamente en Internet, suele realizar una operación técnica que facilita la transmisión. En esta operación, que se produce automáticamente, lo que hace el proveedor es almacenar provisionalmente los datos que debe hacer llegar al destinatario final de la transmisión, simplemente a los efectos de poder realizar dicha transmisión (almacenamiento que es ya una copia o reproducción de datos y por tanto tiene implicaciones jurídicas, particularmente desde el punto de vista del derecho de reproducción de obras protegidas por la normativa de propiedad intelectual). Se trata, sin embargo, de un almacenamiento efímero, que dura sólo el tiempo razonablemente necesario para realizar la transmisión, y en el que el proveedor de servicios tiene una intervención puramente pasiva. La directiva ha querido dejar claro que la exención de responsabilidad abarca también las mencionadas operaciones técnicas y pasivas de almacenamiento automático, provisional y transitorio de los datos transmitidos, siempre que este almacenamiento sirva exclusivamente para ejecutar la transmisión a la red de comunicaciones, y que su duración no supere el tiempo razonablemente necesario para dicha transmisión³.

Ahora bien, la directiva limita el ámbito de la exclusión de responsabilidad advirtiendo que no afectará a la posibilidad de que los tribunales o autoridades administrativas, de acuerdo con los sistemas jurídicos de los Estados miembros, exijan a un prestador de servicios intermediarios que impida o ponga fin a una infracción (art. 12.3). Por tanto, cuando en un caso concreto el prestador de servicios reciba esta orden de un tribunal o de una autoridad administrativa, y la orden implique abstenerse de seguir prestando los servicios mencionados, si los continúa prestando ya no podrá hacer uso de la exención de responsabilidad.

2. La exención de responsabilidad en el *caching*.

El llamado *caching* es una herramienta esencial para reducir las congestiones en la red y la lentitud en la carga de las páginas *web*. Consiste en acercar los contenidos al usuario final. Cuando un proveedor de servicios de Internet detecta que sus clientes solicitan con frecuencia visitar determinadas páginas que se hallan alojadas en servidores geográficamente lejanos, el proveedor hace y conserva una copia de esas páginas en su propio servidor. De este modo, cuando otros clientes vuelvan a pedir ver la misma página no será preciso ir a buscar los datos al sitio de alojamiento original, sino que bastará con mostrarle la copia que el proveedor tiene en su memoria *cache*.

La directiva establece una exención de responsabilidad específica para el *caching* (que el texto castellano traduce por “memoria tampón”). El artículo 13 del texto comunitario

² De hecho, normalmente, la solicitud de transmisión que cursa el destinatario del servicio desde su ordenador (cliente) originará de forma automática que el mensaje sea transmitido por la red hacia su destino desde el ordenador (servidor) del prestador del servicio.

³ Es claro que esta descripción no cubre los servicios habituales de correo electrónico, en los que tanto los mensajes que el cliente envía como los que éste recibe (con los correspondientes documentos adjuntos) se almacenan durante meses en el *servidor* del prestador del servicio.

establece 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 podrá 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.

El prestador de servicios no será responsable del almacenamiento en *caching* siempre que, por supuesto, no modifique la información (art. 13.1.a); y siempre que cumpla cumulativamente con una serie de requisitos de diligencia, que son los siguientes:

- cumplir las condiciones de acceso a la información (art. 13.1.b). Con esto se quiere hacer referencia a las condiciones que tiene establecidas el propietario del sitio original para acceder a la información, y que el prestador de servicios que tiene la copia en *cache* debe hacer respetar.
- cumplir las normas relativas a la actualización de la información especificadas de manera ampliamente reconocida y utilizada por el sector (art. 13.1.c). No sería aceptable que las copias *cache* mostraran una información significativamente distinta a la que constara en el sitio original, y es por ello que el prestador debe preocuparse de actualizar la información almacenada, siguiendo las prácticas que al respecto son habituales y aceptadas en el sector.
- no interferir en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector con la finalidad de obtener datos sobre la utilización de la información (art. 13.1.d). El titular de la *web* original está interesado, por muchos motivos, en saber cómo, cuándo, quién, y sobre todo cuántas veces, se consulta su página. Habida cuenta de que muchas visitas no se hacen a la página original sino a la copia *cache*, el proveedor que tiene la copia ha de permitir que el titular de la información original pueda obtener esos datos mediante la tecnología existente al efecto.
- actuar con prontitud para retirar la información que haya almacenado, o hacer que sea imposible acceder a ella, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se hallaba inicialmente, o de que se ha imposibilitado el acceso a la misma, o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir el acceso a la misma (art. 13.1.d).

Ahora bien, de igual modo que en el primer grupo de casos, se establece también aquí que esta exención de responsabilidad no afectará a la posibilidad de que los tribunales o autoridades administrativas, de acuerdo con los sistemas jurídicos de los Estados miembros, exijan a un prestador de servicios intermediarios que impida o ponga fin a una infracción.

3. La exención de responsabilidad en el supuesto del servicio de alojamiento de datos.

El artículo 14 de la directiva formula y define los límites de la exención de responsabilidad para las actividades de *hosting* o alojamiento de datos, esto es, del servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio de forma que puedan ser consultados a través de la red. Es el caso, por ejemplo, del prestador de servicios que aloja en su servidor una determinada página *web*, a solicitud de una persona, física o jurídica, que desea tener esta página en la red. En estos supuestos se elevan

notablemente los requisitos subjetivos que deben concurrir en la actuación del prestador de servicios para que de ella no pueda derivarse responsabilidad.

Concretamente, para que el prestador pueda gozar de la exención se establece el requisito subjetivo negativo de falta de conocimiento efectivo de la ilicitud de la actividad o de la información que aloja. Y en particular, ante una acción de reclamación de daños y perjuicios, no haber tenido conocimiento de hechos o de circunstancias por las cuales se revele el carácter ilícito de la actividad o de la información. Este requisito negativo se complementa con la obligación de desplegar una actividad positiva tan pronto como el prestador de servicios tenga conocimiento de aquellos extremos; actividad que consiste en actuar con prontitud para retirar los datos, o bien hacer que el acceso a los mismos sea imposible.

Por otra parte, es preciso que exista una verdadera independencia entre el prestador del servicio de alojamiento y el destinatario que lo solicita. Si este último actúa bajo la autoridad o el control del prestador de servicios, la exención de responsabilidad no será aplicable.

De acuerdo con el artículo 14.3 de la directiva, esta exención 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 impedir la. Y tampoco afectará a la posibilidad de que los Estados miembros establezcan procedimientos que por los que se rija la retirada de los datos o el hecho impedir el acceso a los mismos.

4. El alcance de las exenciones.

Hemos visto hasta aquí cómo se han formulado en la directiva los supuestos de hecho a los que resultarán aplicables las exenciones de responsabilidad. Veamos ahora, sin embargo, cual es el alcance concreto de dichas excepciones.

En los casos de mera transmisión y en los de provisión de acceso, la exención que otorga la directiva consiste en que no se podrá considerar al prestador de este tipo de servicios “responsable de los datos transmitidos” (art. 12); en el caso del *caching*, en que no podrá considerársele “responsable del almacenamiento” descrito (art. 13); y en el caso del alojamiento, en que no se le pueda considerar “responsable de los datos almacenados” (art. 14).

A nuestro entender es claro que ninguna de estas formulaciones comporta una exención absoluta de responsabilidad en el sentido de garantizar al prestador del servicio que no será responsable *de ningún resultado dañoso que se haya derivado de su actuación*. No es muy difícil pensar en casos en los que el servicio prestado se habrá ajustado a la descripción y a los requisitos objetivos y subjetivos indicados en los artículos 12, 13 ó 14, y en que no obstante podremos exigir determinadas responsabilidades al prestador. Por ejemplo podremos exigirle responsabilidad contractual por la prestación defectuosa del servicio, con el correspondiente resarcimiento de los daños y perjuicios ocasionados. Ciertamente no será responsable *de los datos almacenados* en *hosting*, esto es, no deberá responder por ejemplo de los daños que se deriven del hecho de que estos datos sean ilícitos; pero sí deberá responder ante el destinatario del servicio si -por ejemplo- la forma en que hace accesibles en red aquellos datos no es la acordada contractualmente. También podremos exigirle responsabilidad extracontractual derivada de los daños que ocasione y que caigan fuera del ámbito de inmunidad que quiere ofrecer la exención. Así, el prestador del servicio de transmisión no será responsable *de los*

datos transmitidos; pero podrá serlo -por ejemplo- de los daños causados por haber utilizado en la transmisión un *software* defectuoso que ha ocasionado perjuicios a otras personas.

5. Las acciones de cesación y/o impedimento de una infracción.

El considerando número 45 de la directiva señala que las limitaciones de la responsabilidad de los prestadores de servicios intermediarios establecidas en la directiva *no afectan* a la posibilidad de ejercitar acciones de cesación de diverso tipo. Y que estas acciones de cesación pueden consistir en particular en “órdenes de los tribunales o de las autoridades administrativas por las que se exija poner fin a cualquier infracción o impedir que se cometa, incluso retirando la información ilícita o haciendo imposible el acceso a la ella”.

Este principio se reitera en cada uno de los supuestos de exención considerados advirtiendo que el precepto que recoge la exención 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 (cfr. arts. 12.3, 13.2 y 14.3 inciso primero). En el caso del alojamiento de datos se dispone además que tampoco se impide a los Estados miembros establecer procedimientos por los que se rija la retirada de datos o se impida el acceso a los mismos (art. 14.3).

De este modo, para lograr la exoneración, el prestador de servicios no sólo deberá cumplir a) los requisitos objetivos (naturaleza de la actividad); b) los subjetivos negativos (falta de conocimiento efectivo); y c) subjetivos positivos o de diligencia (actuación pronta a partir de haber tenido conocimiento de la ilicitud, con todos los problemas de indefinición que surgirán para determinar si se ha cubierto o no esta diligencia) previstos para cada supuesto; ya que puede tener que hacer frente además, a una acción de cesación, cosa que simplemente significa que, en relación a un caso determinado, se le exige *plus* de diligencia, consistente en realizar los actos oportunos para poner fin a cierta infracción o para impedirla. Si no observa esta diligencia adicional no podrá beneficiarse de la exención de responsabilidad en relación al servicio concreto al que se refiera la orden judicial o administrativa⁴.

Fijémonos, sin embargo, en el cariz que puede tener esta diligencia añadida. En todo caso responde a una orden comunicada al prestador por parte de un tribunal o de una autoridad administrativa. No basta, pues, con el hecho de que el prestador reciba un requerimiento o notificación procedente de un particular. (Atención: no basta *para quedar obligado a desplegar esta diligencia adicional*, pero puede muy bien ser que el requerimiento privado se considere suficiente para que el prestador deba llevar a cabo las acciones que le exige la propia directiva para los casos en que llega al conocimiento del mismo el carácter ilícito de la información o de la actividad).

Por lo demás, la orden del tribunal o de la autoridad administrativa puede exigir al prestador que ponga fin a una infracción, o bien *que la impida*. Impedir una infracción supone poner los medios adecuados para evitar que llegue a producirse un ilícito que aún no se ha producido. Y esto, se mire como se mire, significa (o por lo menos puede significar) *control previo*. Control previo ajustado al sistema jurídico del Estado miembro, pero control previo al fin y al cabo.

⁴ Sabemos que esta diligencia adicional sólo se le podrá exigir *de conformidad con los sistemas jurídicos de los Estados miembros*. Pero surge inmediatamente el problema de la competencia de jurisdicción y de ley aplicable (que no abordaremos aquí): ¿deberá ser necesariamente de conformidad con el sistema jurídico del Estado miembro en que el prestador se halle establecido?, ¿será preciso que la orden la emita un tribunal o una autoridad administrativa del Estado miembro de establecimiento del prestador?

Lo cual, si la orden dictada no es suficientemente específica y determinada, traslada al prestador de servicios el difícil deber de discriminar qué es lo que debe permitir y qué lo que debe impedir al efecto de evitar la consumación de la infracción. Con el riesgo de equivocarse tanto por exceso como por defecto.

Estas posibles obligaciones de control previo no son, sin embargo, obligaciones establecidas de forma general en el ordenamiento, sino que nacen de la concreta orden judicial o administrativa dictada y notificada al prestador de servicios. Ahora bien, la ley del Estado miembro también puede establecer, para cualquier prestador de servicios, deberes de control previo, si bien sólo en relación a casos específicos. Y asimismo (en el caso de los prestadores de servicios de alojamiento) deberes de detección y prevención de determinados tipos de actividades ilegales. Veámoslo con más detalle en el apartado siguiente.

6. Obligaciones de supervisión y de comunicación.

Hemos visto más arriba que *en los casos de servicios de alojamiento de datos* la exención de responsabilidad del prestador del servicio se mueve entre dos extremos: o bien el prestador no tiene conocimiento del carácter ilícito de la actividad o de la información, quedando en tal caso cubierto por la exención; o bien tan pronto como tiene conocimiento de la ilicitud desarrolla una actividad diligente de retirada de los datos o de bloqueo del acceso, con lo que resultará también cubierto por la exención.

Ahora bien: entre el conocimiento y el desconocimiento existe una gran zona gris, que es la situación en la que se halla el prestador que ignora “culpablemente”. La pregunta es si podemos considerar que el prestador de servicios queda cubierto por la exención en los casos en que ciertamente no se le puede tachar de negligente en los deberes de retirada o bloqueo de los datos puesto que precisamente por ignorar el carácter ilícito de los mismos tales deberes no le eran exigibles. Esta ignorancia, cabe plantear, puede a veces parecer precisamente una falta de diligencia en el sentido de no haber tomado ninguna iniciativa para conocer si la información alojada era o no ilícita. Dicho de otro modo: la cuestión es si el régimen que establece la directiva deja espacio para que los Estados miembros impongan al prestador, como deber de diligencia, la obligación de inspeccionar o examinar los datos que aloja al efecto de conocer si la actividad o la información es o no ilícita.

En la respuesta a este punto es preciso distinguir entre obligaciones de carácter general y obligaciones específicas. De acuerdo con el artículo 15.1 de la directiva, los Estados miembros no pueden imponer a los prestadores de servicios una obligación *general*, ya sea de supervisar los datos que transmitan o almacenen, ya sea de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas en relación a los servicios de alojamiento, y *también* en los de transmisión de datos, de provisión de acceso a la red y de *caching*⁵. Hay que destacar, no obstante, que la directiva no excluye la posibilidad de

⁵ Este artículo de la directiva plantea el problema de saber qué relevancia tiene, desde el punto de vista de la responsabilidad, el hecho de que el prestador de servicios tenga conocimiento de la ilicitud en los supuestos de servicios distintos del alojamiento, es decir, en los de mera transmisión de datos, de provisión de acceso a la red y de almacenamiento en *caching*.

Si el prestador no tiene una obligación *general* de supervisar la licitud o ilicitud de los datos (ya sabemos que en efecto no puede tenerla, ya que la directiva prohíbe a los Estados imponerla), es claro que no se le podrá retirar la exención de responsabilidad argumentando que no ha desplegado la diligencia exigida para descubrir que efectivamente la información o la actividad era ilícita. Esto (prohibir el establecimiento de deberes generales de supervisión) tiene sentido respecto de la actividad de alojamiento, porque en tal caso, el hecho de tener o no conocimiento de esta ilicitud es un extremo esencial para la aplicabilidad de la exención. De hecho, a la vista del

establecer obligaciones de supervisión *que no sean de carácter general* (por ejemplo obligaciones de supervisión del contenido procedente de algún sitio determinado de la red).

Por otra parte, la directiva no pone ningún impedimento a los Estados miembros para establecer obligaciones de comunicación. Concretamente prevé la posibilidad de que los Estados exijan a los prestadores de servicios de la sociedad de la información que comuniquen con prontitud a las autoridades los datos presuntamente ilícitos o las actividades ilícitas llevadas a cabo por los destinatarios de sus servicios; o también que les impongan la obligación de comunicar a las autoridades, a solicitud de éstas, información que permita identificar a los destinatarios de sus servicios con los que hayan celebrado acuerdos de almacenamiento (cfr. art. 15.2).

Son muchos, pues, los aspectos en los que el legislador comunitario deja un amplio margen de decisión a los Estados. No conocemos todavía qué opciones tomará finalmente nuestro legislador a la hora de transponer la directiva. Pero tenemos ya algunas pistas: las contenidas en el anteproyecto de 18 de enero de 2001. Y será oportuno examinarlas seguidamente.

III. LA FUTURA TRANSPOSICIÓN AL DERECHO INTERNO DEL RÉGIMEN DE EXENCIONES DE RESPONSABILIDAD SEGÚN EL ANTEPROYECTO DE 18 DE ENERO DE 2001.

El Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico se encarga de realizar la transposición al derecho interno de la directiva de comercio electrónico, y a la vez transpone parcialmente la directiva 98/27/CE, de 19 de mayo de 1998, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, a los efectos de regular este tipo de acciones en relación a los actos de los prestadores de servicios. Como es obvio todavía es un texto provisional, pero ha pasado ya varias fases de redacción. La versión actual, y que aquí examinaremos, es la de 18 de enero de 2001⁶.

artículo 15 el razonamiento es llano: de una parte el prestador que conoce debe actuar retirando los datos o bloqueando el acceso, pero de otra parte no se le puede obligar a que se dedique sistemáticamente a averiguar si los datos son o no ilícitos: el legislador entiende que esto último le supondría una carga excesiva.

No obstante, en el caso de las actividades de mera transmisión, de simple provisión de acceso, y de almacenamiento en *caching* (arts. 12 y 13) parece claro que la exoneración de responsabilidad es aplicable con independencia de si el prestador tiene o no conocimiento de la ilicitud de los datos. Y por tanto el incumplimiento de una eventual obligación general de supervisión no debería ser relevante desde el punto de vista de la responsabilidad, razón por la cual tampoco parece necesario, *desde la perspectiva estricta del establecimiento del régimen de exenciones de la responsabilidad*, que la directiva prohíba a los Estados el establecimiento de tal obligación en relación a estos servicios.

Quizá la *ratio* del artículo 15 en este punto deba buscarse en la voluntad del legislador de dejar bien claro que no se podrá reprochar a los prestadores de los servicios contemplados en los artículos 12 y 13 haber incurrido en negligencia si no supervisan la licitud de los datos que transmiten o guardan. O quizá sea una manera de establecer indirectamente una limitación al alcance de la exención: la exención no sería aplicable cuando existiendo una obligación limitada y específica de supervisión (por ejemplo respecto de un *website* determinado) el prestador ha llevado a cabo el servicio a pesar de la ilicitud de la información (ilicitud conocida o bien ignorada precisamente por haber descuidado la obligación impuesta de supervisar). Esto, sin embargo, sería contrario a la interpretación que parece más clara, y que es la ya expuesta: la exención en estos servicios es independiente del hecho de que el prestador conozca o no la ilicitud (al margen siempre, claro está, de los casos en que haya recibido una orden de un tribunal o autoridad competente exigiéndole una determinada actuación).

⁶ Disponible en: http://www.setsi.mcvt.es/novedad/consulta_anteproyecto.htm

1. Las normas generales sobre responsabilidad.

El anteproyecto inicia esta materia con dos artículos (13 y 14), francamente criticables por desenfocados. El artículo 13 empieza declarando que “los prestadores de servicios de la sociedad de la información [todos: no sólo los de servicios intermediarios] están sometidos a las normas generales del ordenamiento jurídico sobre responsabilidad civil, penal y administrativa, con las particularidades que deriven de la aplicación de la legislación sobre derechos de los consumidores y usuarios [sic]”. Declaración perfectamente superflua, tras la cual señala que no obstante “asumirán una responsabilidad específica [sic] por los contenidos transmitidos por la red, que se regula por las normas establecidas en esta sección”. Y sin embargo esta declaración no se corresponde en absoluto con el contenido de dicha sección, que no hace otra cosa que recoger simplemente un conjunto de supuestos de exención de responsabilidad, y referidos únicamente a los prestadores de servicios intermediarios.

El siguiente artículo, 14, bajo la rúbrica de “[r]egla general y limitaciones de responsabilidad” dispone que “[c]on carácter general [sic (!)], los prestadores de servicios de la sociedad de la información sólo serán responsables por los contenidos que ellos mismos elaboren o que se hayan elaborado por cuenta suya” y que “[n]o serán responsables por el ejercicio de las actividades de intermediación que impliquen la transmisión, copia, almacenamiento o localización de contenidos ajenos, si respetan las normas recogidas en los artículos que siguen”. Esta bonita declaración, tan ambigua como innecesaria, podría a lo más aparecer en una exposición de motivos. Incluirla como texto de un precepto de la futura ley parece un evidente despropósito de técnica legislativa.

Dejemos de lado, no obstante, este mal inicio y vayamos a ver con detalle la regulación de las exenciones de responsabilidad de los diferentes servicios intermediarios que el anteproyecto establece a continuación (arts. 15 y ss.).

2. Las exenciones de responsabilidad.

Siguiendo la misma sistemática que la directiva, el anteproyecto distingue tres supuestos de prestaciones: a) las de transmisión de datos y de provisión de acceso; b) las de almacenamiento en *caching*; y c) las de alojamiento de datos. Añade además otro grupo que la directiva menciona pero no disciplina: los servicios de facilitar *hyperlinks*, directorios y/o motores de búsqueda de contenidos.

2.1. Transmisión de datos o provisión de acceso a red.

El anteproyecto (art. 15) define estos servicios de manera prácticamente idéntica a como lo hace la directiva: “un servicio de la sociedad de la información que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta”.

Desde el punto de vista de los sujetos, en lugar de hablar de prestadores de servicios intermediarios habla de operadores de redes y de proveedores de acceso; terminología que parece bastante correcta para este tipo de servicios, siempre que no se interprete en un sentido reduccionista: a los efectos de este artículo, será “proveedor de acceso” cualquier prestador que proporcione este servicio, aunque preste además otros y sea también, por ejemplo, prestador de servicios de alojamiento.

La parte dispositiva del precepto establece directamente que “no serán responsables por la información transmitida”, y que “[s]in embargo, esa responsabilidad sí podrá exigirse cuando ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a sus destinatarios”. Dispone también que no se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos que tiene lugar durante su transmisión (añadido de carácter técnico que no aparece en la directiva). Y que las actividades de transmisión y provisión de acceso mencionadas incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario (declaración prácticamente idéntica a la de la norma comunitaria).

Es preciso que nos detengamos brevemente en esta expresión ya transcrita: “(...) *esa responsabilidad sí podrá exigirse cuando (...)*”. En este precepto, igual que en la directiva, se determinan perfectamente unos supuestos en los que el prestador del servicio queda exento de responsabilidad. Pero *de ninguna manera se fijan aquí, ni tampoco en la directiva, unos requisitos necesarios específicos para que se le pueda imputar responsabilidad*, a pesar de que la redacción del precepto pueda dar a primera vista tal impresión. Dicho de otro modo: si el prestador del servicio cumple los requisitos de la exención quedará exento; y si no los cumple... entonces ya veremos si finalmente se le puede imputar o no responsabilidad. Éste último resultado jurídico necesita de la conjunción de muchos otros elementos, requisitos, valoraciones, inferencias y en definitiva arbitrio judicial; es decir, será un supuesto más al que habrá que aplicar las normas generales de responsabilidad civil y que simplemente no podrá beneficiarse de una exención legal porque no ha cubierto los requisitos exigidos a tal fin.

2.3. Almacenamiento en *caching*.

En lo que se refiere al *caching*, el anteproyecto dispone (art. 16) que “[l]os prestadores de un servicio de la sociedad de la información que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, *no serán responsables por la reproducción temporal de esos datos*, si (...)” cumplen determinados requisitos.

Tales requisitos, con pequeñas variaciones, son los mismos que fija la directiva: los de no modificar; cumplir las condiciones de acceso; actualizar la información; no interferir en la obtención de datos sobre la utilización de la información; y retirar o imposibilitar el acceso a la información en cuanto tenga conocimiento de que ha sido retirada del lugar original, o de que se ha impedido el acceso a la misma, o que un tribunal o autoridad ha ordenado su retirado o que se impida el acceso a ella.

2.3. Alojamiento o *hosting*.

En relación a los servicios de alojamiento de datos, el anteproyecto (art. 17) recoge con pocas diferencias la misma exención que establece la directiva: quien preste dicho servicio no será responsable de la información almacenada a petición del destinatario si no tiene conocimiento efectivo de la ilicitud de la actividad o de la información. En caso de tener conocimiento deberá actuar diligentemente para retirar los datos o hacer imposible el acceso a ellos.

La redacción se aparta un poco de la directiva en cuanto a la fijación, por ejemplo, del requisito de no conocer. El anteproyecto exige a los prestadores que “no tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que puede lesionar bienes o derechos de un tercero susceptibles de indemnización”. No hace, por tanto, la distinción que sí hace la directiva entre responsabilidad en general y responsabilidad exigida en una acción de resarcimiento de daños y perjuicios, donde basta con un conocimiento indirecto o indiciario para perder la exención de responsabilidad.

Al igual que en la directiva, se hace referencia tanto a información como a actividad ilícita. La redacción del anteproyecto resulta aquí algo más precisa en el sentido de que deja claro que se trata de la ilicitud de la actividad del destinatario del servicio (cosa que no dice expresamente la directiva).

Reitera también el anteproyecto el requisito de independencia del prestador respecto del destinatario del servicio: no se eximirá de responsabilidad si este destinatario actúa bajo su dirección, autoridad o control. Y se recuerda también la posibilidad de que la autoridad competente ordene al prestador que retire los datos o que imposibilite el acceso a los mismos. Y que si la retirada o bloqueo de datos puede afectar a derechos de intimidad o de libertad de expresión habrá que respetar las normas establecidas para su protección.

2.4. Hiperenlaces, directorios y motores de búsqueda.

La directiva de comercio electrónico no trata directamente de la responsabilidad que puede derivarse del hecho de presentar *links* (enlaces directos a otro lugar de la red mediante hipertexto) o de los instrumentos o motores de búsqueda de contenidos en la red. Pero es esta una cuestión que el legislador comunitario tiene muy presente, hasta el punto de que en el proceso de revisión de la directiva, previsto en su artículo 21, se exige que el informe correspondiente analice “especialmente la necesidad de presentar propuestas relativas a la responsabilidad de los proveedores de hipervínculos y servicios de instrumentos de localización”.

El anteproyecto establece que “[l]os prestadores de un servicios de la sociedad de la información que faciliten enlaces a otros contenidos en la red o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por dirigir a los destinatarios de los servicios a contenidos ilícitos, siempre que:

- no tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que puede lesionar bienes o derechos de un tercero susceptibles de indemnización, o
- si lo tienen, supriman o inutilicen el enlace.”

El artículo añade que “[e]n lo demás, será de aplicación lo que se dispone en el artículo anterior”, es decir, el régimen ya expuesto de la exención de responsabilidad para los servicios de alojamiento de datos.

Ahora bien: ¿cuál es la extensión material de la exoneración de responsabilidad que se concede? Lo que nos dice este precepto es que el prestador (si cumple las dos condiciones expresadas) no será responsable *por dirigir a los destinatarios de los servicios a contenidos ilícitos*. Desde el punto de vista del derecho de daños parece que esta exención tan sólo contempla los daños que puede sufrir el usuario del servicio que activa el *link* y accede a un

contenido que es de tal manera ilícito que el hecho de acceder a él le provoca ya un perjuicio. Quizá ha ido a un sitio en el que ha sufrido una ofensa o una injuria, o bien a un lugar de comercio electrónico donde ha sido estafado... Se presupone que el problema es el carácter ilícito del contenido o actividad hacia donde el *link* nos encamina. Con ello se dejan fuera de la exención los casos en los que el contenido del sitio de destino es lícito, y la ilicitud está más bien en el propio *link*. Así, por ejemplo, cuando mediante el *link* resultan infringidos los derechos de propiedad intelectual del titular de la página a la que el enlace nos lleva, haciendo uso de una parte sustancial de una base de datos ubicada en al página de destino a través de “enlaces profundos”: aquellos que nos conducen directamente a elementos específicos del *website* de destino, saltándose la visualización de la página inicial en la que aparece la publicidad, o incluso aparentando, mediante técnicas de *framing*, que estos contenidos pertenecen a la página que hemos visitado en primer lugar.

3. Límites y obligaciones en la prestación de servicios

Aprovechando el margen de discreción que la norma comunitaria permite a los Estados miembros para establecer deberes específicos, el anteproyecto prevé unas restricciones generales a la libre prestación de servicios de la sociedad de la información y, además, una serie de obligaciones concretamente dirigidas a los prestadores.

3.1. Restricciones a la libre prestación de servicios.

El artículo 9 del anteproyecto, bajo la rúbrica de “[r]estricciones a la libre prestación de servicios por atentar contra principios fundamentales de la convivencia social”, dispone que en los supuestos de servicios de la sociedad de la información que atenten o puedan atentar gravemente contra los principios que a continuación enumeraremos, las autoridades competentes para la protección de estos principios podrán adoptar las medidas necesarias para retirar los datos que los vulneren o impedir el acceso a los mismos. Estos principios son: el orden público, en particular, la investigación penal, la seguridad pública y la defensa nacional; la protección de la salud pública y de los consumidores o usuarios, incluso cuando actúen como inversores en el ámbito del mercado de valores; el respeto a la dignidad humana y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad o cualquier otra circunstancia personal o social; y la protección de la infancia y la juventud.

En la adopción y cumplimiento de estas medidas restrictivas habrá que respetar -señala el mismo precepto- los procedimientos previstos en el ordenamiento para proteger los derechos a la intimidad personal y familiar y a la libertad de expresión, cuando estos derechos resulten afectados. Además, se exige que las medidas sean objetivas, proporcionadas y no discriminatorias. y se deberán adoptar de conformidad con los procedimientos previstos en la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien de acuerdo con la legislación procesal que corresponda (art. 9.2).

3.2. Obligaciones de comunicación a las autoridades.

Hemos visto más arriba cómo el artículo 15 de la directiva de una parte prohíbe a los Estados miembros establecer obligaciones generales de supervisión y de búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, pero de otra parte permite establecer

obligaciones de comunicación a las autoridades, ya sea de presuntos datos o actividades ilícitas de los destinatarios de sus servicios, ya sea de información para identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento.

Siguiendo este margen que concede la directiva, y haciéndolo extensivo a todos los prestadores de servicios de la sociedad de la información (y no sólo a los de servicios intermediarios) que se hallen establecidos en España, el anteproyecto establece -en relación con los contenidos- las obligaciones de comunicación siguientes (art.12.1):

- comunicar a las autoridades judiciales o administrativas competentes, en cuanto tengan conocimiento de ello, la actividad presuntamente ilícita realizada por el destinatario del servicio.
- comunicar a las autoridades judiciales o administrativas competentes, a solicitud de éstas, la información que les permita identificar a los destinatarios de los servicios.

3.3. Obligaciones de supervisión en casos específicos.

Hemos destacado también que la prohibición de establecer obligaciones generales de supervisión del artículo 15 de la directiva no es obstáculo para imponer obligaciones de supervisión en casos específicos (cfr. considerando 45). Pues bien, el anteproyecto hace uso de esta posibilidad estableciendo que la autoridad judicial competente podrá requerir a cualquier prestador de servicios que supervise, o que conserve, todos los datos relativos a un determinado sitio de Internet durante un período máximo de seis meses y que las ponga a su disposición (art. 12.d).

No se dice nada más, pero, de acuerdo con las normas generales, parece claro que cuando, fruto de esta supervisión, el prestador de servicios tenga conocimiento de datos o actividades ilícitas deberá desplegar toda la diligencia expresada en los artículos 13 y 14 de la directiva para poder disfrutar de la exención de responsabilidad. En un intento de contabilizar estas obligaciones de supervisión selectiva con los requerimientos empresariales de la actividad del prestador de servicios, el anteproyecto le permite generosamente hacer esta supervisión o conservación de datos de la forma en que, siendo eficaz para el objeto que se persigue, resulte menos gravosa para el prestador de servicios.

3.4. Obligación de poner fin a una infracción o de impedirla.

Por último, el anteproyecto aprovecha también el hecho de que la directiva no impide 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, ni tampoco prohíbe que se establezcan procedimientos que rijan la retirada de datos o impedir el acceso. Y el anteproyecto usa de tal libertad fijando la obligación para todos los prestadores de servicios establecidos en España de “suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio de la sociedad de la información para poner fin a una infracción o impedirla cuando así se lo solicite una autoridad judicial o administrativa competente” (art. 12.c). Ya hemos tenido ocasión de exponer el sentido de que la directiva permita al legislador nacional estas posibilidades: el prestador no se podrá refugiar en la exención de responsabilidad para incumplir la orden de poner fin a la infracción o de impedirla.