10.18800/themis.202101.004

LA RETIRADA DE CONTENIDOS ILÍCITOS POR LOS PRESTADORES DE SERVICIOS EN LÍNEA

THE REMOVAL OF ILLEGAL CONTENT BY ONLINE SERVICE PROVIDERS

Lidia Moreno Blesa[*]
Universidad Complutense de Madrid

The irruption of the internet in a globalized world brings great advantages in the commercial and business sector. However, this new reality also has a strong social impact within the sphere of people's privacy, especially when it comes to social networks

This article explores the Judgement of Eva Glawischnig-Piesczek against Facebook Ireland Limited of the Court of Justice of the European Union case, in order to identify the extent to which online service providers are liable for illegal content that is shared on their websites. To accomplish this, the author debates if Facebook is a data hosting service provider to which the European Union regulations can be applied and what liability regime would be applicable to it for the broadcast of illegal content within their website. After that, she reviews the international judicial competence and the applicable law in the face of the violation of personal rights due to the dissemination of these contents. Finally, she reviews the territorial scope that an obligation to remove this type of content imposes.

Keywords: Internet; social media; Facebook; data hosting service providers; removal of illegal content.

La irrupción de internet en un mundo globalizado trae consigo grandes ventajas en el sector comercial y empresarial. No obstante, esta nueva realidad tiene también una fuerte repercusión social dentro del ámbito de la privacidad de las personas, en especial cuando se trata de redes sociales.

El análisis del presente artículo se enmarca en el caso Eva Glawischnig-Piesczek contra Facebook Ireland Limited del Tribunal de Justicia de la Unión Europea, con el fin de identificar hasta dónde llega la responsabilidad de los prestadores de servicios en línea por los contenidos ilícitos que se viertan en los sitios web que estos gestionan. En esta línea, la autora, define si Facebook es un prestador de servicio de alojamiento de datos al cual se le pueden aplicar las normas de la Unión Europea y qué régimen de responsabilidad es aplicable a estos servicios por la emisión de contenidos ilícitos dentro de sus portales. Después, revisa la competencia judicial internacional y el Derecho aplicable ante la vulneración de derechos de la personalidad a causa de la difusión de estos contenidos. Finalmente, repasa el alcance territorial que impone una obligación de retirada de este tipo de contenidos.

Palabras clave: Internet; redes sociales; Facebook; prestadores de servicios de alojamiento de datos; retirada de contenidos ilícitos.

[*] Abogada. Doctora en Derecho por la Universidad Complutense de Madrid. Ex profesora de Derecho Internacional Privado en la Universidad Europea de Madrid desde 1998 hasta 2018. Ex directora de tal Departamento desde 2004 hasta 2010. Profesora Ayudante Doctora de Derecho Internacional Privado de la Universidad Complutense de Madrid (Madrid, España). Acreditada como Profesora Contratada Doctora por la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid. Contacto: lidimore@ucm.es.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 5 de enero de 2021, y aceptado por el mismo el 21 de marzo de 2021.

I. INTRODUCCIÓN

En un mundo globalizado como el actual, en donde –en algunos casos– se han reducido y –en otros– se han eliminado los obstáculos a la libre circulación de mercancías, servicios y capitales, la irrupción de internet ha supuesto la desaparición de fronteras. La principal externalidad positiva que se deriva de lo anterior está relacionada con los beneficios que comporta para la rapidez de las transacciones comerciales. Se trata de una realidad que genera nuevas expectativas para el desarrollo de los negocios internacionales, así como también ventajas para los participantes en este entorno digital (Palao Moreno, 2017, p. 270). Incluso la Organización Mundial del Comercio tiene un programa de trabajo sobre el comercio electrónico, el cual fue adoptado en septiembre de 1998 y que, aunque solo a los efectos del programa de trabajo, incluye una definición de comercio electrónico: producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos (Organización Mundial del Comercio, 1998).

El avance experimentado en las telecomunicaciones ha tenido un gran impacto en el mundo empresarial y, consecuentemente, también una fuerte repercusión social incluso en el ámbito de la privacidad con los límites a la intimidad, lo que exige un tratamiento jurídico especializado. El mundo tecnológico se abre hacia el exterior y presenta, por ende, un carácter ubicuo, con la consecuencia de no tener límites aparentes (Davara Rodríguez, 2005, p. 25). Esta ausencia de márgenes definidos plantea serias dudas en cuanto al respeto de los derechos básicos de los individuos, de tal forma que, en un escenario diáfano como es internet, será muy complicado o prácticamente imposible evitar que la convivencia pacífica entre los sujetos se vea comprometida.

Internet ha supuesto una transformación sin precedentes en prácticamente todos los campos que se nos ocurran, hasta tal punto que su presencia ha desatado la denominada Tercera Revolución Industrial (Ortego Ruiz, 2020, p. 21). En efecto, internet se considera un elemento estructural de la 'sociedad de la información' desde el momento en que facilita los más variados servicios electrónicos interactivos y la comunicación de todo tipo de informaciones como texto, imágenes, sonido, video, entre otros. Su principal característica ha sido la capacidad de distribuir información y conocimiento globalmente y a gran velocidad (Barrio Andrés, 2017, p. 33). No es de extrañar que su inusitado éxito se deba a su capacidad de difusión por todo el mundo y, por ende, a su cualidad de ser un sistema de comunicaciones de carácter universal. Por lo tanto, es su enorme potencial para distribuir información y llegar a cualquier lugar, lo cual otorga al ciberespacio un estatus especial y único, diferente de todo lo demás, ya que permite la interacción entre personas físicas y jurídicas de todo el planeta.

El espacio donde se llevan a cabo los intercambios electrónicos se configura como una dimensión paralela a la real, donde los comportamientos se producen de manera virtual. Pues bien, son los comportamientos de las redes sociales y, en particular, los de Facebook, los que van a centrar nuestra atención. El motivo se encuentra en la sentencia del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) del 3 de octubre de 2019 en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18), por cuanto revisten especial interés las cuestiones planteadas en este caso, de cara a concretar hasta dónde llega la responsabilidad de los prestadores de servicios en línea por los contenidos ilícitos que se viertan en los sitios web que ellos gestionan. En concreto, el asunto en cuestión tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 del Tratado de Funcionamiento de la Unión Europea, por el Oberster Gerichtshof (Tribunal Supremo de lo Civil y Penal de Austria), mediante resolución de 25 de octubre de 2017, recibida en el TJUE el 10 de enero de 2018, en el procedimiento entre Eva Glawischnig-Piesczek y Facebook Ireland Limited.

En síntesis, el litigio del que trae causa la sentencia mencionada surgió de una petición a Facebook Ireland Limited para que procediera a la retirada de un comentario humillante que se había compartido en dicha red social. La información controvertida hacía referencia a la señora Glawischnig-Piesczek, en tanto actora en el procedimiento principal, y había sido incluida por un usuario del sitio web en cuestión. La perjudicada tomó cartas en el asunto e inició actuaciones judiciales en Austria, país en el que desarrollaba su actividad política objeto de la afirmación ofensiva, con el fin de conseguir que se eliminase totalmente cualquier contenido que menoscabara su reputación. El Tribunal austríaco que estaba conociendo del asunto ordenó, mediante auto de medidas cautelares, que Facebook Ireland dejara de mostrar inmediatamente y hasta el cierre definitivo del procedimiento relativo a la acción de cesación, las declaraciones contrarias al honor de la demandante. No obstante ello, la existencia de normativa en la Unión Europea sobre las obligaciones de los prestadores de servicios de alojamiento de datos que gestionan redes sociales planteó algunas dudas en relación con el alcance que habría de darse a una obligación de este tipo.

Al respecto, el Tribunal Supremo de lo Civil y Penal de Austria planteó al TJUE una serie de cuestiones

prejudiciales relativas a si las obligaciones impuestas al proveedor de la red social de retirar el contenido inicialmente publicado por el correspondiente usuario y declarado ilícito, se extendían también a otros contenidos ilícitos o similares. Además, propuso si esa obligación de retirada podía ir referida a todo el mundo o solo al Estado miembro de que se trata y también cuestionó si la retirada de esos otros datos podía adoptarse solo con respecto al contenido del usuario en cuestión (De Miguel Asensio, 2019). Para poder dar respuesta a las dudas que se acaban de esgrimir, se tendrán en cuenta varios aspectos que inciden de lleno en la materia controvertida.

En primer lugar, se despejará la incógnita de si Facebook, en tanto red social, es un prestador de servicios de alojamiento de datos al que pueden aplicársele las normas de la Unión Europea, las cuales regulan las obligaciones que recaen sobre este tipo de intermediarios. A continuación, se concretará el régimen de la responsabilidad por contenidos ilícitos que asumen los prestadores de servicios de alojamiento de datos y, por ende, si Facebook lo fuera, el que se les atribuye a las redes sociales. Unido a lo anterior, se ofrecerán algunos ejemplos sobre la responsabilidad de los prestadores de servicios, basados en los pronunciamientos jurisprudenciales. Después, serán objeto de atención tanto la competencia judicial internacional por vulneración de derechos de la personalidad como el Derecho aplicable. Al respecto, hay que tener en cuenta que el carácter ubicuo de los contenidos puestos en línea a través de internet exigirá concretar qué jurisdicción es la mejor situada para pronunciarse sobre la eliminación de toda la información ilícita o de los datos que correspondan, así como determinar la ley con la que se resolverá el fondo del asunto, ya bien sea una sola o varias. También se prestará atención al alcance territorial de un requerimiento judicial que impone una obligación de retirada. Los contenidos en internet no entienden de fronteras y se difunden universalmente, lo que exigirá precisar hasta dónde debe llegar la eliminación de los contenidos publicados en línea. Finalmente, se culminará con unas conclusiones que evidencien los comportamientos que deben seguir las redes sociales cuando de la supresión de información ilícita se trate.

II. ¿LAS REDES SOCIALES SON PRESTADORES DE SERVICIOS DE ALOJAMIENTO DE DATOS?

Para el desarrollo del comercio electrónico en redes abiertas resulta clave la figura de los prestadores de servicios de internet. Estos últimos son aquellos que facilitan el acceso a la Red y proporcionan los servicios necesarios para que las diversas aplicaciones de internet puedan ser utilizadas, incluyendo los servicios de alojamiento de datos, entre otros (De Miguel Asensio, 2020a, p. 586).

En la actualidad, los sujetos intervinientes en la prestación de servicios de la sociedad de la información constituyen un grupo muy heterogéneo que realiza diversas funciones (Barrio Andrés, 2017, pp. 325-327). Por un lado, encontramos a los proveedores que suministran acceso a internet que engloban a los operadores de telecomunicaciones, como por ejemplo a Telefónica, además de incluir a las compañías de telefonía móvil. También hay que insertar en este grupo a los operadores de cable y fibra óptica, a los proveedores de acceso a internet y, por último, a los operadores de redes wifi. Por otro lado, están los sujetos que proporcionan servicios en línea para permitir el almacenamiento de contenidos, incluyendo el alojamiento de páginas web, pero que también facilitan plataformas para los contenidos generados por los propios usuarios, tanto con un fin comercial o social. De todos ellos, son estos últimos los que nos interesan y que hacen referencia a las redes sociales que permiten la interacción de los usuarios, como por ejemplo Facebook.

Además de los anteriores, otro grupo de sujetos favorecen la navegación en la web mediante la indexación del contenido disponible en la red, permitiendo así una localización más accesible. Este es el caso de los motores de búsqueda, los agregadores (que agrupan enlaces relevantes clasificados por diversos temas) y todos los sitios web que proporcionan enlaces hacia contenidos de terceros.

También deben citarse los proveedores de economía compartida. Muchas transacciones físicas (reservas de hotel o reservas de taxi, por ejemplo) se realizan a través de una comunicación a distancia entre las partes. Lo que realizan tales proveedores es facilitar la intermediación de aquellas de modo electrónico.

Por último, encontramos a los mediadores comerciales tradicionales. Estos son un grupo muy amplio de actores tradicionales en el comercio y que son replicados en el mundo virtual, tales como minoristas, instituciones financieras, anunciantes y otros operadores muy diversos que facilitan las transacciones y el comercio electrónico.

Como el foco de atención está puesto en las redes sociales, más concretamente, en Facebook (al ser este el demandado en el asunto objeto del análisis principal en este trabajo), lo primero que parece imprescindible es ofrecer una definición de este fenómeno. Al respecto, se pueden catalogar como 'redes sociales' a todos aquellos servicios basados en la web que permiten a los usuarios construir un

perfil público o semipúblico dentro de un sistema delimitado, además de articular una lista de otros usuarios con los que comparten conexiones y, por último, visualizar y rastrear su lista de conexiones y aquellas realizadas por otros dentro del sistema (Boyd & Ellinson, 2007, p. 211). Se trata en estos casos de ofrecer un entorno de la sociedad de la información en el cual los usuarios dispongan de una plataforma de comunicación a través de internet. Una vez dentro del espacio web, los participantes generan un perfil con sus datos personales, facilitando así la creación de comunidades con base en criterios comunes y permitiendo la comunicación entre usuarios, así como su interacción, de tal forma que se puedan entablar relaciones recíprocas mediante mensajes o intercambiando información, imágenes y videos. El objetivo es que todas las publicaciones sean accesibles de forma inmediata para el conjunto de usuarios del grupo (Barrio Andrés, 2017, p. 402).

En concreto, la plataforma Facebook se funda en 2004, lo cual marcó un hito sin parangón en la historia de las redes sociales. Su funcionamiento se basa en la interacción entre usuarios a través de la transferencia entre unos y otros de sucesos cotidianos, con el complemento de fotos e historias. Además, la red se ha caracterizado por su adecuación a diferentes idiomas, por lo que ha podido llegar sin restricción a todas las geografías que correspondan (Gutiérrez de Aizpuru, 2019, p. 234). En lo que respecta a si puede ser considerado un prestador de servicios de alojamiento de datos, en el sentido requerido por la normativa de la Unión Europea, la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* se limita a señalar que "ha quedado acreditado que Facebook es un prestador de servicios de alojamiento de datos" (Caso C-18/18, 2019, apartado 22). En consecuencia, el TJUE no aborda esta cuestión y la da por acreditada.

Por su parte, el Abogado General Maciej Szpunar en sus conclusiones sobre la mencionada sentencia (Caso C-18/18, 2019) indica que el TJUE ya ha tenido ocasión de aclarar que el explotador de una plataforma de red social en línea que almacena en sus servidores información facilitada por usuarios de dicha plataforma, relativa a su perfil, es un prestador de servicios de alojamiento de datos. Además, añade que de la petición de decisión prejudicial se desprende que el órgano jurisdiccional remitente considera acreditado que Facebook Ireland es un prestador de servicios de alojamiento de datos cuyo comportamiento se ciñe al de un prestador intermediario (Caso C-18/18, Szpunar, 2019, apartado 30). Tampoco se aportan argumentos concluyentes que corroboren sus conclusiones sobre esta controvertida cuestión.

Con todo, son las conclusiones del Abogado General Henrik Saugmandsgaard Øe en los asuntos acumulados C-682/18 y C-683/18 (2020) las que pueden despejar alguna incógnita a este respecto. Esto último sin perjuicio de ver si las confirma el TJUE, pues ambos casos están todavía pendientes de decisión.

De entrada, parece desprenderse de tales conclusiones que, para ser considerado un prestador de servicios de alojamiento de datos, es necesario que se den dos requisitos acumulativos: a) debe existir una prestación de un servicio de la sociedad de la información; y b) dicho servicio debe consistir en almacenar datos facilitados por el destinatario del servicio a petición de este último (Casos acumulados C-682/18 & C-683/18, Saugmandsgaard Øe, 2020, apartado 141).

Para que se produzca lo primero, es decir, que exista una prestación de un servicio de la sociedad de la información, las mencionadas conclusiones hacen referencia a que se debe tratar de un servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios (Casos acumulados C-682/18 & C-683/18, Saugmandsgaard Øe, 2020, apartado 142). Por su parte, el segundo requisito exigirá, de conformidad con el abogado Saugmandsgaard Øe, que el prestador de servicios lo sea de intermediación, en el sentido de que el prestador desempeñe un papel neutro y su comportamiento sea meramente técnico, automático y pasivo, de manera que no tenga conocimiento ni control de la información que almacena (Casos acumulados C-682/18 & C-683/18, 2020, apartado 148). Lo contrario, es decir, que el prestador desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados, impediría considerarle como un prestador de servicios de alojamiento de datos.

Pues bien, el TJUE ya ha tenido ocasión de declarar en el caso *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*, antes de la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* que el explotador de una plataforma de red social en línea almacena en sus servidores información facilitada por usuarios de dicha plataforma, relativa a su perfil, y que de este modo es un prestador de servicios de alojamiento de datos (Caso C-360/10, 2012, apartado 27). De esto se deduce que Facebook, al ser una red social, es un prestador de servicios de alojamiento de datos. Además, de conformidad con las conclusiones del Abogado General en los asuntos acumulados C-682/18 y C-683/18 (Saugmandsgaard Øe, 2020), aquel presta un servicio de la sociedad de la información a cambio normalmente de

una remuneración, a distancia, por vía electrónica y a petición individual, al mismo tiempo que su actividad presenta un carácter de intermediación, por cuanto desempeña un papel neutro y su comportamiento es meramente técnico, automático y pasivo, sin conocimiento ni control de la información que almacena.

Esto último no resulta contradicho por el comportamiento del proveedor de una red social cuando determina, mediante la aplicación de sus algoritmos, qué contenidos alojados en sus servicios se muestran a sus usuarios, lo que podría hacer dudar de que su intervención fuera meramente automática y pasiva (De Miguel Asensio, 2019). Al respecto, en las conclusiones del Abogado General en los asuntos acumulados C-682/18 y C-683/18 se indica, en el apartado 160, que el hecho de que el prestador haya desarrollado herramientas –y, en particular, algoritmos que permiten el tratamiento de los datos– y que controle, en concreto, las condiciones de aparición de los resultados de las búsquedas, no demuestra que controle el contenido de los datos buscados (Saugmandsgaard Øe, 2020). En resumidas cuentas, afirma que su intervención no deja de ser meramente automática y pasiva, de tal forma que no tiene conocimiento ni control de la información que almacena.

III. EL RÉGIMEN DE LA RESPONSABILIDAD POR CONTENIDOS ILÍCITOS

En el contexto de la Unión Europea, la Directiva sobre el comercio electrónico (en adelante, DCE), de 8 de junio de 2000 (Directiva 2000/31), es la que ha venido a disciplinar la responsabilidad de los prestadores de servicios de alojamiento.

En particular, son los artículos 12 a 15 de la DCE los que se han dedicado a regular las obligaciones que pesan sobre los prestadores de servicios de alojamiento de cara, sobre todo, al control de los contenidos que se difunden por terceros. Dichos preceptos se enmarcan en la sección cuarta, del capítulo segundo de la DCE, que lleva por título el de la responsabilidad de los prestadores de servicios intermediarios. Pero, en concreto, de todos ellos nos interesa especialmente el artículo 14, por cuanto se refiere al prestador de servicios de alojamiento de datos. Habiendo quedado acreditado en el epígrafe anterior que Facebook Ireland es un prestador de servicios de alojamiento de datos, resulta evidente que la responsabilidad por contenidos ilícitos, en la que podría incurrir, entra dentro del ámbito de aplicación del artículo 14 de la DCE.

Tal y como se indica en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, el apartado 1 del artículo 14 de la DCE tiene por objeto eximir de responsabilidad al prestador de servicios de alojamiento de datos cuando cumpla uno de los dos requisitos establecidos en la citada disposición: a) no tener conocimiento de que la actividad o la información es ilícita; o b) actuar con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible en cuanto tenga conocimiento de estos puntos (Caso C-18/18, 2019, apartado 23).

Para despejar cualquier duda que pudiera existir sobre la aplicación de esta exención de responsabilidad a una red social y, en concreto, a Facebook, hay que tener en cuenta el considerando número 42 de la DCE. En este último se señala que, para beneficiarse de la correspondiente exención:

a) la actividad del prestador de servicios debe limitarse al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros sea transmitida o almacenada temporalmente, con el fin de hacer que la transmisión sea más eficiente; y

b) la actividad en cuestión debe ser de naturaleza meramente técnica, automática y pasiva, lo que implica que el prestador de servicios no tenga conocimiento ni control de la información transmitida o almacenada.

Como quiera que todos los atributos que se acaban de señalar ya fueron exigidos también para identificar a los prestadores de servicios de alojamiento de datos, en el epígrafe tercero de este trabajo, y se catalogó a las redes sociales y, en particular, a Facebook como un ejemplo de este tipo de prestadores, puede asegurarse sin temor a equivocarnos que, por ende, aquellos se benefician de la exención de responsabilidad.

Ahora bien, la razón de ser de la DCE no era establecer un régimen mínimo de responsabilidad de los prestadores de servicios de alojamiento de datos, sino de blindarles mediante la creación de una zona de exención de responsabilidad para favorecer la prestación transfronteriza de servicios de la sociedad de la información (Ortego Ruiz, 2015, p. 34). A pesar de la exención, en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* se señala, en su apartado 24, que del apartado 3 del artículo 14 de la DCE, en relación con su considerando 45, se desprende la posibilidad de que un tribunal o una autoridad administrativa nacional exija al prestador de servicios de alojamiento de datos que se trate de poner fin a una infracción o impedirla, incluso suprimiendo los datos ilícitos o impidiendo el acceso a ellos. Aquello se justifica porque, debido a la peculiar posición de los in-

termediarios, la actuación de estos proveedores puede resultar determinante para lograr que cese la actividad infractora por parte del responsable, típicamente al hacer efectiva la retirada o bloqueo de los contenidos ilícitos (De Miguel Asensio, 2015, p. 240).

Ha quedado acreditada la existencia de una exención de responsabilidad para los prestadores de servicios de alojamiento de datos y, por consiguiente, para las redes sociales y Facebook, por los contenidos ilícitos vertidos por los usuarios. Exención que, no obstante, puede ser mitigada con la obligación de que aquellos pongan fin a la infracción o la impidan, incluso suprimiendo los datos ilícitos o impidiendo el acceso a ellos.

Por su parte, hay que tener en cuenta el artículo 15, apartado 1, de la DCE. Este precepto impide que los Estados miembros impongan a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, así como una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios previstos en los artículos 12, 13 y 14. De tal forma que, en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* las cuestiones prejudiciales que se plantearon al TJUE por el Tribunal Supremo austríaco se circunscribieron a concretar el alcance personal y material de los mandamientos de retirada de contenidos ilícitos, así como el territorial, aunque este último lo abordaremos más adelante en el epígrafe sexto de este trabajo.

Por lo que respecta al alcance personal y material de los requerimientos judiciales de retirada de contenidos ilícitos, se debe precisar que lo prohibido por el artículo 15, apartado 1, de la DCE son las obligaciones de supervisión general. Sin embargo, se permiten las obligaciones de supervisión en casos específicos, tal y como se predica en el considerando 47 de la DCE. Lo que se entiende por supervisión en casos específicos ha sido precisado por el TJUE en el apartado 35 de la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18, 2019). Al respecto, se indica que tal caso específico puede tener su origen, en particular, como sucede en el litigio principal, en una información precisa, almacenada por el prestador de servicios de alojamiento de datos de que se trata a instancia de un determinado usuario de su red social. El contenido de la información en cuestión, además, ha sido analizado y apreciado por un tribunal competente del Estado miembro que, al término de su apreciación, lo ha declarado ilícito. Si bien esta delimitación de que se entiende por 'supervisión en casos específicos' toma como referencia las circunstancias del asunto en el litigio principal, nada impide apreciar que puede haber situaciones en las que concurran otros elementos y la supervisión quede igualmente limitada a casos específicos (De Miguel Asensio, 2019).

En consecuencia, se constata que existe un riesgo real de que una información que ha sido declarada ilícita sea reproducida y compartida posteriormente por otro usuario de la red. Pero, al mismo tiempo, el artículo 15, apartado 1, de la DCE impide que para evitar ese peligro se imponga una obligación excesiva al prestador de servicios de alojamiento de datos, tal y como rezan los apartados 36 y 44 de la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited.* Por lo tanto, el TJUE se tuvo que manifestar sobre la posibilidad de que el artículo 15, apartado 1, de la DCE se opusiera a que un órgano jurisdiccional de un Estado miembro pudiera obligar a un prestador de servicios de alojamiento de datos a suprimir los datos que almacene. En concreto, cuando el contenido sea 'idéntico' o 'similar' al de una información declarada ilícita con anterioridad o a bloquear el acceso a ellos, sea cual fuere el autor de la solicitud de almacenamiento de tales datos.

Al respecto, el Abogado General en el apartado 109 de sus conclusiones sobre el asunto *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18, Szpunar, 2019), se decantó por interpretar el artículo 15, apartado 1, de la DCE como compatible con un mandamiento judicial que obligue a un prestador de servicios de alojamiento de datos a que busque e identifique, entre todos los datos difundidos por los usuarios, datos idénticos a los declarados ilícitos. Para los datos similares, sin embargo, solo lo consideró apropiado si se circunscribía a los difundidos por el usuario que publicó tales datos. Para justificar su decisión, en el apartado 74 de sus conclusiones, tuvo en cuenta que imponer una obligación de identificar datos similares a los declarados ilícitos procedentes de cualquier usuario no garantizaría un justo equilibrio entre la protección de la intimidad y los derechos de la personalidad, libertad de empresa y libertad de expresión e información (Caso C-18/18, Szpunar, 2019). Además, añadió que la búsqueda e identificación de esos datos precisaría de soluciones costosas, que deberían ser desarrolladas e implantadas por el prestador de servicios de alojamiento de datos (Caso C-18/18, Szpunar, 2019). Incluso, consideró que la aplicación de esas soluciones daría lugar a una censura, de modo que la libertad de expresión y de información podría verse sistemáticamente limitada.

Por su parte, el TJUE en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* ha optado por una interpretación más amplia. En

este sentido, considera ajustado al artículo 15, apartado 1, de la DCE un mandamiento judicial que obligue a un prestador de servicios de alojamiento de datos a que realice una supervisión y búsqueda de los datos idénticos a los declarados ilícitos, con independencia del autor que los haya difundido (Caso C-18/18, 2019). También si versa sobre datos de contenido similar y aunque provengan de cualquier usuario del servicio (Caso C-18/18, 2019, apartado 53). En efecto, para las informaciones similares, la obligación de eliminarlas no se limita a las vertidas por el autor que publicó las catalogadas de ilícitas con anterioridad. Esta solución parece razonable, habida cuenta de que no cabe excluir que, en ocasiones, medidas de retirada relativas a contenidos similares de otros usuarios puedan ser precisas y estar configuradas de manera que no impongan soluciones excesivamente costosas ni menoscaben de manera excesiva la libertad de expresión ni el resto de los derechos fundamentales afectados (De Miguel Asensio, 2019).

Además, el TJUE en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* ofrece aclaración sobre cómo acreditar los datos similares (Caso C-18/18, 2019, apartado 45). Al respecto, indica que deben contener elementos concretos debidamente identificados por el autor de la medida cautelar, como el nombre de la persona víctima de la infracción constatada anteriormente, las circunstancias en las que se ha comprobado dicha infracción, así como un contenido similar al que se ha declarado ilícito. Por lo tanto, será posible imponer a los prestadores de servicios de alojamiento de datos medidas de supervisión tanto de los contenidos idénticos, como de los similares a los declarados ilícitos anteriormente, ya bien se hayan difundido por el autor de estos últimos o por cualesquiera otros usuarios del servicio.

Ahora bien, hay doctrina que disiente con el planteamiento que se acaba de esbozar. Así, en el caso de los datos similares a los declarados ilícitos anteriormente, se viene a indicar que el estado actual de la tecnología impide identificar información parecida cuya equivalencia con la controvertida puede venir del contexto en el que se ha producido o del sentido que se le quiere otorgar, por ejemplo, si su significado pretende satirizar o criticar el contenido original. Esta situación requeriría que las plataformas tuvieran que acudir a la supervisión humana para realizar una serie de evaluaciones sustantivas que, además, serían indefinidas en el tiempo. De tal forma que los prestadores de servicios de alojamiento de datos tendrían que seguir evaluando cualquier nueva circunstancia que pudiera entrar en colisión con el contenido ilícito declarado con anterioridad. Incluso, a la inversa, podría ocurrir que la información sobrevenida, que hiciera referencia a la actuación posterior del perjudicado inicialmente, convirtiera en lícita y verdadera la difusión de la información que se hubiera dado al respecto (Cavaliere, 2019).

En esta misma línea, se indica que las herramientas de filtrado automatizadas proporcionan fácilmente 'falsos positivos' al identificar incorrectamente el contenido como ilegal, lo que lleva a la eliminación de contenido legítimo. Incluso las herramientas que se basan en la inteligencia artificial son incapaces de comprender la ironía o la sátira o darse cuenta de que el discurso del odio se puede utilizar en una cita para crear conciencia (Rauchegger & Kuczerawy, 2020, p. 1518). También se ha dicho que un contenido idéntico no implica necesariamente un significado idéntico. En algunos casos, el mensaje podría ser idéntico al original, pero en otros casos podría ser diferente, con el resultado de que el contenido, aunque idéntico, podría no ser ilegal, por ejemplo, si está inserto en un comentario más amplio (Rosati, 2019). Esto último se podría producir cuando el contexto modifique el sentido y, en consecuencia, el contenido idéntico presente un significado diferente, de manera que no acabe resultando lesivo.

En definitiva, parecería que la supresión del contenido idéntico o similar no se podría realizar solo de manera automatizada: habría una primera preselección mecanizada de la información y, después, una decisión final por el sujeto correspondiente tras la evaluación oportuna. Al respecto, la regulación más reciente de la Unión Europea en materia de contenido *online* sigue esta misma estela de requerir la revisión de las decisiones de filtrado automatizadas por parte de las personas competentes. Así, por un lado, la Directiva 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital, en su artículo 17, apartado 9, establece que "las decisiones de inhabilitar el acceso a los contenidos cargados o de retirarlos estarán sujetas a examen por parte de personas" (2019). Por otro lado, la Propuesta de reglamento para la prevención de la difusión de contenidos terroristas en línea (Comisión Europea, 2018), en su artículo 9, estipula algo parecido: indica que los prestadores de servicios de alojamiento de datos aplicarán garantías eficaces y adecuadas cuando usen instrumentos automatizados para tomar decisiones sobre la retirada de los contenidos considerados terroristas o bloquear el acceso a ellos. Esto último persigue que las decisiones de retirada o bloqueo sean precisas y bien fundamentadas, para lo que se basarán, en particular, en la supervisión y verificaciones por personas.

IV. ALGUNOS EJEMPLOS SOBRE LA RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS

La responsabilidad de los prestadores de servicios de alojamiento de datos puede quedar exonerada, en un primer momento, si desconocían que la actividad o la información eran ilícitas. En caso contrario, todavía podrían evitar ser reclamados, en un segundo momento, si proceden a la inmediata retirada de los contenidos ilícitos alojados. En relación con el conocimiento sobre la ilegalidad de los contenidos alojados, el TJUE se ha mostrado partidario de interpretarlo de manera extensiva, es decir, mediante el llamado conocimiento indiciario (Ortego Ruiz, 2015, p. 49). La sentencia de 12 de julio de 2011, caso *L'Oréal SA et al. c. eBay International AG et al.*, tuvo ocasión de señalar que la percepción sobre el carácter ilegítimo de los contenidos se equipara a cualquier situación en la que el prestatario en cuestión adquiera conocimiento, de una forma o de otra, de tales hechos o circunstancias (Caso C-324/09, 2011, apartado 121).

La afirmación anterior se ilustra haciendo referencia a que en este supuesto encaja, en particular, la hipótesis en la que el operador de un mercado electrónico descubra la existencia de una actividad o información ilícitas como consecuencia de una investigación realizada por su propia iniciativa. Además, se incluiría el supuesto en el que le sea notificada la existencia de este tipo de actividad o información. Por su parte, para el segundo caso, se aclara que la existencia de una notificación no determina automáticamente que el operador pierda la posibilidad de invocar la exención de responsabilidad. Al respecto, cabría invocarla cuando la notificación de la existencia de actividades o informaciones supuestamente ilícitas resulte excesivamente imprecisa o no esté suficientemente fundamentada. En cualquier caso, la notificación constituye, como regla general, un elemento que el juez nacional debe tomar en consideración para apreciar si el operador tenía realmente conocimiento de hechos o circunstancias a partir de los cuales uno diligente hubiera debido constatar ese carácter ilícito (Caso C-324/09, 2011, apartado 122).

En la misma línea, la sentencia del TJUE de 23 de marzo de 2010, en los asuntos acumulados C-236/08 y C-238/08, también señaló que la responsabilidad de los prestadores de servicios de alojamiento de datos queda acreditada cuando la ilicitud de los datos o de las actividades del destinatario del servicio llegan a su conocimiento. Esto último puede suceder gracias a la información recibida de un perjudicado o de otro modo (Casos acumulados C-236/08 & C-238/08, 2010, apartado 109). Se deduce de todo lo dicho hasta ahora, que la posibilidad de llegar a la convicción de la ilegalidad 'de una forma' o 'de otro modo' son conceptos jurídicos indeterminados que generan inseguridad. Se podría subsanar esta situación con la elaboración de indicadores jurídicos, a modo de norma que lo regulara, en los cuales se especificaran los mecanismos de detección y retirada de contenidos. Ello se hace en la legislación norteamericana a través de la *Digital Millennium Copyright Act* (1998), en donde se ofrecen este tipo de aclaraciones, en la sección 512 (c) (3), lo que, sin duda, aporta confiabilidad al sistema.

Por lo que respecta a la retirada inmediata de los contenidos ilícitos alojados para sustraerse de la responsabilidad, aquella se entiende como una segunda posibilidad para esquivar la reclamación por daños. Pero para proceder a la retirada debe existir certeza de la ilicitud de los contenidos, para lo cual sería necesario precisar a quién le corresponde ponerlo de manifiesto. En situaciones dudosas, el prestador de servicios podría verse obligado a retirar una información que luego pudiera resultar lícita, por lo que también incurriría en responsabilidad por atentar contra la libertad de expresión e información. Es por ello que se necesitan mecanismos que arbitren soluciones efectivas y eficaces, pero, sobre todo, que aporten una prueba fiable o suficiente en Derecho.

Al respecto, la Directiva sobre el comercio electrónico alude en su artículo 14, apartado 3, a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de servicios poner fin a una infracción o impedirla (Directiva 2000/31/CE, 2000). Pues bien, esa podría ser la opción para acreditar la ilicitud: que se encomiende esa tarea al Poder Judicial o al órgano equivalente de la administración. Tal parece ser la solución más garantista y la que se apunta en la sentencia del TJUE de 13 de mayo de 2014, en el caso *Google Spain, S.L. y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (Caso C-131/2012), cuando se alude a la autoridad de control o al órgano jurisdiccional. En concreto, la referencia a ambos se hace con el fin de que ordenen a Google que elimine de la lista de resultados del buscador la información relativa a una persona, de quien ha sido vulnerado su derecho fundamental a la protección de datos (Caso C-131/2012, 2014, apartado 82). De manera que se consigue contar con el filtro categórico de las instancias jurisdiccionales o gubernativas para la acreditación de la vulneración producida; sin que el prestador del servicio tenga ahora la más mínima duda de que, para librarse de la responsabilidad, debe actuar con prontitud a la hora de quitar la información controvertida.

También el Tribunal Europeo de Derechos Humanos del Consejo de Europa ha tenido ocasión de pronunciarse sobre la responsabilidad de los prestadores de servicios. En concreto, la sentencia de 16 de junio de 2015, en el asunto *Delfi AS c. Estonia,* se refirió a la responsabilidad de los portales de noticias por los contenidos difamatorios publicados por los lectores. La cuestión principal que se abordó en la resolución judicial estaba relacionada con la consideración de los portales que alojan foros. Se debatía si debían ser considerados intermediarios de servicios de la sociedad de la información o, por el contrario, debían ser equiparados a los proveedores de contenidos. En el primer caso, se podrían beneficiar de la exención de responsabilidad de la DCE; mientras que, en el segundo, tendrían la obligación de controlar los contenidos. Pues bien, la solución a la que llegó el Tribunal fue estimar que el administrador de un portal de noticias en internet tenía la consideración de editor y, por ende, asumía la responsabilidad directa por los contenidos publicados por los lectores (*Delfi AS c. Estonia*, 2015). Hay, en consecuencia, una equiparación entre estos portales de noticias en internet y los medios de comunicación tradicionales, por lo que se les impone la llamada *culpa in vigilando* por los contenidos (Departamento de Telecomunicaciones & Media de Garrigues, 2013).

Se comparte la opinión que considera discutible la respuesta ofrecida, tanto por los tribunales estonios como por el Tribunal Europeo, en relación con algunos de los comportamientos enjuiciados desde la perspectiva de su conformidad con la DCE (De Miguel Asensio, 2013). En cualquier caso, la conclusión a la que se llegó en este asunto fue la de entender que no se comprometía a libertad de expresión prevista en el artículo 10 del Convenio Europeo de Derechos Humanos, debido a la obligación del portal de suprimir los contenidos lesivos. Además, se le consideró civilmente responsable frente a la víctima por los contenidos difamatorios que terceros habían introducido en sus servicios.

Resultan también relevantes las opiniones de la doctrina respecto a la responsabilidad que debe pesar sobre los prestadores de servicios. Así, encontramos posturas que hacen referencia al estándar mayor de diligencia que se les aplicaría a los portales de noticias y a otros agregadores, como consecuencia de la sentencia del Tribunal Europeo de Derechos Humanos en el caso *Delfi AS c. Estonia.* Esta situación se produce como consecuencia de que queden al margen de la DCE y, por ende, de la imposibilidad de aplicarles la exclusión de responsabilidad propia de las reglas contenidas en dicha norma, lo cual ha sido considerado inaceptable. Al respecto, se indica que las interacciones y las relaciones de la red social con sus usuarios es muy diferente al de un medio de comunicación tradicional respecto de quienes publican en estas plataformas. Incluso se añade que, sin esta regla de exclusión, muchas de las posibilidades de negocios, pero también de expresión, asociadas a las redes sociales, simplemente, no existirían, y de forma consiguiente el pluralismo se resentiría gravemente (Boix Palop, 2016, pp. 93-94).

Por lo tanto, en la sociedad de la información la libertad de expresión adquiere una nueva dimensión, mostrándose como representante de una nueva cultura y de un nuevo modelo de vida (Teruel Lozano, 2010, p. 128). Ahora bien, no puede obviarse que para evitar resultados inopinados y divergentes en las diversas jurisdicciones, resultaría conveniente que las reglas fueran lo suficientemente homogéneas, por lo menos, en toda la Unión Europea (Peguera Poch, 2010, p. 267). En esta línea, la fórmula del Reglamento y no de la Directiva, como hasta ahora ha ocurrido con la DCE, podría ser la solución más adecuada para incrementar la seguridad en el sistema. Optar por reglas idénticas para todos, en lugar de conformarse con normas de mínimos traspuestas en los ordenamientos estatales con diferentes niveles de exigencia, parece un paso más que necesario en el momento actual de la evolución de los servicios de la sociedad de la información y del comercio electrónico.

V. COMPETENCIA JUDICIAL INTERNACIONAL POR VULNERACIÓN DE DERECHOS DE LA PERSONALIDAD Y DERECHO APLICABLE

Presupuesto necesario de la eventual adopción de medidas de retirada de contenidos con alcance mundial es que el órgano al que se solicitan tenga competencia judicial internacional para adoptarlas (De Miguel Asensio, 2019). Por lo que respecta a los litigios en los que se alegue una lesión de los derechos de la personalidad mediante el contenido publicado en un sitio de internet, la jurisprudencia del TJUE ya ha tenido ocasión de pronunciarse sobre la interpretación del instrumento jurídico que en la Unión Europea regula esta cuestión y que se circunscribe al Reglamento 1215/2012 (2012). En concreto, en los litigios relativos a la responsabilidad extracontractual por vulneración de los derechos de la personalidad, como es este caso, los tribunales de los Estados miembros correspondientes a los del domicilio del demandado, del lugar de origen del daño o del centro de intereses de la víctima pueden tener competencia con alcance general, incluyendo medidas de retirada de contenidos de internet sin limitación territorial (De Miguel Asensio, 2020b).

En efecto, de conformidad con la sentencia *eDate Advertising GmbH et al. c. X y Société MGN Ltd,* la interpretación del artículo 7.2 del Reglamento 1215/2012 permite que la persona que se considera lesionada pueda ejercitar una acción de responsabilidad por la totalidad del daño causado, ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses (Casos acumulados C-509/09 & C-161/10, 2011, apartado 48). Se infiere de lo anterior, que los tribunales correspondientes a la residencia del perjudicado, donde con carácter general se sitúa su centro de intereses, son competentes para acordar medidas relativas a la retirada de contenidos de internet con un alcance territorial ilimitado. Además, en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, tal y como se indica por el Abogado General en sus conclusiones (Caso C-18/18, Szpunar, 2019, apartado 84), el órgano jurisdiccional ante el que la demandante ha ejercitado la acción es el de su centro de intereses.

Las ventajas de este foro son claras, ya que potencia la buena administración de la justicia, pues dicho lugar presenta una conexión innegable con el supuesto litigioso. Además, propicia que la competencia del tribunal del lugar en el que la presunta víctima tiene su centro de intereses sintonice correctamente con el principio de previsibilidad (Calvo Caravaca & Carrascosa González, 2017, p. 1549). Esto último se logra por el conocimiento que puede tener el demandado, cuando introduce los datos lesivos, de cuáles son los centros de intereses de las personas que han sido objeto de sus comentarios. Por su parte, el demandante también se ve favorecido, porque puede averiguar sin dificultad el tribunal competente para conocer de su caso, por coincidir con el del lugar donde se encuentra su centro de intereses.

Por consiguiente, tal y como establece el Abogado General en sus conclusiones relativas al asunto *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* los tribunales de un Estado miembro pueden resolver, en principio, sobre la retirada de contenidos fuera del territorio del citado Estado miembro, pues tienen competencia territorial universal (Caso C-18/18, Szpunar, 2019). Aunque podría resultar inviable que los órganos jurisdiccionales de un Estado miembro se pronunciaran sobre la retirada a nivel mundial no ya por un tema de competencia, sino, en su caso, por una cuestión de fondo (Caso C-18/18, Szpunar, 2019, apartado 86). Esto último nos lleva inevitablemente a dedicar las líneas que siguen a la determinación de la ley aplicable a una lesión a los derechos de la personalidad en internet. El motivo de tener que hacerlo se encuentra en que la determinación de la ley aplicable en materia de derechos de la personalidad se presenta como una cuestión clave y de extremada importancia. Esto último se deduce de las frecuentísimas violaciones que en esta materia se producen a través de internet, así como de la nuclear importancia que en la construcción del Estado Social y de Derecho han tenido y tienen los bienes jurídicos protegidos por estos derechos. No en vano están protegidos como derechos fundamentales la libertad de expresión e información, así como el derecho al honor, la intimidad y la propia imagen, límite uno del otro y cuya regulación equilibrada es básica en la configuración del mismo (Ortego Ruiz, 2015, pp. 130-131).

Una dificultad añadida en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* es que aquel va referido a una materia en la que ni el derecho material ni las reglas de conflicto están unificadas en el seno de la Unión Europea. Esta falta de regulación uniforme se deriva de la exclusión de las violaciones de derechos de personalidad del ámbito de aplicación del Reglamento 864/2007 (Roma II), en virtud de su artículo 1.2.g (De Miguel Asensio, 2019). En consecuencia, la determinación de la ley aplicable a una reclamación de ese tipo debe hacerse en los Estados miembros de la Unión Europea según las reglas nacionales del Derecho internacional privado. Sin que sea extraño, desde una perspectiva comparada, que las normas de conflicto en esa materia puedan conducir a la aplicación de una única ley, por ejemplo, la de la sede de la víctima, al conjunto de la reclamación (De Miguel Asensio, 2020b).

En cualquier caso, la ley aplicable al fondo del asunto regulará la precisión de quién es el autor de la vulneración de los derechos de la personalidad y la responsabilidad que debe imputarse al autor de la lesión referida. También deberá concretar qué otros sujetos pueden ser demandados por infracción de estos derechos en internet. Además de decidir la cuestión de la responsabilidad civil de los sujetos que administran *websites,* con enlaces de internet a otros *websites,* en los que se encuentran materiales que lesionan los derechos de personalidad (Calvo Caravaca & Carrascosa González, 2017, p. 1554). Todo ello sin olvidar que en la Unión Europea sería aplicable la DCE, con todo lo que ya hemos visto en relación con el régimen de la responsabilidad por contenidos ilícitos en el epígrafe anterior.

Lo único que nos queda ahora por determinar es el alcance territorial de los mandamientos de retirada. En concreto, abordaremos si la supresión de contenidos por una red social debe referirse solo a los datos del servicio en el Estado miembro cuyos tribunales conocen de litigio principal o también se extiende a las informaciones de cualquier lugar del mundo.

VI. LA EJECUCIÓN DE UNA OBLIGACIÓN DE RETIRADA EN TODO EL MUNDO

Resulta indubitada, de acuerdo con los planteamientos esgrimidos hasta el momento, la obligación que pesa sobre los prestadores de servicios de alojamiento de datos y, por ende, sobre Facebook Ireland, en relación con la retirada o eliminación de los datos declarados ilícitos por la autoridad competente en cuestión. Obligación, por cierto, que se extiende no solo a los datos introducidos en la red social por el autor correspondiente, sino también a los que sean idénticos a los declarados ilícitos y hayan sido difundidos por cualesquiera usuarios del servicio. Incluso abarca a los que sean similares, con independencia también de quién haya sido el autor de la información controvertida. En consecuencia, lo que procede a continuación es delimitar el alcance territorial de la orden de retirada. El motivo se encuentra en las dudas que se plantean en el litigio *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* relativas a si el mandamiento de retirada de los contenidos ilícitos se circunscribe solo a los datos correspondientes en el Estado miembro cuyos tribunales conocen del asunto o tiene también un alcance mundial.

Al respecto, el TJUE, en su sentencia sobre el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, se pronunció con rotundidad al entender que el apartado 1 del artículo 18 de la DCE no limita en modo alguno, en particular territorialmente, el alcance de las medidas que los Estados miembros pueden adoptar con arreglo a la norma citada. Por consiguiente, concluye el TJUE, la DCE no se opone a que las referidas medidas cautelares produzcan efectos a escala mundial (Caso C-18/18, 2019, apartados 49 & 50).

Ahora bien, el principio de la razonabilidad permite cuestionar la aplicación indiscriminada de lo que parecen valores absolutos. A su vez, admite un enfoque misceláneo del derecho internacional privado sobre la base de conceptos tales como las expectativas razonables, vínculos más estrechos, el deber de evaluar y equilibrar, la distinción entre superposición en la regulación y conflicto directo y entre conflicto potencial y choque real (Lowenfeld, 1996, pp. 229-230). Por lo que, para el caso que nos ocupa, se trataría de encontrar una forma lógica y tangible de ejecutar una medida de supervisión de manera segura y efectiva. Sin pretender imponer una pléyade de controles a la red social sobre todos los contenidos vertidos en línea.

La supervisión habría de tener en cuenta, tal y como señala el Abogado General en el apartado 100 de sus conclusiones sobre el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18, Szpunar, 2019), las diferencias que existen entre las leyes nacionales, por un lado, y la protección de la intimidad y de los derechos de la personalidad que dichas leyes establecen, por el otro. De tal forma que, para respetar derechos fundamentales ampliamente reconocidos, sería conveniente que dichos órganos jurisdiccionales adoptaran una postura comedida. Es más, el cumplimiento de una obligación de retirada no debería ir más allá de lo necesario para lograr la protección de la persona lesionada, so pena de ser imposible obtener el reconocimiento y la ejecución de resoluciones en terceros países cuyo orden público entre en contradicción con dichas medidas (De Miguel Asensio, 2020b).

Esta solución es la que parece imponerse de cara al futuro más inmediato con la Propuesta de Reglamento que establece la ley de servicios digitales en la Unión Europea (*Digital Markets Act*, 2020). En efecto, el artículo 8.2.b viene a decir que el alcance territorial de los mandamientos jurisdiccionales o administrativos para actuar contra los contenidos ilegales, sobre la base de las normas aplicables del Derecho estatal y de la Unión, incluida la Carta, y, en su caso, los principios generales del derecho internacional, no excederá de lo estrictamente necesario para alcanzar su objetivo (*Digital Markets Act*, 2020). Además, la propuesta en cuestión supondrá una unificación y no una armonización, como hasta ahora, de las normas que regulan la actuación de las plataformas *online*. Esta última situación se puede catalogar como muy beneficiosa, por su contribución a la seguridad jurídica de todos los participantes en el mundo digital. En efecto, entre las diferentes opciones legislativas, se ha elegido la del Reglamento, en tanto instrumento jurídico de efecto directo e inmediato en todo el territorio y que va a acompañado de una elevada dosis de precisión en la regulación, indispensable a los efectos pretendidos (Soldevila Fragoso, 2021). Por lo tanto, entre los niveles de obligatoriedad existentes en los tipos de normas de la Unión Europea, se opta por el más elevado, lo que claramente está en línea.

VII. CONCLUSIONES

No cabe duda de que internet ha supuesto una revolución sin precedentes en prácticamente todos los ámbitos de actuación del ser humano. Hay relaciones sociales que se producen a través de la red, pero también operaciones económicas, transacciones mercantiles y un sinfín de situaciones jurídicas que se llevan a cabo a través de este medio. Su peculiaridad fundamental es que se trata de una dimensión que no entiende de fronteras y presenta un carácter ubicuo, por lo que el alcance de su

proyección es, en principio, universal. La ausencia de márgenes definidos que presenta el espacio *online* mantiene una convivencia poco pacífica con la fragmentación jurídica que está presente en el mundo *offline*.

En efecto, en un planeta dividido en Estados, cada uno de los cuales regula de manera específica las actividades en línea, los problemas de Derecho internacional privado son recurrentes. Ya bien sean problemas de competencia judicial internacional, de ley aplicable o de eficacia extraterritorial de resoluciones judiciales extranjeras, se irán produciendo en la medida en que la difusión de los contenidos en línea se conecte con un gran número de ordenamientos jurídicos. A ello se une la capacidad que tienen los datos vertidos en un entorno digital para propagarse de manera inmediata y producir, cuando son ilícitos, efectos globales. En estos casos, la existencia de instrumentos jurídicos dirigidos a minimizar los efectos perniciosos de los comportamientos de tráfico jurídico externo contrarios a Derecho, se convierte en el baluarte para equilibrar los menoscabos que hayan podido sufrir los sujetos afectados.

En el contexto de la Unión Europea, la DCE es un buen ejemplo de normativa catalizadora de soluciones adecuadas para los casos de difusión en redes sociales de informaciones controvertidas. La posibilidad de adoptar mandamientos judiciales de retirada de los contenidos lesivos difundidos por los usuarios y que deben cumplir los prestadores de los servicios de alojamiento, se considera una medida muy positiva y eficaz para acabar con la vulneración de un derecho de la personalidad. Además, se impone a los prestadores de servicios de alojamiento de datos una obligación de supervisión no general, pero sí en casos específicos, sobre los datos idénticos y similares a los declarados ilícitos con anterioridad. Sin que los datos tengan que proceder únicamente del autor de los declarados ilícitos con anterioridad, sino que pueden haber sido puestos en circulación por cualquier usuario del servicio.

Incluso no se ponen puertas al campo, en el sentido de entender que las medidas cautelares que los Estados miembros pueden adoptar con arreglo a la DCE pueden surtir efectos extraterritoriales, es decir, serían susceptibles de ser emitidas con un alcance mundial, aunque para ello se pida una postura comedida y no se exija que la retirada vaya más allá de lo necesario para lograr la protección de la persona lesionada. Solución que, por otra parte, consideramos lógica, basada en el sentido común e imbuida por el principio de la razonabilidad y que, además, parece que será la respuesta ofrecida por la Unión Europea en su propuesta de *lege ferenda* para los servicios digitales. Lo contrario, que pasaría por mandamientos indiscriminados de retirada de contenidos ilícitos debe reputarse inadecuado. La necesaria ponderación de los derechos fundamentales afectados, esto es, el de libertad de expresión con el derecho a la intimidad debe permitir que se hagan públicas las informaciones objetivas y debidamente contrastadas. Pero, al mismo tiempo, tiene que impedir que los comentarios ilícitos se propaguen por la red libremente.

Las medidas de supervisión que se imponen a los prestadores de servicios, no con un alcance general, sino para casos específicos pueden catalogarse de apropiadas. Se trata de conseguir que los contenidos idénticos a los declarados ilícitos, con independencia del autor que los haya introducido, acaben desapareciendo de internet. Pero no acaba ahí la responsabilidad de los prestadores, ya que también deberán procurar la eliminación de los datos de contenido similar y aunque provengan de cualquier usuario del servicio. Esto último es lo que, quizá, pueda resultar más controvertido, desde el momento en el que se debe realizar una valoración subjetiva de lo que se pueda considerar parecido a otro comentario declarado lesivo. Para aportar confiabilidad al sistema se podría recurrir a una primera detección por las herramientas automatizadas que identifiquen contenidos afines, para pasar después de ello a la valoración final por parte de las personas competentes. Con todo, no deja de ser un enjuiciamiento humano el que decide, lo que puede conducir a interpretaciones divergentes para los mismos supuestos y, además, sin que se precise el nivel competencial del encargado de esta tarea. Es por ello que podría ser el momento oportuno de regular esta figura, aunque posiblemente se podría equiparar al *compliance officer* que se encargaría, en este caso, de supervisar el cumplimiento tecnológico de la compañía.

REFERENCIAS

Barrio Andrés, M. (2017). *Fundamentos del Derecho de Internet*. Centro de Estudios Políticos y Constitucionales.

Boix Palop, A. (2016). La construcción de los límites a la libertad de expresión en las redes sociales. *Revista de Estudios Políticos*, (173), 55-112. http://dx.doi.org/10.18042/cepc/rep.173.02.

Boyd, D., & Ellinson, N. (2007). Social Networks Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Calvo Caravaca, A. L., & Carrascosa González, J. (2017). *Derecho Internacional Privado* (17ma ed., Vol. II). Editorial Comares.

Cavaliere, P. (2019). Glawischnig-Piesczek v Facebook on private enforcement of speech regulation and international jurisdiction. *European Data Protection Law Review, 5*(4), 573-578. https://dx.doi.org/10.2139/ssrn.3519389

Davara Rodríguez, M. A. (2005). *Manual de Derecho Informático*. Editorial Aranzadi.

De Miguel Asensio, P. A. (12 de octubre de 2013). Sobre el control de los comentarios de terceros en blogs y sitios webs tras el asunto Delfi. https://pedrodemiguelasensio.blogspot.com/2013/10/sobre-el-control-de-los-comentarios-de.html#more

(2015). *Derecho Privado de Internet* (5ta ed.). Editorial Aranzadi.

(13 de junio de 2019). Alcance material de los mandamientos judiciales de retirada de contenidos ilícitos frente a redes sociales [Entrada de blog]. https://pedrodemiguelasensio.blogspot.com/2019/06/alcance-material-de-los-mandamientos.html

(17 de junio de 2019). Alcance territorial de los mandamientos judiciales de retirada de contenidos ilícitos frente a redes sociales [Entrada de blog]. https://pedrodemiguelasensio.blogspot.com/2019/06/alcance-territorial-de-los-mandamientos.html

(4 de octubre de 2019). Alcance de los mandamientos judiciales de retirada de contenidos ilícitos frente a redes sociales: la sentencia Glawischnig-Piesczek [Entrada de blog]. https://pedrodemiguelasensio.blogspot.com/2019/10/alcance-de-los-mandamientos-judiciales.html

(2020a). Contratos de colaboración. En J. C. Fernández, R. Arenas García, & P. A. De Miguel Asensio, *Derecho de los negocios internacionales* (6ta ed., pp. 541-603). Iustel.

(2020b). Internet y Derecho internacional privado: Balance de un cuarto de siglo. En S. Álvarez González, R. Arenas García, P. A. De Miguel Asensio, S. Sánchez Lorenzo, & G. Stampa Casas (eds.), *Relaciones transfronterizas, Globalización y Derecho (Homenaje al Profesor Doctor José Carlos Fernández Rozas)* (pp. 211-228). Thomson Reuters-Civitas.

Departamento de Telecomunicaciones & Media de Garrigues (12 de noviembre de 2013). Sentencia del TEDH sobre la responsabilidad de los foros de internet (Caso Delfi AS v. Estonia). *Garrigues Blog*. http://blog.garrigues.com/sentencia-del-tedh-sobre-la-responsabilidad-de-los-foros-de-internet-caso-delfi-as-v-estonia/?cn-reloaded=1

Gutiérrez de Aizpuru, J. (2019). Implicaciones legales de las redes sociales. En J.F. Estévez, (coord.), *Derecho digital* (pp. 231-278). Thomson Reuters Aranzadi.

Internet (2020). En *Diccionario de la Lengua Española*. *Real Academia Española.* https://dle.rae.es/internet

Lowenfeld, A. (1996). *International Litigation and the Quest for Reasonableness - Essays in Private International Law.* Clarendon Press-Oxford.

Organización Mundial del Comercio. (1998). *Programa de trabajo sobre el Comercio Electrónico* (WT/L/274). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/WT/L/274.pdf&Open=True

Ortego Ruiz, M. (2015). *Prestadores de servicios de internet y alojamiento de contenidos ilícitos.* Editorial Reus.

(2020). *Sin miedo al Derecho a la protección de datos y derechos digitales* (2da ed.). Siglo XXII Legal.

Palao Moreno, G. (2017). Otros contratos. En C. Esplugues Mota (coord.), *Derecho del Comercio Internacional* (pp. 251-274). Tirant lo Blanch.

Peguera Poch, M. (2010). Sobre la necesidad de revisar el marco legal de exclusión de responsabilidad de los proveedores de servicios de intermediación. En L. Cotino Hueso, (ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (pp. 256-268). Publicaciones de la Universidad de Valencia.

Rauchegger, C., & Kuczerawy, A. (2020). Injunctions to remove illegal online content under the eCommerce Directive: Glawischnig-Piesczek. *Common Market Law Review*, *57*(5), 1495-1526. https://dx.doi.org/10.2139/ssrn.3728597

Rosati, E. (2019). Material, Personal and Geographic Scope of Online Intermediaries' Removal Obligations beyond Glawischnig-Piesczek,

C-18/18 and Defamation. *European Intellectual Property Review*, *41*(11), 672-682.

Soldevila Fragoso, S. (2021). La ley de servicios digitales: necesaria y polémica. *Actualidad Administrativa,* (3), 1-8.

Teruel Lozano, G.M. (2010). Apuntes generales sobre la libertad de expresión en internet. *Anales de derecho,* (28), 121-140.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Caso C-131/12, Google Spain S.L. & Google Inc. c. Agencia Española de Protección de Datos (AEPD) & Costeja González, ECLI:EU:C:2014:317 (may. 13, 2014).

Caso C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland Ltd, Conclusiones del Abogado General Sr. Maciej Szpunar, ECLI:EU:C:2019:458 (jun. 4, 2019).

Caso C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland Ltd, ECLI:EU:C:2019:821 (oct. 3, 2019).

Caso C-238/08, Google France SARL. c. Louis Vutton Malletier SA *et al.*, 2010 E.C.R. I-02417.

Caso C-324/09, L'Oréal SA *et al*. c. eBay International AG *et al*., 2011 E.C.R. I-06011.

Caso C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV, ECLI:EU:C:2012:85 (feb. 16, 2012).

Casos acumulados C-509/09 & C-161/10, eDate Advertising GmbH *et al.* c. X & Société MGN Ltd., 2011 E.C.R. I-10269.

Casos acumulados C-682/18 & C-683/18, Frank Peterson c. Google LLC *et al.*, Elsevier Inc. c. Cyando AG, Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe, ECLI:EU:C:2020:586 (jul. 16, 2020).

Delfi AS c. Estonia, Ap. No. 64569/09, Eur. Ct. H.R (2015).

Digital Millennium Copyright Act, H.R. 2281, 105th Cong. (1998).

Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 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), 2000 O.J. (L 178) 1.

Directiva 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, 2019 O.J. (L 130) 92.

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM (2020) 842 final (dic. 15, 2020).

Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea, COM (2018) 640 final (sept. 12, 2018).

Reglamento 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (refundición), 2012 O.J. (L 351) 1 (UE).