



Plataformas digitales y derechos de la personalidad

Digital platforms and personality rights

[FERNANDO CARBAJO CASCÓN](#) 

Catedrático de Derecho Mercantil
Universidad de Salamanca

Abstract

Algunos tipos de plataformas digitales, como las redes sociales, facilitan el encuentro e intercambio de opiniones, informaciones y contenidos entre usuarios que, con frecuencia, pueden vulnerar derechos de la personalidad de terceros, afectando a su privacidad. En su condición de intermediarios en línea las plataformas se benefician en la UE de un régimen de exención de responsabilidad frente a los daños que a terceros pueden causar las actividades, informaciones o contenidos compartidos por los usuarios de su servicio, siempre que se den ciertos y cumplan con los deberes de diligencia debida establecidos en el Reglamento de Servicios Digitales de 2022. De no cumplirse esas condiciones podrán resultar responsables de vulneraciones a los derechos de la personalidad o datos personales de terceros cometidas por los usuarios de su servicio de plataforma.

Some types of digital platforms, such as social networks, facilitate the meeting and exchange of opinions, information and content between users, which can often infringe the personality rights of third parties, affecting their privacy. As online intermediaries, platforms benefit in the EU from a regime of exemption from liability for damage that may be caused to third parties by activities, information or content shared by users of their service, provided that the due diligence duties set out in the Digital Services Regulation 2022 are met and complied with. Failure to comply with these conditions may make them liable for infringements of the personal rights or personal data of third parties committed by users of their platform service.



Keywords: Plataformas digitales; Privacidad; Derechos de la personalidad; Datos personales; Responsabilidad de intermediarios en línea; Puerto seguro

Summary: [1. Planteamiento del problema.](#) – [2. Concepto y tipos de servicios en línea.](#) – [3. Régimen de responsabilidad de los servicios de plataforma en línea.](#) – [3.1. Los precedentes: el régimen de puerto seguro establecido en la Directiva 2000/31/CE, de comercio electrónico.](#) – [3.2. La interpretación del requisito del conocimiento efectivo por el Tribunal Supremo español.](#) – [3.3. La interpretación del Tribunal de Justicia de la UE sobre el alcance de las reglas de puerto seguro.](#) – [3.4. Ponderación de derechos e intereses por parte del intermediario en línea a la hora de cumplir con su deber de reacción diligente en la retirada de contenidos infractores de derechos de la personalidad de terceros.](#) – [4. El régimen de responsabilidad de los intermediarios en línea en el reglamento de servicios digitales de la unión europea.](#) – [4.1. Las reglas de exención de responsabilidad de intermediarios de alojamiento de datos en el Reglamento \(UE\) de Servicios Digitales.](#) – [4.2. Obligaciones de diligencia debida de los prestadores de servicios de alojamiento de datos, en particular plataformas en línea de comercio electrónico.](#) – [5. Naturaleza de la responsabilidad de los intermediarios en línea. En particular, su posible responsabilidad por intromisiones en la privacidad.](#) – [5.1. Consideraciones previas sobre la clase de responsabilidad imputable a las plataformas digitales.](#) – [5.2. La responsabilidad aplicable a las plataformas digitales en casos de intromisiones en la privacidad.](#)

1. Planteamiento del problema.¹

Internet permite a millones de usuarios acceder a todo tipo de contenidos, interactuar entre sí y generar contenidos propios o información en general ("*user-generated contents*") que comparten con el resto de internautas a través de diferentes tipos de aplicaciones y servicios en línea; desde páginas web, blogs o diarios y revistas digitales que generan y ofrecen información dejando espacio para los comentarios de los usuarios en foros de opinión, a grupos de chats (Whatsapp, Telegram) y redes sociales de distinta naturaleza (Facebook/Meta, Twitter/X, Instagram), pasando por servicios que agregan información generada por los usuarios (webs de enlaces) o que permiten compartir vídeos u otros contenidos (YouTube, Twitch, TikTok).

Estos servicios en línea han transformado radicalmente la forma en que las personas obtienen, suministran y comparten contenidos e información, opinan, comentan e interactúan entre sí, hasta el punto de crear y consolidar un nuevo contexto social y económico que identificamos como Sociedad de la Información, Sociedad Conectada o Sociedad Digital. La Red ofrece grandes oportunidades de negocio, consumo e interacción social, pero genera también

¹ El autor es Investigador Principal 1 del Proyecto de Investigación que lleva por título "Marco regulador de las plataformas en línea en la economía digital: competencia y responsabilidad en el uso de datos y contenidos (PID2020-119002RB-I00), financiado por el Ministerio de Ciencia e Innovación en el marco de los programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico del sistema de i+d+i y de i+d+i orientada a los retos de la sociedad, para el periodo 1 de septiembre de 2021 a 31 de agosto de 2024.

grandes riesgos al constituir un cauce para realizar actividades ilícitas y comentarios lesivos de derechos de diferente naturaleza: derechos de marca, derechos de autor y derechos conexos, derechos sobre los datos personales o derechos de la personalidad (intimidad, honor y propia imagen), entre otros.

Internet ha supuesto así un paso de gigante para la democratización de la información, maximizando las libertades de expresión e información, al permitir a los usuarios acceder con facilidad a información plural, generar información por sí mismos y compartirla expresando sus opiniones libremente. Tan libremente -y sin pudor alguno en muchas ocasiones- que se ha convertido en un fenómeno habitual la utilización ilegítima de datos personales e imágenes para el insulto o la difamación a personas públicas (políticos, periodistas, deportistas, artistas, etc.) y privadas, atentando contra su honor, intimidad o imagen.

En este contexto debe analizarse cuidadosamente la posición que ocupan los servicios en línea cuando sus responsables y/o sus usuarios vulneran derechos de terceros en los contenidos e informaciones que generan y comparten entre sí; especialmente la posición de aquellos servicios en línea mixtos o híbridos que además de generar sus propios contenidos actúan como intermediarios en línea al permitir a los usuarios mostrar sus pareceres y comentarios en foros de opinión (diarios y revistas digitales), así como la de los servicios de intermediación puros que permiten a los usuarios interactuar entre sí compartiendo información y contenidos de muy diferente naturaleza (agregadores de información, redes sociales y servicios de compartición en línea).

Es claro que los servicios en línea que proveen y suministran contenidos o cualquier tipo de información generada por ellos mismos serán responsables -por hecho propio o por hecho ajeno, ex artículos 1902 y 1903 CC- de las posibles infracciones de derechos de terceros que puedan producirse con motivo de su actividad; entre ellas las intromisiones ilegítimas en la intimidad, el honor o a la propia imagen (cfr. artículo 18 CE y LO 1/1982, de 5 de mayo) o la utilización no autorizada de datos personales. Igualmente serán responsables directos por infringir derechos de terceros los usuarios (internautas) que generen o compartan contenidos ilícitos o que realicen comentarios atentatorios contra los derechos de la personalidad en cualquier servicio en línea del que sean titulares o usuarios, siempre que se les pueda identificar adecuadamente.

Pero cuando esos contenidos o informaciones son generados o compartidos por usuarios que recurren a servicios de intermediación en línea híbridos o puros para suministrarlos o compartirlos surgen dificultades inherentes a las propias características de la Red: la dificultad para identificar a usuarios que permanecen en el anonimato o que se esconden tras un alias o "*nick-name*" y la naturaleza de intermediarios de los servicios en línea que permiten a los usuarios compartir información. En estas situaciones es cuando se plantea la posición que deben ocupar los intermediarios en línea que facilitan a los usuarios el servicio técnico para llevar a cabo el intercambio de contenidos y de información que vulnera derechos de terceros: ¿Han de quedar exentos de toda responsabilidad por contenidos o informaciones generadas y compartidas por usuarios sobre los que no tienen ningún tipo de control? ¿O se les puede considerar responsables por las infracciones de derechos de terceros realizadas

por los usuarios de su servicio si no despliegan una diligencia mínima para identificar y retirar los contenidos o informaciones infractores?

El anonimato es uno de los pilares de Internet y uno de los grandes atractivos para los usuarios a la hora de generar contenidos y expresar sus opiniones y comentarios; y está amparado legalmente en la medida en que los operadores de redes de comunicaciones y los proveedores de servicios en línea únicamente estarían obligados a revelar la identidad de los usuarios de sus servicios cuando medie un requerimiento judicial y solamente en casos de detección, investigación y enjuiciamiento de delitos graves (cfr. Ley 25/2007, de 18 de octubre, de conservación de los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que incorpora la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006), toda vez que los datos de las comunicaciones electrónicas se consideran datos de carácter personal que permiten extraer conclusiones sobre la vida de las personas^{2/3}.

Ante esta perspectiva los perjudicados por el suministro de contenidos ilegales o por comentarios o informaciones difamatorios tienen que dirigirse contra los servicios en línea que permiten visibilizar y compartir esos contenidos e informaciones generados por los usuarios de esos servicios que atentan contra sus derechos, bien para solicitar la retirada de esos contenidos o comentarios o bien para exigir responsabilidad por los daños y perjuicios sufridos si los intermediarios no realizan una actuación diligente para retirarlos. Incluso pueden preferir dirigirse contra los servicios en línea, aun cuando pudieran identificar a los usuarios responsables de los contenidos e informaciones infractores de sus derechos⁴, por simples razones de economía procesal (la imposibilidad o poca eficacia práctica de dirigirse contra múltiples infractores y las dudas sobre su solvencia)⁵.

² STJUE (Gran Sala), de 21 de diciembre de 2016 (Asuntos acumulados C-203/15 y C-698/15, "Tele2 Sverige y Watson y otros", ap. 99); y STJUE (Gran Sala) de 8 de abril de 2014 (Asuntos acumulados C-293/12 y C-594/12, "Digital Rights Ireland y Seitlinger y otros", ap. 27).

³ Aunque el TJUE consideró nula la Directiva 2006/24/CE al considerar que la Directiva e-Privacy, y en especial su artículo 15, se opone (como norma general) a medidas legislativas que establezcan, para la prevención, la investigación, el descubrimiento y la persecución de delitos, la conservación generalizada e indiferenciada, con carácter preventivo, de los datos de comunicaciones electrónicas, admitiendo no obstante que las legislaciones nacionales promulgadas para incorporar esa Directiva pueden resultar válidas y eficaces siempre que cumplan el requisito de proporcionalidad, estableciendo reglas claras y precisas sobre el alcance de la conservación de datos y comunicaciones e impongan unas exigencias mínimas en relación con las circunstancias y requisitos que debe cumplir una medida para el tratamiento de datos personales. Sin embargo, el Tribunal Supremo español ha afirmado la plena vigencia y aplicación de la Ley 25/2007, de 18 de octubre, poniendo de manifiesto que recoge la exigencia de autorización judicial previa (artículo 6.1) para acceder a datos personales conservados por los operadores de redes de comunicaciones que no se contemplaba en la Directiva. Vid. POLO ROCA, A., "La regulación sobre la conservación de datos en las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión", IDP-Revista de Internet, Derecho y Política, nº 33, octubre de 2021, accesible en <https://idp.uoc.edu>.

⁴ El Tribunal de Justicia de la UE considera que la Directiva 2006/24 no excluye una normativa nacional como la basada en el artículo 8 de la Directiva 2004/48 del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, que, a efectos de la identificación de un abonado a Internet o de un usuario de Internet, permite que se requiera judicialmente a un proveedor de acceso a Internet para que comunique al titular de un derecho de autor la identidad del abonado a quien se ha asignado una determinada dirección IP que supuestamente ha servido para la vulneración de dicho derecho, al ser una materia ajena al ámbito de aplicación "*ratione materiae*" de la Directiva 2006/24. Cfr. STJUE de 19 de abril de 2012 (Asunto C-461/10, "Bonnier Audio").

⁵ Vid. JULIÀ BARCELÓ, R., "Liability for Online-Intermediaries: A European Perspective", EIPR, 1998/12, p. 454.

Surgen importantes dudas, en particular, sobre la posición que tienen los servicios de intermediación en línea, especialmente aquellos que prestan servicios de alojamiento de datos ("*hosting*") o servicios de búsqueda y enlace ("*searching & linking*") al facilitar a los usuarios compartir contenidos e informaciones de distinta naturaleza, incluyendo datos e informaciones de carácter personal de terceros, ante posibles requerimientos y demandas de quienes resultan afectados por el uso indebido de datos personales o por intromisiones en su intimidad, su honor o su propia imagen⁶.

2. Concepto y tipos de servicios en línea.

La legislación española (Anexo de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico; LSSICE), que trae razón de la legislación comunitaria europea (Directiva 2000/31/CE, de 8 de junio, 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; DCE) ofrece un concepto claro de servicios de la sociedad de la información y de los servicios de intermediación: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, comprendiendo también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios^{7/8}.

Los servicios de intermediación se configuran como una especie dentro del género de los servicios de la sociedad de la información, definiéndolos el mentado Anexo LSSICE 2002 como aquellos servicios de la sociedad de la información por los que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. De modo que un servicio de intermediación se convierte en pieza clave para utilizar cualesquiera otros servicios de la sociedad de la información. Se incluyen entre ellos los servicios de acceso a Internet ("*Internet Service Providers*"), los servicios de transmisión de datos por redes de telecomunicaciones ("*mere conduit*" o

⁶ Vid. VAN DER SLOOT, B., "Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations en Europe", JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, accesible en <https://www.jipitec.eu/issues/jipitec-6-3-2015/4318>. Vid. también, LÓPEZ RICHARD, J., "Difamación en la Web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", Derecho Privado y Constitución, nº 26, enero-diciembre 2012, pp. 143-201 (cfr. pp. 147-148).

⁷ La misma definición, con mayores explicaciones, se contiene en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo: Todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios; entendiéndose por servicio "a distancia" un servicio prestado sin que las partes estén presentes simultáneamente, "por vía electrónica" un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, y "a petición individual de un destinatario de servicios" un servicio prestado mediante transmisión de datos a petición individual (cfr. artículo 1.1 letra b).

⁸ Entre ellos se incluyen los servicios de contratación de bienes o servicios por vía electrónica (servicios de comercio electrónico); la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales; la gestión de compras en la red por grupos de personas; el envío de comunicaciones comerciales; los servicios de suministro de información por vía telemática; el vídeo bajo demanda, como servicio en que el usuario pueda seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

"*routing*"), los servicios que ofrecen la realización de copia temporal de las páginas de Internet solicitadas por los usuarios ("*system caching*" o memoria tampón), los servicios de alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por terceros ("*hosting*") y los servicios que ofrecen instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet ("*searching & linking*").

Dentro de los servicios de intermediación en línea, los llamados "*Servicios de Plataforma*" son servicios de alojamiento o almacenamiento de datos (servicios de "*hosting*" 2.0). Estos intermediarios en línea responsables de los servicios de plataforma se han convertido en actores fundamentales del mercado y de la sociedad digitales, actuando en ocasiones como auténticos prestadores de servicios de intermediación en línea y en otras como generadores de sus propios contenidos o distribuidores de sus propias mercancías o servicios (plataformas híbridas o mixtas).

En esta línea, como una evolución del concepto básico de servicios de intermediación en línea, en el nuevo Reglamento (UE) 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales, RSD, de aplicación a partir del 17 de febrero de 2024), se contemplan de forma específica las "plataformas en línea" como una subespecie de los servicios intermediarios del tipo o modalidad "*hosting*", definiéndolas en su artículo 3 letra i) como prestadores de servicios de alojamiento de datos que, a petición de un destinatario del servicio, almacenan y difunden al público información, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento.

De forma similar, el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales; RMD)⁹, establece en su artículo 2.2 que el "servicio básico de plataforma" hace referencia a cualquiera de los siguientes elementos: *a)* servicios de intermediación en línea; *b)* motores de búsqueda en línea; *c)* servicios de redes sociales en línea; *d)* servicios de plataformas de intercambio de vídeos; *e)* servicios de comunicaciones interpersonales independientes de numeración; *f)*

⁹ En los mercados digitales los efectos de red directos e indirectos propios de los "*multi-side-markets*" creados en torno a las plataformas digitales (que sirven como punto de encuentro entre usuarios, entre éstos y los anunciantes, y entre oferentes y demandantes de productos y servicios), generan un efecto conocido como "*winner takes it all*" ("el ganador se lleva la mayoría") que favorece la adquisición de un importante poder de mercado por parte de algunas de estas plataformas hasta convertirlas en auténticos guardianes de acceso al mercado digital ("*Gatekeepers*"), circunstancia que ha forzado una regulación "*ex ante*" para frenar el excesivo poder de mercado de estas plataformas y garantizar así la equidad y disputabilidad de los mercados, por medio del nuevo Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). Vid. RUIZ PERIS, J.I. (Dir.), *Competencia, compensación de daños y mercados digitales*, Tirant lo Blanch, Valencia, 2022.

sistemas operativos; g) navegadores web; h) asistentes virtuales; i) servicios de computación en la nube; j) servicios de publicidad, incluidas las redes de publicidad, los intercambios publicitarios y cualquier otro sistema de intermediación publicitaria, prestados por una empresa que preste cualquiera de los servicios básicos de plataforma enumerados en las letras a) a i). Servicios de plataforma que tendrán la consideración de guardianes de acceso si cumplen con los requisitos o condiciones establecidos al efecto en el artículo 3 RMD.

En el presente estudio nos centraremos en la actividad de las plataformas digitales que ofrecen con carácter principal o accesorio un servicio de intermediación puro o mixto que facilita el intercambio de contenidos o todo tipo de opiniones e informaciones entre los usuarios de su servicio, incluyendo -en particular- los servicios de redes sociales.

3. Régimen de responsabilidad de los servicios de plataforma en línea.

Para poder abordar con claridad y garantías el régimen de responsabilidad de las plataformas digitales por posibles infracciones a la intimidad, el honor y la propia imagen de terceros, es preciso hacer un rápido recorrido por la normativa relativa a la responsabilidad o no responsabilidad de los servicios de intermediación en la sociedad de la información. Esto es, por el régimen general de exención de responsabilidad de los intermediarios en línea o normas de puerto seguro ("*safe harbour*"), tal y como fue regulada en la Directiva 2000/31 de Comercio Electrónico (DCE) y en la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE) e interpretada por el Tribunal Supremo y el Tribunal de Justicia de la Unión Europea.

La regla general es que los prestadores de servicios de la sociedad de la información, incluidos los servicios de intermediación en línea, están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de las reglas especiales de exención de responsabilidad previstas para los intermediarios en línea (cfr. artículo 13 LSSICE).

3.1. Los precedentes: el régimen de puerto seguro establecido en la Directiva 2000/31/CE, de comercio electrónico.

El artículo 14 de la Directiva 2000/31/CE, sobre servicios de la sociedad de la información, en particular el comercio electrónico ("Alojamiento de datos"), norma incorporada en el artículo 16 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico ("Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos"), establece las bases del beneficio de la exención de responsabilidad o puerto seguro para los servicios de intermediación consistentes en el almacenamiento de datos, disponiendo que el prestador de servicios no puede ser considerado responsable por los datos almacenados a petición de los destinatarios de su servicio a condición de que:

a) No tenga conocimiento efectivo de que la actividad o la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga

conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que;

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

c) La exención no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios.

El Considerando nº 42 de la Directiva 2000/31 aclara que las exenciones de responsabilidad establecidas en la presente Directiva sólo se aplican a aquellos casos en que la actividad del prestador de servicios de la sociedad de la información se limita al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros es transmitida o almacenada temporalmente, con el fin de hacer que la transmisión sea más eficiente. Esa actividad es de naturaleza meramente técnica, automática y pasiva, lo que implica que el prestador de servicios de la sociedad de la información no tenga conocimiento ni control de la información transmitida o almacenada. Este considerando actúa como pauta interpretativa del régimen de exención de responsabilidad de los intermediarios, y aunque inicialmente se previó aparentemente para los servicios de "routing" y "caching" de los proveedores de acceso a Internet (ISPs), el TS y el TJUE la extendieron más tarde a los servicios de "hosting 2.0" con los que se identifican los servicios de motores de búsqueda y las plataformas en línea de comercio electrónico.

El legislador español decidió ampliar el régimen de exención de responsabilidad a otra categoría de intermediarios: los prestadores de servicios de búsqueda y enlaces, disponiendo el artículo 17 LSSICE ("Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda") que este tipo de intermediarios no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

c) La exención de responsabilidad no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos

Es decir el legislador español establece un régimen de exención de responsabilidad común para los servicios de alojamiento de datos y de búsqueda y enlace, por más que los motores de búsqueda y los servicios que facilitan enlaces a otros sitios en línea actúan en realidad como servicios de alojamiento de datos "*lato sensu*"¹⁰.

¹⁰ Vid. CLEMENTE MEORO, M., "La responsabilidad civil de los prestadores de servicios de la sociedad de la información", en Clemente Meoro, M./Cavanillas Múgica, S. (Dirs.), *Responsabilidad civil y contratos en Internet. Su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Comares, Granada, 2003, pp. 1-116; APARICIO VAQUERO, J.P., "El nuevo régimen de prestación de servicios de la sociedad de la información", *Revista de Derecho y Nuevas Tecnologías*, 2003, núm. 2, pp. 87-111; PEGUERA POCH, M., *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Granada, 2007; y BUSTO LAGO, J.M., "La responsabilidad civil de los prestadores de servicios de la sociedad de la información

Ambas reglas se complementan con lo dispuesto en el artículo 15 de la misma Directiva 2000/31, que establece la inexistencia de una obligación general de supervisión para todos los servicios de intermediación ("*routing*", "*caching*" y "*hosting*"), disponiendo que los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar "*ex ante*" los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas. Esta regla general no impedirá, sin embargo, que un intermediario en línea pueda quedar sujeto a obligaciones de supervisión "*ex post*" ante reclamaciones dirigidas por terceros por contenidos o informaciones suministrados por los usuarios de su servicio.

El principal problema para delimitar la responsabilidad del intermediario de servicios de alojamiento reside en establecer qué debe entenderse por "conocimiento efectivo" de la ilicitud de los datos almacenados en su sistema. Conforme al tenor de la norma, no bastaría la mera sospecha de la actividad ilícita o un conocimiento abstracto de la posibilidad de que se estén lesionando bienes o derechos de terceros, sino que ha de ser un conocimiento actual, real o, como dice la Ley, "efectivo". Para intentar clarificar el alcance de este requisito, que se establece como regla básica para la exención de responsabilidad en ambos casos, el legislador español decidió ir más lejos de lo establecido en la DCE, indicando que se entenderá que el prestador de servicios de intermediación tiene el conocimiento efectivo de que determinada actividad o información incluida en su servicio por algún usuario es ilícita cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Esta precisión sobre el alcance del requisito del conocimiento efectivo resultaba sumamente favorable para los prestadores de servicios de intermediación consistentes en el alojamiento de datos y de búsqueda de información y suministro de enlaces, ya que prácticamente les exime de todo tipo de diligencia en la identificación y retirada de información, contenidos o actividades compartida por los usuarios de su servicio que pueden vulnerar derechos de terceros salvo cuando tengan conocimiento por cualquier medio de que esa información, contenidos o actividades ha sido declarada ilícita por una resolución administrativa o sentencia judicial firmes.

No obstante, parece sugerirse que los servicios de intermediación tipo "*hosting*" y "*searching & linking*" pueden trabar conocimiento efectivo de posibles informaciones, contenidos o actividades ilícitos dentro de su plataforma o servicio de intermediación en línea si implementan procedimientos de detección y retirada ("*notice & take down*"). De modo que en el régimen de puerto seguro establecido en la DCE y LSSICE para los intermediarios de la sociedad de la información la implementación de estos servicios o procedimientos de denuncia y retirada tiene carácter meramente

(ISPs)", en Reglero Campos, L.F. (Dir.), *Tratado de Responsabilidad Civil*, T. II, Thomson-Aranzadi, Navarra, 2003, pp. 971 y ss., especialmente pp. 995 y ss.

voluntario, fruto de la autorregulación de los servicios de intermediación o con motivo de compromisos adquiridos en códigos de conducta generales o sectoriales. Con todo, su efectiva implementación lógicamente puede variar las condiciones establecidas sobre el alcance del conocimiento efectivo, pues se sugiere (“sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse”) que si los intermediarios tuvieran conocimiento de actos, contenidos o informaciones ilícitas subidos y compartidos por los usuarios de servicio en línea a través de estos procedimientos técnicos de detección voluntariamente implementados estarían obligados a satisfacer el segundo requisito para exonerar su responsabilidad: reaccionar diligentemente para retirar esa información (incluyendo la retirada de enlaces) o impedir el acceso a la misma a los usuarios de su servicio, sin tener que esperar ya al conocimiento por cualquier medio de la existencia de una resolución administrativa o sentencia judicial firmes.

La Ley menciona que pueden establecerse “otros medios de conocimiento efectivo”. Este último inciso actúa como cláusula de cierre de todo el sistema de responsabilidad, ya que pretende dar legitimidad a cualquier otra práctica que permita probar que el proveedor de alojamiento conocía (o debía conocer sin faltar a la buena fe) la ilicitud de los contenidos, actividades o informaciones que albergaban sus servidores. El supuesto paradigmático es la denuncia de la existencia de tales contenidos por parte de los afectados, aunque también puede considerarse el conocimiento público de la más que presunta ilicitud de determinadas informaciones alojadas en un determinado servidor (evidentes muchas veces en el caso de comentarios injuriosos, violaciones palmarias de la privacidad o ilícitos manifiestos contra derechos de autor y conexos o derechos de marcas y diseños industriales).

3.2. La interpretación del requisito del conocimiento efectivo por el Tribunal Supremo español.

La interpretación tan restrictiva del requisito del “conocimiento efectivo” realizada por el legislador español en los artículos 16 y 17 LSSICE, yendo más allá de lo previsto en la DCE, consagraba en la práctica un régimen de impunidad para los intermediarios de la sociedad de la información por las actividades o informaciones ilícitas de los usuarios de su servicio, con el consiguiente trastorno y -en algunos casos- indefensión para los titulares de derechos flagrante y masivamente vulnerados a través de esos servicios de agregación.

Sin embargo, esta interpretación tan restrictiva resultó corregida por la Sala Primera del Tribunal Supremo cuando en su Sentencia de 9 de diciembre de 2009 (caso “putasgae”), en un caso de infracción del derecho al honor de una persona jurídica, señaló que una interpretación tan restrictiva del “conocimiento efectivo” por parte del prestador de servicios de “hosting” no es conforme con la Directiva de Comercio Electrónico (cfr., Considerando nº 42 y artículo 14.1), “ya que reduce injustificadamente las posibilidades de obtención del “conocimiento efectivo” de la ilicitud de los contenidos almacenados y amplía correlativamente el ámbito de la exención, en relación con los términos de la

norma armonizadora, que exige un efectivo conocimiento, pero sin restringir los instrumentos aptos para alcanzarlo”.

El TS realizó así una lectura del artículo 16.1 LSSICE (extensible al artículo 17 LSSICE) conforme al espíritu y finalidad de la DCE, la cual persigue un equilibrio adecuado entre la seguridad jurídica que necesitan los intermediarios de la sociedad de la información y el respeto a la libertad de expresión e información con la adecuada tutela de terceros que se puedan ver afectados por el uso que se haga de los servicios de esos intermediarios, permitiendo formas más flexibles de obtención del conocimiento efectivo de la ilicitud.

Concluyó entonces el Alto Tribunal ratificando la necesidad de una interpretación más flexible de las posibles formas de obtener el conocimiento efectivo por parte de los prestadores de servicios de alojamiento (y, por extensión, de los prestadores de servicios de enlaces a contenidos e instrumentos de búsqueda), apuntando al respecto que *“(A)demás de que el propio artículo 16 permite esa interpretación favorable a la Directiva -al dejar a salvo la posibilidad de “otros medios de conocimiento efectivo que pudieran establecerse”-, no cabe prescindir de que la misma atribuye igual valor que al “conocimiento efectivo” a aquel que se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate”.*

Esta doctrina fue reiterada posteriormente por el Alto tribunal en casos similares de responsabilidad de intermediarios por actos de sus usuarios que suponen una intromisión en la intimidad, el honor o la propia imagen de terceros, en las SSTs (Civil) de 18 de mayo de 2010 (caso “quejasonline.com”)¹¹, 10 de febrero de 2011 (caso “alabarricadas.com”, 26 de febrero de 2013 (caso “Ramoncín”) y 5 de mayo de 2016 (caso “Izquierda Unida”).

Por lo que se refiere al segundo requisito de exención de la responsabilidad de los intermediarios de la sociedad de la información, la STS de 18 de mayo de 2010 (caso “quejasonline.com”) viene a reconocer que su valoración debe realizarse *“ad hoc”*, a la luz de las circunstancias concurrentes en el caso concreto en torno a la mayor o menor diligencia del intermediario para, una vez detectada la información o actividad infractora, valorar la procedencia o improcedencia de su retirada o bloqueo de acceso. Es este precisamente el principal problema al que se deben enfrentar los intermediarios en línea cuando detecten por cualquier medio la existencia de actividades, contenidos o informaciones compartidos por los usuarios de su servicio que infringen derechos de terceros; muy particularmente en el caso de intromisiones ilegítimas en los derechos a la intimidad, al honor o la propia imagen: la decisión de si procede o no la retirada de ese contenido, actividad o información, pues ello exige que realicen una valoración de los distintos derechos en juego, por una parte los legítimos derechos de propiedad intelectual o derechos de la personalidad de los terceros afectados y por otra parte los también legítimos derechos a la libertad de expresión e información y de acceso a la información de los usuarios de su servicio de intermediación en línea.

¹¹ Vid. el comentario de RUBÍ PUIG, A., “Derecho al honor online y responsabilidad civil de ISPs”, Indret.com, octubre 2010.

El problema de fondo reside en que la reacción diligente del intermediario para retirar actividades, contenidos o informaciones ilícitas de su plataforma en línea de las que tenga conocimiento por cualquier medio y evitar así cualquier tipo de responsabilidad por algo que realmente realizan los usuarios de su servicio, genera el riesgo de precipitación que puede desembocar en la vulneración de los derechos de sus usuarios y, con ello, de posibles demandas por infracción de los derechos constitucionales a la libertad de expresión e información o el legítimo acceso a la información (cfr. artículos 18 y 44 CE), así como de las propias reglas del contrato de prestación del servicio.

El Tribunal Supremo ha ratificado su doctrina sobre la interpretación más flexible del requisito del conocimiento efectivo en la STS 235/2020, de 2 de junio (caso "meneame.com"), relativo a infracción del derecho al honor en comentarios que contienen expresiones insultantes a partir de una información subida por un usuario (en forma de enlace) sobre un determinado cargo político. Considera el Alto Tribunal que el servicio de intermediación (web de enlaces de prensa compartidos por los usuarios) tuvo conocimiento efectivo de las expresiones injuriosas incluidas en un foro de opiniones a partir de la denuncia efectuada por el afectado a través de un correo ordinario y un burofax, sin que hubiera una reacción diligente del intermediario para retirar esa información o bloquear su acceso desde la plataforma.

En respuesta al recurso de amparo formulado por el responsable del servicio de intermediación planteando un conflicto entre la protección del derecho al honor y la libertad de expresión e información, el Tribunal Constitucional responde en su STC 83/2023, de 4 de julio (caso "meneame.com") que el requisito del conocimiento efectivo puede y debe interpretarse en sentido amplio (pudiendo obtenerse a través de cualquier método idóneo) para conjugar adecuadamente los distintos intereses y derechos involucrados, concluyendo que no se produce una lesión del derecho a la tutela judicial efectiva (artículo 24 CE) ni a la libertad de expresión e información (artículo 20 CE) por el hecho de interpretar en sentido amplio dicho requisito del conocimiento efectivo.

3.3. La interpretación del Tribunal de Justicia de la UE sobre el alcance de las reglas de puerto seguro.

Primero en la STJUE (Gran Sala) de 23 de marzo de 2010 (Asuntos acumulados C-236/08 a C-238/08, "Google France"), y más tarde en la STJUE (Gran Sala) de 12 de julio de 2011 (Asunto C-324/09, "L'Oréal c. eBay UK"), el Tribunal de Justicia de la UE puso las bases de la interpretación de las reglas de puerto seguro de los intermediarios de la sociedad de la información¹². Aunque se trata de sentencias dictadas en materia de infracciones marcarias, dado el carácter horizontal del régimen de puertos seguros en materia de exención de responsabilidad de los intermediarios en línea, la doctrina del TJUE se puede

¹² Vid. DE MIGUEL ASENSIO, P.A., "Comercio electrónico y protección de marcas: Aspectos internacionales", en AA.VV., *Problemas actuales de derecho de la propiedad industrial (VIII Jornadas de Barcelona de Derecho de Propiedad Industrial)*, Tecnos, Madrid, 2018, pp. 17-63. Vid. también CARBAJO CASCÓN, F., "Las plataformas digitales ante la distribución de mercancías y el suministro de contenidos digitales ilícitos", *Revista de Derecho de la Competencia y de la Distribución*, nº 30, enero-junio 2022, pp. 7 y ss.

considerar aplicable a cualquier otro tipo de responsabilidad que pudiera imputarse a los usuarios de los servicios de intermediación de la modalidad de alojamiento de datos o “hosting”, pues el Tribunal aclara de antemano que los motores de búsqueda fungen realmente como servicios de alojamiento de datos al proporcionar información mediante enlaces a sus usuarios.

Según el TJUE los prestadores de servicios de alojamiento de información no responderán por los actos de sus usuarios siempre que:

a) Actúen de forma neutral, automática y pasiva, y;

b) cuando tengan conocimiento por cualquier medio de una información o acto ilícito, reaccionen diligentemente para retirar la información ilícita o inhabilitar el acceso a la misma.

Expresado en sentido inverso, como excepción a la regla general que establece la exención de responsabilidad de los intermediarios en línea, los prestadores de servicios de alojamiento de información serán responsables de los actos cometidos por los usuarios de su servicio:

a) cuando no actúen de forma neutral, automática y pasiva, desempeñando un papel activo que les permita tener conocimiento, por cualquier medio, de los datos e informaciones ilícitos de sus usuarios y les presten asistencia para optimizar y promover la presentación y oferta de sus productos, servicios o contenidos, o;

b) cuando actuando de forma neutral, automática y pasiva tengan conocimiento efectivo por cualquier medio de infracciones a derechos de terceros cometidas por los usuarios de su servicio y no actúen con prontitud para retirar la información o imposibilitar el acceso a los mismos.

En definitiva, el TJUE deja claro que las reglas de puerto seguro sólo se aplicarán a los prestadores de servicios de alojamiento de información cuando actúen como intermediarios puros, siendo su actuación neutral, automática y pasiva en relación con las informaciones almacenadas por los usuarios de su servicio. Y establece asimismo el alcance del principio de reacción diligente en el caso de esas actuaciones como verdaderos intermediarios, señalando que la exención de responsabilidad sólo tendrá lugar si reaccionan con prontitud para retirar información ilícita de su plataforma cuando tengan conocimiento por cualquier medio de su existencia.

Para evitar interpretaciones excesivamente restrictivas de qué debe entenderse por “conocimiento efectivo”, el Tribunal señala que para retirar el beneficio de la exención de responsabilidad bastará con que el intermediario haya tenido conocimiento “por cualquier medio” (incluidas reclamaciones de los titulares de derechos afectados en servicios de “notice & take down” implementados voluntariamente por la propia plataforma en línea) de hechos o circunstancias a partir de los cuales un operador económico diligente hubiera debido deducir ese carácter ilícito y actuar rápidamente para retirar los datos o impedir su acceso¹³. Así pues, para eludir el régimen de exoneración de responsabilidad de las plataformas digitales, será necesario acreditar que el intermediario conocía o al menos debería conocer sin faltar a la buena fe objetiva el carácter ilícito de las actividades o informaciones en cuya edición, promoción y difusión colabora y, a pesar de ello, no adoptó ninguna medida

¹³ Cfr. STJUE de 12 de julio de 2011, Asunto “eBay”, apartados 120 y 124.

para retirarlas de su plataforma. Pero no sólo eso, pues en la STJUE (Gran Sala) de 12 de julio de 2011 (Asunto C-324/09, "L'Oréal c. eBay Uk") el Tribunal aclara que la reacción diligente debería implicar no sólo la inmediata retirada de los datos o informaciones infractoras de derechos de terceros cuando el gestor del servicio de intermediación reciba un aviso o reclamación judicial o extrajudicial del titular de derechos afectado ("*notice & take down*"), sino también la adopción de medidas eficaces para evitar que esos datos o informaciones infractoras vuelvan a ser cargadas en la plataforma ("*notice & stay down*").

No siendo posible exigir una supervisión general "a priori" de la información que almacenan a los prestadores de servicios de alojamiento de datos, vedada por el artículo 15 de la Directiva 2000/31, se abre la puerta sin embargo a una supervisión particular "a posteriori" y "para casos específicos", cuando el intermediario tenga conocimiento por cualquier medio de la existencia de actos o informaciones que vulneran derechos de terceros; en particular, cuando reciban una comunicación o notificación motivada por parte de terceros afectados. El TJUE considera, en concreto, que es posible dirigir requerimientos efectivos y proporcionados a los operadores de mercados electrónicos para que, si éstos no deciden por sí mismos suspender la cuenta de quien vulneró los derechos de marca reclamados para evitar que el mismo usuario vuelva a cometer infracciones de esta naturaleza en relación con las mismas marcas, puedan ser obligados a ello mediante una orden judicial¹⁴.

El propio TJUE ratificó esta postura en su STJUE de 3 de octubre de 2019 (Asunto C-18/18, "Eva Glawischnig Piesctek v. Facebook"), en relación con infracciones al derecho al honor y a la intimidad, donde dispuso que la Directiva 2000/31/CE no se opone a que un Tribunal pueda obligar a un prestador de servicios de alojamiento de datos (en el caso una red social) a suprimir los datos que almacene, y cuyo contenido sea idéntico al de una información declarada ilícita con anterioridad, o a bloquear el acceso a ellos, sea quien fuere el autor de la solicitud de almacenamiento de tales datos. De esta forma, cuando un servicio de plataforma (o, más en general, un servicio de intermediación tipo "*hosting*") no reaccione con prontitud para retirar información que vulnera derechos de terceros, a petición de los perjudicados u obligado por un tribunal, podría resultar responsable ante una demanda de esos terceros en reclamación de daños y perjuicios¹⁵.

En particular esta relevante decisión del TJUE dispone que el artículo 15 DCE debe interpretarse en el sentido de que no se opone a que un tribunal de un Estado miembro pueda obligar a un prestador de servicios de alojamiento de datos a suprimir o bloquear: *i*) el acceso a datos o informaciones que almacene y cuyo contenido sea idéntico al de una información declarada ilícita con

¹⁴ Cfr. STJUE de 12 de julio de 2011, Asunto "eBay", apartado 141. Del mismo modo, es posible requerir al operador para que adopte medidas que faciliten la identificación de sus clientes vendedores, pues si bien es cierto que resulta necesario respetar la protección de datos personales, no lo es menos que, cuando el autor de la infracción actúa en el tráfico comercial y no en el ámbito de su esfera privada, debe ser claramente identificable, de acuerdo con la filosofía del artículo 6 de la Directiva 2000/31/CE (cfr. apartado 142). Vid. SCHRIJVERS M., "European Court Rules on the Position of eBay Regarding the Sale of Infringing Products: L'Oréal v eBay", EIPR, Vol. 33, nº 11, 2011, pp. 723-724.

¹⁵ Vid. un repaso a la jurisprudencia española en GONZÁLEZ SAN JUAN, J.L., "Jurisprudencia española sobre la protección del honor, la intimidad y la propia imagen en Internet", Ibersid, nº 9, 2015, pp. 83-88.

anterioridad; ii) siempre que la supervisión y la búsqueda de los datos a los que se refiera la medida cautelar judicial se limiten a aquellos que transmitan un mensaje cuyo contenido permanezca esencialmente inalterado con respecto al que dio lugar a la declaración de ilicitud y que contenga los elementos especificados en dicha medida, y en la medida en que las diferencias en la formulación de dicho contenido similar al que caracteriza a una información declarada ilícita con anterioridad no puedan obligar al prestador de servicios de alojamiento de datos a realizar una apreciación autónoma de ese contenido; iii) pudiendo extenderse esa obligación de supresión o bloqueo a nivel mundial en el marco del Derecho internacional pertinente.

Con ello se contempla la posibilidad de que un Juez o Tribunal de un Estado miembro imponga a un prestador de servicios de alojamiento mediante una medida cautelar la obligación de filtrar contenidos idénticos a los ya retirados tras haber sido declarados ilícitos, así como otros similares, siempre y cuando sea posible detectarlos mediante técnicas o medios de búsqueda y reconocimiento automatizado, y siempre y cuando no obliguen al prestador de servicios a realizar una valoración autónoma (no automatizada) del carácter infractor de esos contenidos o informaciones. Esto es, el TJUE viene a admitir que este filtrado específico “a posteriori” no constituye una labor de supervisión general (vedada por el artículo 15 DCE) ni tampoco supone una carga excesiva para el intermediario, siempre y cuando no obligue a una supervisión autónoma no automática de esos contenidos o informaciones.

3.4. Ponderación de derechos e intereses por parte del intermediario en línea a la hora de cumplir con su deber de reacción diligente en la retirada de contenidos infractores de derechos de la personalidad de terceros.

Para poder exonerar su responsabilidad ante posibles infracciones a la intimidad, el honor o la propia imagen resultante de contenidos, informaciones o comentarios suministrados o proferidos por los usuarios de su servicio, el intermediario en línea que tenga conocimiento de su existencia por cualquier medio (en particular si tuviera incorporados en su servicio mecanismos de denuncia o notificación y retirada o bloqueo) deberá realizar una ponderación de los intereses en juego, y, con ello, de derechos constitucionales frecuentemente confrontados, antes de proceder a la retirada o bloqueo de acceso a los mismos.

Los intermediarios en línea se sitúan, así, en una auténtica encrucijada, al tener que realizar una ponderación, compleja “*per se*”, entre los derechos constitucionales al honor, la intimidad y la propia imagen de los terceros afectados (artículo 18 CE) y los derechos constitucionales a la libertad de expresión e información de los usuarios de su servicio (artículo 20 CE), a fin de eludir una posible responsabilidad indirecta por la infracción de tales derechos, viéndose obligados así a anticipar un juicio cuyo control último corresponde a los Tribunales de Justicia y, en último término, al Tribunal Constitucional.

Nace así un conflicto a tres bandas con motivo de la actividad de los intermediarios en línea, entre el denunciante titular de derechos presuntamente infringidos, el prestador del servicio de alojamiento y el usuario de su servicio que genera y/o comparte contenidos o informaciones

presuntamente atentatorios contra la privacidad, el honor o la imagen, el cual podría reclamar responsabilidades al intermediario si retirase información con motivo de una denuncia del titular de derechos que considerase absolutamente infundada o cuando menos dudosa¹⁶. El prestador de servicios de alojamiento se sitúa en el centro de esa encrucijada entre, de un lado, los derechos al honor, la intimidad y la propia imagen (u otros derechos como la propiedad industrial e intelectual), y de otro lado, los derechos a la libertad de expresión e información.

La sentencia del Tribunal Europeo de Derechos Humanos (ECtHR) de 10 de octubre de 2013 (“Delfi AS v. Estonia”, 64569/09) y la posterior sentencia de la Gran Cámara de 16 de junio de 2015 (“Delfi AS v. Estonia”, 64569/09) establecieron que un portal de noticias en línea que facilita a los usuarios reaccionar sin identificarse frente a las informaciones publicadas mediante un foro de comentarios tiene derecho a invocar la libertad de expresión pero debe también responder por los comentarios de los usuarios de su servicio que dañen intereses y derechos de terceros relacionados con la privacidad y el honor¹⁷.

El Tribunal Europeo de Derechos Humanos entendió que, al publicar un artículo sobre la empresa de transporte marítimo, el portal de noticias Delfi tenía que haber previsto posibles reacciones negativas por parte del público y un riesgo mayor de que los comentarios excedieran de lo que puede considerarse una crítica aceptable para incurrir en auténticas injurias contra la empresa, razón por la que cabía esperar del portal de noticias mayores cautelas en la vigilancia y retirada de esos posibles comentarios injuriosos¹⁸. Aunque el portal tenía implementados procedimientos para detectar y retirar automáticamente comentarios excesivos (en forma de filtros de palabras inapropiadas y un sistema de notificación y retirada para los terceros afectados), consideró que su actuación como intermediario no fue lo suficientemente diligente para evitar causar daños al honor y reputación de terceros, sobre todo porque reaccionó muy tarde para retirar los comentarios injurioso, máxime cuando se benefició de la polémica con una mayor afluencia de usuarios que pueden realizar comentarios sin necesidad de identificación ni registro¹⁹.

¹⁶ El ordenamiento estadounidense, antes visto, otorga una garantía de no responsabilidad al proveedor de alojamiento siempre que en la retirada de contenidos se ajuste al estricto procedimiento previsto en la Sect. 512 c) 17 USC.

¹⁷ En el caso, ante una denuncia de una empresa de transporte marítimo por los múltiples comentarios injuriosos vertidos por usuarios del portal de noticias estonio delfi.ee, este intermediario decidió retirar los comentarios pero no atendió la solicitud de indemnización. Los tribunales estonios decidieron que Delfi tenía que indemnizar a la empresa de transportes demandante. Elevada la cuestión a la Corte Europea de Derechos Humanos por infracción del artículo 10 del Convenio Europeo de Derechos Humanos (libertad de expresión), el Tribunal consideró que los tribunales estonios no habían interferido ilegítimamente en el derecho a la libertad de expresión al declarar al portal de noticias Delfi responsable de los comentarios publicados por los usuarios de su portal de noticias.

¹⁸ Sobre la responsabilidad de intermediarios por infracciones al honor de personas jurídicas cometidas por los usuarios de su servicio, en particular analizando el asunto Delfi, véase GARCÍA SILVA, M., “La protección del derecho al honor de las personas jurídicas en redes sociales. La vía civil y la responsabilidad de las plataformas digitales”, Aranzadi Civil, nº 8, septiembre 2022 (versión digital).

¹⁹ Vid. VAN DER SLOOT, B., “Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations en Europe”, cit., pp. 7-9.

En relación con el conflicto habitual entre derechos de la personalidad y la libertad de expresión e información, conviene recordar la doctrina del Tribunal Europeo de Derechos Humanos a la hora de ponderar el peso de ambos derechos fundamentales en una concreta situación. Señala en concreto que cuando se trata de contrastar el derecho a la libertad de expresión contra el derecho al respecto a la privacidad, el equilibrio o balance de intereses ha de tener en cuenta, entre otros, los siguientes elementos: la contribución de la información a un debate de interés general, el mayor o menor grado de conocimiento público de la persona natural o jurídica afectada por la información, el objeto del reportaje o información, la conducta previa de la persona afectada, el método de obtener la información y su veracidad, el contenido, forma y consecuencias de la publicación y la severidad mayor o menor de la sanción o indemnización solicitada²⁰.

De acuerdo con la doctrina del Tribunal Supremo y del Tribunal Constitucional²¹, el juicio de ponderación constitucional entre libertad de expresión e información y los derechos de la personalidad requiere un examen de la intensidad y trascendencia con que cada derecho pueda resultar afectado en una situación determinada, respetando la posición prevalente inicial de las libertades de expresión e información teniendo en cuenta la mayor o menor relevancia o interés público de la información, por razón de la materia y/o de las personas, y la necesaria proporcionalidad en la difusión de las opiniones, debiendo proscribirse el empleo de expresiones manifiestamente injuriosas, vejatorias o que no guarden relación con la información o no sean necesarias para transmitir la idea crítica²². Cuando los afectados por informaciones y comentarios difundidos públicamente son personas de relevancia pública, ejercen funciones públicas o resultan implicados en asuntos de relevancia pública, el Tribunal Constitucional pone en primer plano un nivel máximo de eficacia justificadora del ejercicio de la libertad de expresión frente al derecho al honor que tendrá así una protección menor²³, del mismo modo que será inferior la tutela del derecho honor frente a la libertad de expresión e información cuando su titular sea una persona jurídica²⁴.

Pues bien, si el intermediario en línea (plataforma digital) realiza una valoración precipitada de este complejo conflicto, optando por retirar -sin una cuidadosa motivación- la información o contenidos presuntamente infractores de derechos de la personalidad de terceros, puede encontrarse con una demanda dirigida contra él por la infracción del derecho a la libertad de opinión, expresión e información del artículo 20 CE. Por el contrario, si decide conservar la información presuntamente infractora, puede encontrarse con una demanda de responsabilidad civil, *ex* artículo 1902 CC, interpuesta por el tercero

²⁰ Cfr. sentencias del Tribunal Europeo de Justicia (ECtHR) de 14 de junio de 2007 (*Associes v. France*, 71111/01) y de 12 de junio de 2012 (*MGN Ltd/UK*, 39401/04), entre otras.

²¹ Cfr. STC 58/2018; STC 133/2018; SSTS 488/2017, de 11 de septiembre ó 429/2019, de 16 de julio.

²² A diferencia de lo que sucede con la libertad de expresión, la libertad de información trata sobre la difusión de hechos objetivos, razón por lo que las opiniones y comentarios realizados por personas que no son profesionales de la información gozarán de mayor libertad (o menores restricciones) mientras que las informaciones expresadas por profesionales de los medios de comunicación están sujetos a los requisitos de diligencia y veracidad (cfr. STC 232/2002, de 9 de diciembre)

²³ Cfr. STC 344/2015, de 16 de junio.

²⁴ Cfr. STC 35/2017, de 19 de enero. Vid. GARCÍA SILVA, "La protección del derecho al honor de las personas jurídicas en redes sociales...", cit., pp. 4-5 (versión digital).

afectado por esa información, contenidos o comentarios, sobre todo cuando hubiera notificado por cualquier medio la existencia de la misma en la plataforma o servicio del intermediario y vio cómo éste no reaccionaba de forma diligente para retirar la información.

En ocasiones, las intromisiones en el honor, la intimidad o la propia imagen son tan evidentes ("*res ipsa loquitur*") que el intermediario no debería tener ninguna duda a la hora de reaccionar con prontitud para retirar la información o contenidos infractores de su plataforma o servicio de intermediación en línea²⁵. Es el caso, por ejemplo, de los graves atentados a la intimidad, el honor y a la propia imagen que tienen lugar con las llamadas prácticas de "*deepfake*" o "*ultrafalsificaciones*"; sobre todo las "*porno deepfake*" consistentes en la utilización de imágenes de personas famosas para crear fotografías de desnudos o vídeos pornográficos falsos mediante programas de inteligencia artificial²⁶. También en aquellos otros casos donde se manipula la voz a imagen de personas famosas para crear noticias falsas o en los que se usa la voz de intérpretes famosos -incluso ya fallecidos- cantando canciones creadas por inteligencia artificial²⁷.

Pero en otros casos donde la intromisión en derechos de la personalidad no resulte tan evidente el intermediario deberá realizar una cuidadosa y diligente ponderación, debidamente motivada, si quiere evitar demandas o reclamaciones por parte de los terceros afectados por la información, de un lado, o de los usuarios de su servicio, por otro lado²⁸.

En el caso de indebido tratamiento y difusión de datos personales (que constituye también un derecho de la personalidad o de la privacidad entendida "*lato sensu*", pero diferente del derecho a la intimidad, honor e imagen) en plataformas digitales, se estará a lo dispuesto en las propias políticas de algunas plataformas y en la normativa específica del sector²⁹, aplicándose las

²⁵ Cfr. STS 235/2020, de 2 de junio y STC 83/2023, de 4 de julio (caso "meneame.com").

²⁶ Son archiconocidos los casos que han afectado a las cantantes Rosalía y Taylor Swift (con más de 35 millones de visualizaciones en la red social X antes de que ésta procediera a eliminar esos contenidos de su plataforma). En nuestro país, sin afectar a personas famosas, resultó impactante el caso de las imágenes manipuladas presentando desnudas a un grupo de menores de Almendralejo.

²⁷ El incremento de casos de "*deepfakes*" llevó al Parlamento Europeo a encargar el estudio *Tackling Deepfakes in European Policy*, julio 2021 (algunas de cuyas conclusiones se han plasmado en el Reglamento UE sobre Inteligencia Artificial). En este estudio se ha inspirado seguramente el Grupo Parlamentario Sumar para promover un cambio legislativo por medio de la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, publicado en el Boletín Oficial de las Cortes Generales el día 13 de octubre de 2023, proponiendo cambios en la Ley 13/2022, de 13 de julio, General Audiovisual, en la LO 1/1892, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen, el Código Penal (para modificar el delito de injurias), la Ley de Enjuiciamiento Civil (para crear una medida cautelar específica), la LO 3/2018, de Protección de datos personales y garantía de derechos digitales, y la Ley 3/1991, de 5 de enero, de Competencia Desleal, entre otras.

²⁸ Vid. LÓPEZ RICHARD, J., "Difamación en la Web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", cit., pp. 143-201.

²⁹ El artículo 1.5 b) de la Directiva 2000/31, de comercio electrónico dispuso que la Directiva no se aplica a cuestiones relacionadas con la protección de datos personales en la sociedad de la información. El artículo 2.4 g) RSD 2022 señala que las reglas sobre responsabilidad de los intermediarios en línea previstas en el mismo se entenderán sin perjuicio del Derecho de la Unión en materia de datos personales. Por su parte, el artículo 2.4 del Reglamento (UE) 2016/678 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, dispone que su normativa se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

sanciones pertinentes directamente a las plataformas digitales en los casos en que la plataforma sea el responsable del tratamiento de los datos personales, e indirectamente, en su caso -aplicando las reglas de responsabilidad de intermediarios en línea,- cuando los responsables del tratamiento ilícito sean usuarios de la plataforma pero ésta no actúe como verdadero intermediario (neutral y pasivo) o, haciéndolo, cuando no reaccione con prontitud para la retirada de los mismos de su sitio en línea una vez advertida del tratamiento ilegítimo de datos personales por cualquier medio y en particular por la denuncia de los titulares de esos datos³⁰.

Estas complejas situaciones, cada vez más frecuentes debido al creciente protagonismo de las plataformas digitales en la sociedad digital como punto de encuentro y comunicación, venían reclamando reglas más precisas para delimitar el contenido del requisito de la reacción diligente de los intermediarios a la hora de retirar información, contenidos o comentarios infractores de derechos de terceros, y muy en particular de derechos de la personalidad, y ofrecer seguridad jurídica a todas las partes implicadas: los usuarios de servicios de intermediación en línea, los terceros afectados por los contenidos, informaciones o comentarios compartidos por esos usuarios y el gestor del servicio de intermediación en línea.

Estas reglas han sido desarrolladas por las instituciones de la Unión Europea en el nuevo Reglamento de Servicios Digitales aprobado por las instituciones de la Unión Europea y normativa ulterior de desarrollo del mismo.

4. El régimen de responsabilidad de los intermediarios en línea en el reglamento de servicios digitales de la unión europea.

4.1. Las reglas de exención de responsabilidad de intermediarios de alojamiento de datos en el Reglamento (UE) de Servicios Digitales.

El nuevo Reglamento (UE) 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales; en adelante RSD), cuya plena aplicación tendrá lugar a partir del 17 de febrero de 2024³¹, apuesta por la conservación de las reglas generales de exención de responsabilidad de los servicios de intermediación en línea establecidas en la Directiva 2000/31, de comercio electrónico (DCE), si bien considera conveniente precisar determinados elementos de ese marco normativo teniendo en cuenta la jurisprudencia del TJUE (Considerando nº 16).

Por lo tanto, el Reglamento de Servicios Digitales conserva el enfoque horizontal de las reglas de puerto seguro o exención de responsabilidad de los servicios intermediarios por los datos o informaciones transmitidos o almacenados a petición del usuario de sus servicios, señalando que sólo

³⁰ VANDERSLOOT, B., "Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe", cit., pp. 5-6.

³¹ El Reglamento de Servicios Digitales se aplica a las plataformas digitales y motores de búsqueda de muy gran tamaño que fueron designados por la Comisión Europea en una Decisión de 25 de abril de 2023 (DO C 249 de 14 de julio de 2023, p. 2), ejerciendo frente a ellos las competencias de ejecución previstas en el Capítulo IV, Secc. 4, artículo 49.3 del mismo RSD.

determinan cuándo no se pueden exigir responsabilidades al prestador de servicios intermediarios en relación con contenidos o informaciones ilícitos proporcionados por los destinatarios del servicio, sea cual sea la naturaleza del contenido ilícito y de la responsabilidad, correspondiendo así a las disposiciones de los ordenamientos nacionales determinar cuándo se pueden exigir responsabilidades a los prestadores de servicios intermediarios (Considerando nº 17 RSD).

En relación con los servicios intermediarios de alojamiento de datos, entre los que el propio Reglamento sitúa, como subespecie, a los servicios de plataforma en línea, el artículo 6, apartados 1 y 2 RSD reproduce la misma regla general de exención de responsabilidad que antes recogía el artículo 14 DCE, de modo que no serán responsables de las informaciones almacenadas por los destinatarios de su servicio a condición de que:

a) no tengan conocimiento efectivo de una actividad ilícita o de un contenido ilícito, o de hechos o circunstancias que revelen el carácter ilícito de una actividad o un contenido, o de que;

b) en cuanto tengan conocimiento de estas circunstancias actúe con prontitud para retirar el contenido ilícito o inhabilitar el acceso al mismo (el llamado principio de reacción diligente).

Lo anterior siempre que el usuario no actúe bajo la autoridad o el control del prestador de servicios, en cuyo caso se entiende que éste será en todo caso directamente responsable de los daños y perjuicios causados por la actividad o información suministrada por el usuario de su servicio³².

Con todo, el artículo 6.3 RSD establece una nueva regla de responsabilidad directa de los intermediarios de alojamiento de datos y plataformas en línea en caso de infracciones de derechos de los consumidores y usuarios, en aquellos casos de plataformas de comercio electrónico que permitan celebrar contratos en línea entre usuarios profesionales y usuarios finales, cuando sean los intermediarios quienes presenten el elemento de información concreto o hagan posible la transacción comercial de manera que puedan inducir a un consumidor medio a creer que esa información o el producto o servicio objeto de la transacción se proporcione por la propia plataforma en línea por un usuario comercial que actúe bajo su control o dirección.

El artículo 8 RSD reproduce la inexistencia de una obligación general de supervisión "*ex ante*" de los intermediarios que establecía el artículo 15 DCE, al indicar que no se impondrá a los prestadores de servicios intermediarios ninguna obligación general de monitorizar la información que transmitan o

³² El Considerando nº 18 RSD recoge la jurisprudencia del TJUE para ayudar a la interpretación de las normas de puerto seguro de los servicios intermediarios, pensando fundamentalmente en los servicios de alojamiento de datos o servicios de plataforma. Apunta, así, que las exenciones de responsabilidad establecidas en el Reglamento de Servicios Digitales para los prestadores de servicios de "*hosting*" no deberán aplicarse cuando, en lugar de limitarse a la prestación neutra de los servicios mediante un tratamiento puramente técnico y automático de la información proporcionada por el destinatario del servicio, el prestador de servicios intermediarios desempeñe un papel activo de tal índole que le confiera el conocimiento de dicha información, o control sobre ella. En la misma línea, el Considerando nº 20 RSD apunta que cuando un prestador de servicios intermediarios colabore deliberadamente con un destinatario de los servicios a fin de llevar a cabo actividades ilícitas, se ha de considerar que el servicio no se ha prestado de forma neutra y, por tanto, no debe poder acogerse a las exenciones de responsabilidad estipuladas en el Reglamento. Y en el Considerando nº 23 se indica, en concreto, que la exención de responsabilidad no puede aplicarse cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios de alojamiento.

almacenen, ni de buscar activamente hechos o circunstancias que indiquen la existencia de actividades ilícitas; aunque el artículo 7 RSD deja abierta la posibilidad de que los intermediarios realicen, de buena fe y de modo diligente, investigaciones voluntarias por iniciativa propia con el fin de detectar, identificar y retirar contenidos ilícitos o bloquear el acceso a éstos, pudiendo acogerse igualmente al régimen de exención de responsabilidad previsto con carácter general en los artículos 4 a 6 RSD.

4.2. Obligaciones de diligencia debida de los prestadores de servicios de alojamiento de datos, en particular plataformas en línea de comercio electrónico.

Las condiciones que delimitan el régimen de exención de responsabilidad de los servicios intermediarios, en especial los de alojamiento de información, deberán ser interpretadas ahora a la luz de las obligaciones de diligencia debida ("*due diligence*") introducidas por el Reglamento de Servicios Digitales para crear un entorno en línea transparente y seguro, con la finalidad de prevenir y corregir con prontitud posibles infracciones de derechos de terceros por parte de los usuarios profesionales de la plataforma. Obligaciones de diligencia que constituyen -sin duda- una de las principales y más reseñables novedades de la normativa aplicable a los servicios de intermediación en el nuevo Reglamento de Servicios Digitales, junto a las reglas que establecen una estructura de gobernanza para garantizar la cooperación y la coordinación entre las autoridades competentes de los Estados miembros y la Comisión europea en cuanto a la supervisión y la exigencia del cumplimiento de esas obligaciones de diligencia debida.

Entre las obligaciones de diligencia debida destaca la obligación para los servicios de alojamiento de datos de establecer mecanismos internos sencillos de notificación y acción, de fácil acceso y manejo, para la comunicación electrónica de denuncias de contenidos u ofertas presuntamente ilícitas por parte de los usuarios finales del servicio (artículo 16 RDS), otorgando prioridad a las notificaciones que realicen los denominados "alertadores fiables", las cuales deberán tramitar y resolver sin dilaciones (artículo 22 RSD). De tal manera, lo que bajo el régimen de la DCE 2000 era meramente voluntario, ahora se convierte en un mecanismo obligatorio para los intermediarios de "*hosting*" en el RSD 2022.

Los intermediarios de alojamiento de datos, entre los que se encuentran las plataformas digitales, deben facilitar el envío de notificaciones suficientemente precisas y adecuadamente fundamentadas. Se considerará que las notificaciones enviadas proporcionarán un conocimiento efectivo o permitirán ser consciente del elemento de información de que se trate, cuando permitan a un prestador diligente de servicios de alojamiento determinar, "sin un examen jurídico detallado"³³, que la información o la actividad denunciadas

³³ Con ello parecen compartirse posibles responsabilidades en la retirada de contenidos, sobre todo en aquellos casos donde sea más complejo realizar una adecuada ponderación de derechos e intereses, como sucede con los conflictos entre libertad de expresión e información con el derecho a la privacidad, el honor y la intimidad. De modo que los terceros afectados tienen la carga legal de facilitar la comprensión y valoración del conflicto a la plataforma digital, la cual tendrá más fácil no atender solicitudes de retirada de

son ilícitas (artículo 16.3 RSD) y, en consecuencia, reaccionar con prontitud para retirarla de su plataforma y bloquear su carga ulterior. El intermediario enviará un acuse de recibo y notificará, sin dilación indebida, su decisión respecto a la retirada o no de la información, incluyendo información sobre las vías de recurso de su decisión (artículo 16.4 y 5 RSD).

El prestador del servicio que aprecie la ilicitud o ilegalidad de informaciones, contenidos o actividades ofrecidos desde su plataforma deberá establecer restricciones a su visibilidad, incluida la eliminación de contenidos, el bloqueo del acceso a los mismos o su relegación, además de la cesación, suspensión u otra restricción de los pagos monetarios, la suspensión o cesación total en la prestación del servicio de intermediación, y la suspensión o supresión de la cuenta del destinatario, ofreciendo al usuario afectado una explicación clara sobre su decisión y los hechos y circunstancias que la hubieran motivado, incluyendo si actuó previa notificación de un tercero o por su propia iniciativa (artículo 18 RSD). Para ello, el intermediario deberá emitir una declaración de motivos clara y específica dirigida a los destinatarios de su servicio de intermediación en relación con su decisión de bloqueo o restricción de visibilidad de contenidos o informaciones ilícitos, suspensión o cesación total o parcial del servicio, suspensión o supresión de la cuenta del destinatario, incluyendo información clara y precisa sobre vías de recurso de su decisión, a través de mecanismos internos de reclamaciones, órganos de resolución extrajudicial de litigios y recursos judiciales (artículo 17 RSD).

A tal fin, todo intermediario en línea de alojamiento de datos tendrá la obligación de mantener un sistema interno de gestión de reclamaciones eficaz, electrónico y gratuito que permita a los usuarios afectados por una decisión de retirada o bloqueo de informaciones, o de suspensión o cesación total en la prestación del servicio de intermediación, la interposición de reclamaciones por vía electrónica y gratuita, debiendo notificar su decisión motivada sin dilaciones y la posibilidad de recurrir a un mecanismo de solución extrajudicial de conflictos o a los órganos jurisdiccionales competentes (artículos 20 y 21 RSD).

Por su parte, los Estados miembros deberán implementar mecanismos de resolución extrajudicial de litigios (conflictos) por un órgano certificado al efecto por el coordinador de servicios digitales nacional, cuyas decisiones no serán vinculantes para las partes (artículo 21 RSD). Los Estados miembros solo están obligados a cumplir con esta obligación de gobernanza que supone el nombramiento de un coordinador de servicios digitales y el organismo de resolución extrajudicial de conflictos antes de la plena aplicación del RSD, el 17 de febrero de 2024.³⁴ Sin embargo, dado que la Comisión europea implementó sus funciones de ejecución para plataformas digitales y motores de búsqueda de gran tamaño el día 25 de abril de 2023, y considerando que es necesario contar con la asistencia y cooperación de las autoridades nacionales de los Estados miembros, decidió promulgar la Recomendación (UE) 2023/2425 de 20 de octubre de 2023, sobre la coordinación de respuestas a incidentes,

informaciones y contenidos cuando las denuncias recibidas sean imprecisas, salvo -entendiendo- en los casos donde la infracción de los derechos de terceros sea evidente a la luz de las circunstancias.

³⁴ No se ha previsto nada aún en nuestro país sobre cuál puede ser este órgano de resolución de conflictos, de modo que el Ejecutivo puede optar bien por crear un órgano "*ad hoc*" para resolver los conflictos relacionados con la retirada de contenidos, informaciones o actividades por parte de los intermediarios en línea, o bien por habilitar esta función en el seno de algún organismo ya existente (como la CNMC).

especialmente los derivados de la difusión de contenido ilícito, en anticipación a la plena entrada en aplicación del Reglamento 2022/2065 (Reglamento de Servicios Digitales)³⁵.

Por lo demás, más allá de la obligación de implementar los mecanismos de denuncia, retirada y bloqueo ("*notice & take down & stay down*"), se establece que las plataformas digitales deberán suspender -durante un periodo razonable y después de haber realizado una advertencia previa- la prestación de su servicio a los usuarios que proporcionen con frecuencia contenidos manifiestamente ilícitos (artículo 23.1 RSD); como deberán suspender igualmente la tramitación de avisos y reclamaciones a las personas físicas o jurídicas que envíen con frecuencia avisos o reclamaciones que sean manifiestamente infundados (artículo 23.2 RSD). En sus condiciones de uso, los intermediarios expondrán de manera clara y detallada su política respecto de usos indebidos de usuarios y terceros reclamantes (artículo 23.4)³⁶.

Por último, el Reglamento contiene una serie de reglas especiales en forma de obligaciones adicionales de gestión de riesgos sistémicos para prestadores de plataformas en línea y motores de búsqueda en línea de muy gran tamaño ("*gatekeepers*" o guardianes de acceso; cfr. artículos 33 y ss. RSD), que resultan especialmente importantes desde el punto de vista de la prevención por lo que se refieren a la evaluación diligente de riesgos sistémicos que deriven del diseño y funcionamiento de su servicio (artículo 34 RSD) y, sobre todo, con la obligación de aplicar medidas de reducción de riesgos razonables detectados en su sistema teniendo en cuenta especialmente las consecuencias de esas medidas sobre los derechos fundamentales (artículo 35 RSD)³⁷.

Esta última obligación sugiere la posibilidad de implementar medidas o técnicas de reconocimiento automático de contenidos potencialmente ilícitos para facilitar su posterior retirada, en caso de comprobar su manifiesta o más que probable ilicitud. Técnicas estas que, realmente, estarían matizando o

³⁵ C(2023) 7170. DO L de 26 de octubre de 2023. En realidad, con esta solución provisional la Comisión europea busca una respuesta rápida y activa, coordinada y coherente, de los Estados miembros a los incidentes derivados de la difusión de contenido ilícito en plataformas digitales de muy gran tamaño que planteen un claro riesgo de intimidación a determinados grupos de población y de desestabilizar las estructuras políticas y sociales en la Unión o en parte de ella, incluido el contenido que pueda constituir una amenaza grave para la seguridad pública o la salud pública (en particular los contenidos relacionados con la guerra entre Rusia y Ucrania y Hamás e Israel). Aunque seguramente servirá de excusa para incentivar la designación rápida de un Coordinador de Servicios Digitales y la participación en la red de cooperación con la Comisión.

³⁶ Esta posibilidad de suspender el servicio a los usuarios especialmente o reiteradamente ofensivos y de no tramitar denuncias poco o escasamente fundadas puede ser muy importante en la práctica para las plataformas digitales en el caso de reclamaciones por comentarios presuntamente ofensivos o injuriosos, a la vista del elevadísimo número de comentarios insultantes que pueden encontrarse en foros digitales y redes sociales, así como al previsiblemente frecuente número de denuncias con que pueden encontrarse por parte de los afectados. Será determinante el contenido más o menos preciso de la reclamación que realice el afectado y que evite a la plataforma tener que realizar una compleja ponderación de derechos.

³⁷ Destaca especialmente en la protección de derechos de la personalidad (privacidad), lo previsto en el artículo 35 letra k): la adopción de medidas adecuadas para "*garantizar que un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeja notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos, se distinga mediante indicaciones destacadas cuando se presente en sus interfaces en línea y, además, proporcionar una funcionalidad fácil de utilizar que permita a los destinatarios del servicio señalar dicha información*". De este modo las grandes plataformas y motores de búsqueda están obligados legalmente a actuar de manera especialmente diligente en la vigilancia, detección e identificación de ultrafalsificaciones o "*deepfakes*", lo que facilitará a su vez su rápida retirada por la propia plataforma o a instancia de las personas afectadas.

relativizando para las grandes plataformas la prohibición -establecida en el derogado artículo 15 DCE y el vigente artículo 8 RSD- de vigilancia o monitorización o búsqueda activa de hechos o circunstancias que indiquen la existencia de actividades ilícitas en su sistema, pero que a su vez entroncan con la posibilidad de realizar investigaciones propias y en cumplimiento del Derecho prevista en el artículo 7 RSD; máxime cuando el cumplimiento del Derecho en cuestión viene obligado por el mismo RSD para las grandes plataformas y motores de búsqueda de muy gran tamaño en relación con riesgos sistémicos que deriven del diseño y funcionamiento de sus servicios (como puede suceder, en particular, con las redes sociales en relación con posibles infracciones de derechos a la intimidad, el honor o la imagen).

A la postre, conjugar la prohibición del artículo 8 RSD con las medidas voluntarias del artículo 7 RSD y las obligaciones para grandes plataformas de los artículos 34 y 35 RSD, requiere un cuidadoso diseño y aplicación de las técnicas de reconocimiento automatizado de contenidos o informaciones, lo que exige salvaguardar en todo caso los derechos de los usuarios, primero con un diseño o ajuste estricto de ese tipo de técnicas de reconocimiento al reconocimiento de los supuestos de infracción más evidentes y socialmente alarmantes, y segundo, con una aplicación rigurosa de los mecanismos de recurso a favor de los usuarios y, llegado el caso, la rápida reposición de los contenidos e informaciones indebidamente retirados³⁸.

En definitiva, aunque el Reglamento de Servicios Digitales reitera el principio de inexistencia de un deber general de supervisión a priori, establece la obligación de implementar mecanismos de denuncia ("*notice, take down & stay down*") que servirá de prueba del despliegue de una diligencia debida en caso de enfrentarse a demandas de responsabilidad por infracciones de derechos de terceros cometidas por los usuarios de su servicio de intermediación. Establece asimismo la obligación para estos intermediarios de implementar mecanismos internos de recurso contra sus decisiones de retirada, bloqueo, suspensión o cesación de su servicio a los usuarios presuntamente infractores de derechos de terceros. Y establece, finalmente, la obligación de las plataformas y motores de búsqueda de muy gran tamaño de aplicar medidas de reducción de los riesgos razonables propios de su modelo de negocio y, por tanto, del diseño y funcionamiento de su servicio. Con lo cual, al tiempo que garantiza una mejor detección de contenidos, informaciones o actividades ilícitas, concretando la forma de tomar conocimiento efectivo por el intermediario, el legislador de la Unión incrementa notablemente el deber reacción diligente de las plataformas en línea en caso de recibir un aviso de infracción por parte de los titulares de derechos afectados por los contenidos, informaciones y actividades de su plataforma (que será especialmente frecuente en el caso de derechos de la personalidad), a modo de deber de supervisión a posteriori y específico. Los

³⁸ En relación con esta cuestión, pero en el contexto de la retirada de contenidos infractores de derechos de autor y conexos, comentando los equilibrios enfatizados por la STJUE de 26 de abril de 2022 (Asunto C_401/19, "República de Polonia c. Parlamento Europeo y Consejo de la Unión Europea") en relación con el artículo 17 de la Directiva 2019/790, del Parlamento Europeo y del Consejo, de 17 de abril de 2010, sobre los Derechos de Autor y Derechos Afines en el Mercado Único Digital, vid. LÓPEZ RICHARD, J., "Sistemas de reconocimiento automatizado de contenidos y ponderación de derechos fundamentales: el difícil equilibrio en la transposición del artículo 17 DDAMUD", en López Richard, J. y Saiz García, C. (Coords.), Digitalización, acceso a contenidos y propiedad intelectual, Dykinson, S.L., 2023, pp. 137-186.

intermediarios en línea deberán así evitar reacciones precipitadas a denuncias o notificaciones de terceros con escaso fundamento. Por el contrario, deberán buscar en sus decisiones un equilibrio entre los derechos de terceros (muy especialmente en el caso de los derechos al honor, la intimidad y la propia imagen, así como el tratamiento indebido de datos personales) y los derechos de sus usuarios (libertad de expresión e información).

Solo si extreman su diligencia en la forma establecida en el Reglamento de Servicios Digitales, podrán los intermediarios de alojamiento de datos y plataformas digitales exonerar su responsabilidad ante posibles infracciones de derechos de terceros cometidas por los usuarios de su servicio.

5. Naturaleza de la responsabilidad de los intermediarios en línea. En particular, su posible responsabilidad por intromisiones en la privacidad.

5.1. Consideraciones previas sobre la clase de responsabilidad imputable a las plataformas digitales.

De la jurisprudencia dictada al hilo de la interpretación del régimen de puertos seguros previsto en la DCE e incorporado en la LSSICE no queda claro cuál puede o debe ser el criterio o título de imputación de esa posible responsabilidad, pues ni el TS ni el TJUE han abordado directamente esta problemática.

En las sentencias dictadas hasta la fecha, los tribunales no se ocupan de la naturaleza de la posible responsabilidad en que puedan incurrir los servicios intermediarios de alojamiento de datos. Realmente el Tribunal no establece reglas de responsabilidad de los servicios de intermediación, sino -únicamente- las condiciones para que no se apliquen las reglas de puerto seguro o exención de responsabilidad de los intermediarios.

La Directiva de Comercio Electrónico no aclara nada al respecto, pero de su texto se deduce que los prestadores de servicios de intermediación responden por sus propias actividades y no por hechos ajenos³⁹. Esto es, que su posible responsabilidad será por su comportamiento en el almacenamiento y difusión de contenidos propios o elaborados por él mismo o por cuenta suya, pero también por los actos destinados a facilitar, sin control alguno, las informaciones y actividades de los usuarios de su sistema, distinta por tanto de la responsabilidad que corresponda a los usuarios por los ilícitos cometidos contra derechos e intereses de terceros.

Por lo tanto, la responsabilidad de los operadores de redes y proveedores de acceso es una responsabilidad por hecho propio de índole subjetiva (el mismo

³⁹ Vid. APARICIO VAQUERO, "El nuevo régimen de prestación de servicios de la sociedad de la información", cit., p. 98. El único supuesto establecido en la norma de responsabilidad por hecho ajeno es aquel en que un usuario actúe bajo la dirección, autoridad o control del prestador del servicio de intermediación, en el caso de los prestadores de servicios de alojamiento (artículo 12.1 letra b. DCE; artículo 16.2 LSSICE) y prestadores de servicios de búsqueda (artículo 17.2 LSSICE), de forma similar a la responsabilidad del artículo 1903 CC. En contra, RUBÍ PUIG, "Derecho al honor online y responsabilidad civil de los ISPs", cit., para quien la responsabilidad del intermediario es una responsabilidad por hecho ajeno (por las infracciones cometidas por los usuarios del servicio).

régimen de exención de responsabilidad excluye a priori una calificación de su responsabilidad como cuasi-objetiva u objetiva); cuestión distinta es que los datos o información causantes del daño a terceros provengan de terceros sujetos. Quiere esto decir que la responsabilidad civil, penal o administrativa no les será impuesta por el mero hecho de que un usuario profesional o particular del servicio de intermediación realice conductas que son o puedan considerarse ilícitas utilizando los servicios y recursos técnicos provistos por el intermediario (lo que nos llevaría a una responsabilidad objetiva por el mero riesgo que supone su actividad), sino por sus propias actuaciones en relación a tales conductas y la diligencia mostrada en evitarlas o impedirles una vez conocidas⁴⁰. Así pues, el intermediario de la sociedad de la información puede responder por acción u omisión propia en todo caso, pero -como se ha dicho ya- no responderá en ningún caso por el incumplimiento de una genérica obligación de supervisión de contenidos, que no puede exigírsele a priori por impedirlo el art. 15 DCE.

Pues bien, teniendo claro en todo caso que nunca se tratará de una responsabilidad vicaria o por hecho ajeno, sino que serán siempre supuestos de responsabilidad propia del intermediario derivada de su actuación no neutral o negligente (en caso de no reaccionar con prontitud para la retirada de contenidos ilícitos), la naturaleza y -por consiguiente- el título de imputación de responsabilidad a las plataformas digitales por las infracciones cometidas por los usuarios de su servicio debería determinarse en principio por las reglas de responsabilidad nacionales, o, en su caso, por conceptos autónomos del Derecho de la UE.

Llegados a este punto, es preciso decidir si la responsabilidad imputable, en su caso, a los intermediarios de servicios de alojamiento, incluyendo las plataformas en línea, es una responsabilidad indirecta por contribuir con su actividad a la infracción de derechos de terceros cometida por los usuarios de su plataforma, o si se trata más bien de una responsabilidad directa por el mismo concepto infractor que cometan los usuarios de su servicio; a saber, infracciones marcarias, contra derechos de autor o conexos, contra derechos de los consumidores o usuarios, intromisiones en el honor, la intimidad o la propia imagen, o tratamiento ilegítimo de datos personales.

La cuestión de fondo, entonces, es si los perjudicados pueden exigir al servicio intermediario (la plataforma digital) la misma responsabilidad que podrían exigir a los usuarios de la plataforma infractores de sus derechos, en el caso de la responsabilidad directa. O si, por el contrario, sólo podrían exigir una responsabilidad indirecta o secundaria ("*secondary Liability*") por contribuir o facilitar esas infracciones de derechos ("*contribution infringement Liability*") que debería reconducirse al esquema general de la responsabilidad civil extracontractual.

En la STJUE de 2 de abril de 2020 (Asunto C-567/18, "Coty Germany c. Amazon Services"), la cual versa sobre una cuestión prejudicial en materia de infracción marcaria por un vendedor de la plataforma "*Amazon Marketplace*"

⁴⁰ BUSTO LAGO, "La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs)", cit., pp. 1002 y ss., habla al respecto de los principios de "autorresponsabilidad", "cooperación" y "reacción diligente", por más que lo reconduce a supuestos de responsabilidad por hecho ajeno, ex artículo 1903 CC.

que se prevale de los servicios de promoción, almacenamiento y envío proporcionados por “Amazon Logistics”, el Tribunal rechazó que pudiera apreciarse una infracción directa del derecho de marca por parte de Amazon en virtud de lo previsto en el artículo 9.3 b) del Reglamento (UE) 2017/1001, de 14 de junio de 2017, sobre la marca de la UE, el cual -dice- ha de interpretarse en el sentido de que debe considerarse que una persona que tiene en depósito por cuenta de un tercero productos que infringen un derecho de marca, sin tener conocimiento de esta infracción, no almacena estos productos con el fin de ofrecerlos o comercializarlos en el sentido de estas disposiciones cuando no persigue ella misma estos fines⁴¹.

Sin embargo, en la STJUE (Gran Sala) de 22 de diciembre de 2022 (Asuntos acumulados C-148/21 y C-184/21, “Louboutin c. Amazon”) el Tribunal se aparta del criterio propuesto por el Abogado General, estableciendo una nueva doctrina más garantista para los titulares de derechos de marca al disponer que cuando el operador de un sitio de venta en línea que integra, además de sus propias ofertas de venta, un mercado electrónico utiliza él mismo un signo idéntico a una marca de la Unión ajena, para productos idénticos a aquellos para los que está registrada la marca, cuando terceros vendedores ofrecen para su venta en dicho mercado, sin el consentimiento del titular de la marca, tales productos provistos de ese signo, si un usuario normalmente informado y razonablemente atento de ese sitio establece un vínculo entre los servicios de ese operador y el signo en cuestión, lo que ocurre, en particular, cuando, habida cuenta de todos los elementos que caracterizan la situación, ese usuario podría tener la impresión de que es ese operador quien comercializa, él mismo, en su propio nombre y por cuenta propia, los productos provistos de ese signo.

Es decir, el TJUE sanciona un régimen de responsabilidad directa de la plataforma digital de comercio electrónico por infracción de marcas ajenas, entendiendo que se produce un uso no autorizado de las mismas por las plataformas híbridas que entremezclan sus propias ofertas de venta con las ofertas de los vendedores o usuarios profesionales de su servicio de plataforma mediante una presentación uniforme de todas ellas incluyendo su propio logotipo de renombre en todos los anuncios, empleando reclamos comunes (“las mejores ventas”, “las mejores ofertas”), contestando en común a preguntas de los usuarios demandantes sobre los productos, y prestando servicios de almacenamiento, envío y gestión de las devoluciones sin distinguir entre productos propios y ajenos (cfr. apartados 51 a 53). De modo que la infracción directa de marcas de terceros por el uso no autorizado de las mismas es cometida tanto por los usuarios profesionales como por la plataforma que

⁴¹ Sin embargo, el Abogado General Manuel Sánchez-Bordona sí que entró al fondo de esta cuestión en las Conclusiones presentadas con fecha de 28 de noviembre de 2019, donde además de afirmar la responsabilidad directa de Amazon por su actividad logística en el depósito y envío de mercancías vendidas por usuarios de su plataforma infringiendo derechos de marca de terceros, sugiere también la vía alternativa de la responsabilidad indirecta de la plataforma como intermediario de la sociedad de la información que no actúa de forma neutral, automática y pasiva, poniendo de manifiesto en ambos casos que la destacada implicación de las plataformas en línea que gestionan mercados electrónicos en la comercialización de productos provoca que se les pueda demandar un “*especial esmero (diligencia) respecto del control de la licitud de los bienes con los que comercian*”; precisamente porque las plataformas digitales son o deberían ser conscientes de que, sin ese control, es fácil que sirvan de cauce a la venta de productos ilícitos que vulneran derechos de propiedad de terceros, no pueden, sin más, descargarse de su responsabilidad atribuyéndosela en exclusiva al vendedor (cfr. apartado 82 de las Conclusiones).

da cobertura a sus ofertas como si fueran propias. Aunque no se puede hablar de una responsabilidad directa y objetiva, pues la infracción se hace depender de una serie de condiciones o criterios que deberán ser apreciados en cada caso concreto por los jueces y tribunales nacionales competentes⁴².

En definitiva, el TJUE establece las condiciones para poder diferenciar entre infracciones directas e infracciones indirectas a la hora de examinar la posible responsabilidad de las plataformas en línea, de manera que habrá una infracción directa de derechos de terceros cuando la plataforma realice por sí misma una conducta tipificada dentro de un derecho exclusivo de propiedad intelectual (marcas, derechos de autor y conexos), o resulte responsable directa -como editora- de información que atente contra la intimidad, el honor o la propia imagen, que no respete la normativa sobre datos personales o que no respete las normas de protección de consumidores y usuarios; mientras que habrá una infracción indirecta cuando contribuya a la infracción de derechos de terceros por parte de los usuarios de su servicio, bien porque no implementa ningún mecanismo eficaz de denuncia y retirada o bloqueo para impedir la infracción de esos derechos de terceros siendo o debiendo ser consciente de que se están produciendo, porque implementando esos mecanismos o teniendo conocimiento por cualquier otro medio de contenidos ilícitos no reacciona con prontitud para retirarlos, o bien porque estimula, incita o incluso controla esos comportamientos infractores.

5.2. La responsabilidad aplicable a las plataformas digitales en casos de intromisiones en la privacidad.

La alusión genérica a intromisiones en la privacidad incluye tanto las infracciones por intromisión en el honor, la intimidad o la propia imagen de terceros, así como en el tratamiento ilegítimo de datos personales. El concepto anglosajón de privacidad ("*Privacy*") hace referencia a cualquier ámbito de la vida privada que se tiene derecho a proteger frente a posibles intromisiones o utilidades inconsentidas⁴³, incluyendo no sólo la intimidad, la imagen o cualquier situación que afecte al honor, sino también la utilización de datos personales. Así, mientras la intimidad hace referencia a las esferas de mayor reserva privada de una persona, libre de cualquier injerencia pública, el concepto más amplio de privacidad incluye toda información relativa a una persona que puede servir para su identificación. En este contexto, la protección

⁴² A diferencia de lo establecido por el mismo Tribunal en materia de infracciones directas de derechos de autor y derechos conexos por parte de las plataformas digitales que permiten a los usuarios compartir contenidos en línea, conducta fue considerada por la STJUE de 14 de junio de 2017 (Asunto C-610/15, "*The Pirate Bay*"), como un acto de puesta a disposición en línea sujeto al derecho exclusivo de autores, intérpretes y productores (artículo 3 de la Directiva 29/2001/CE, de 22 de mayo, sobre derechos de autor y derechos afines en la sociedad de la información) por parte de la propia plataforma prescindiendo por completo de su condición de intermediario en línea, provocando el cambio normativo plasmado luego en el artículo 17 de la Directiva 2019/790, de 19 de abril, sobre derechos de autor y derechos afines en el mercado único digital (cfr. artículo 73 del Real Decreto-Ley 22/2021, de 2 de noviembre). Vid. CARBAJO CASCÓN, F., "*Las plataformas digitales ante la distribución de mercancías y el suministro de contenidos digitales ilícitos*", cit., pp. 22 y ss.

⁴³ El artículo 12 de la Declaración Universal de los Derechos Humanos, se refiere a la privacidad como el derecho a que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

de datos personales no es en rigor un derecho de la personalidad pero sí que se incluye, obviamente, en una tutela más amplia de la privacidad, pues tiene como objeto garantizar a las personas naturales el control de toda información relacionada con su persona y actividades frente al tratamiento por parte de terceros.

El servicio de intermediación en línea responderá directamente frente a los afectados cuando esa intromisión tenga su origen en información o contenidos generados por el propio intermediario (en el caso de plataformas o servicios de intermediación mixtos o híbridos, como puede ser el caso de diarios y revistas digitales que ofrecen al mismo tiempo foros de opinión y comentarios). En tales casos los afectados podrán dirigir contra el servicio en línea las acciones previstas en la legislación española en la Ley Orgánica 1/1982, de 5 de mayo (artículo 9.2). Lo mismo puede decirse cuando la plataforma digital lleve a cabo un tratamiento ilegítimo de datos personales, estando a lo dispuesto en la normativa de la Unión y de los Estados miembros sobre protección de datos personales y sin perjuicio de solicitar indemnizaciones por la vía de la responsabilidad extracontractual del artículo 1902 CC.

Sin embargo, la responsabilidad del intermediario será indirecta en el caso de tener conocimiento efectivo por cualquier medio (fundamentalmente mediante denuncias o notificaciones realizadas por el afectado en el canal interno de reclamaciones de la plataforma) de contenidos, actividades o informaciones suministrados por los usuarios de su servicio⁴⁴ que vulneren o puedan vulnerar el derecho al honor, a la intimidad o a la propia imagen de terceros, o por el tratamiento ilícito de datos personales, y no reaccione con prontitud para retirar esa información y bloquear el acceso posterior de la misma a la plataforma; lo que incluye, como se dice en la STJUE de 3 de octubre de 2019 (Asunto C-18/18, "Eva Glawischnig Piesctek v. Facebook"), la obligación no sólo de retirar o bloquear el acceso a la información suministrada por un concreto usuario identificada en la denuncia o notificación del tercero afectado ("*notice & take & stay down*"), sino también la de suprimir o impedir el acceso a cualesquiera otros datos o informaciones cuyo contenido sea idéntico al de una información declarada ilícita con anterioridad, sea quien fuere el autor de la solicitud de almacenamiento de tales datos, lo que incluye la obligación de implementar sistemas de filtrado y reconocimiento automatizado de contenidos o informaciones que sean idénticos al de una información declarada ilícita con anterioridad o a bloquear el acceso a los mismos, sea quien sea el responsable de la solicitud de almacenamiento de los mismos.

De modo que si el intermediario tiene conocimiento efectivo por cualquier medio -en particular por notificaciones o comunicaciones de los afectados, pero también por la implementación de mecanismos o técnicas de reconocimiento automatizado de contenidos ilícitos- de informaciones, contenidos o comentarios compartidos por usuarios de su servicio que vulneran el derecho al honor, la intimidad o la propia imagen de terceros, o un tratamiento ilegítimo de datos personales, y no reacciona de forma diligente y rápida para retirarlos o bloquear su acceso, podrá ser objeto de una demanda de responsabilidad civil

⁴⁴ Tanto quienes sean autores o responsables directos de las informaciones infractoras como los que contribuyan a su difusión realizando valoraciones personales también negativas podrán ser perseguidos por los terceros afectados, civil y penalmente (injurias y calumnias), en caso de poder ser identificados.

por el tercero afectado; responsabilidad civil, no por la infracción directa por el intermediario de esos derechos de la personalidad o privacidad, sino por contribuir a la infracción al poner los medios para facilitar posibles intromisiones en el honor, la intimidad, la propia imagen o el tratamiento ilegítimo de datos personales de terceros y no reaccionar con prontitud para retirar la información o contenidos infractores cuando tenga conocimiento efectivo de su existencia en su servicio o plataforma, lo que obligaría al afectado a ejercitar acciones contra el intermediario con fundamento en la cláusula general del derecho de daños, artículo 1902 CC, y no en la LO 1/1982 de 5 de mayo o en la normativa sobre protección de datos personales (que sí podrá aplicarse contra la plataforma digital en forma de denuncias ante la Autoridad nacional de protección de datos). Es así porque realmente es el usuario y no la plataforma quien comete una intromisión en la privacidad, honor o imagen del tercero, o quien hace una difusión no autorizada de datos personales, pero la vulneración de derechos de terceros se produce por la falta de neutralidad, en su caso, o falta de reacción diligente de la plataforma en caso de tener conocimiento de esas infracciones.

En definitiva, la exención de responsabilidad o la imputación de responsabilidad indirecta de los intermediarios en línea por infracciones de derechos de la personalidad, deberá valorarse caso por caso a la luz del mayor o menor grado de cumplimiento de sus obligaciones de diligencia debida en la forma de trabar conocimiento efectivo sobre la existencia de posibles infracciones y en la motivación sólida de su reacción diligente al retirar contenidos e informaciones, bloquear su acceso presente y futuro o, en los casos más graves, en la suspensión o cese definitivo del servicio al usuario infractor.

Lógicamente, cuanto mayor relevancia pública tenga la persona y más evidente sea la intromisión en su honor, intimidad o propia imagen, así como el uso no autorizado de sus datos personales, mayor celeridad debe mostrar la plataforma (especialmente en el caso de las redes sociales) para retirar la información e impedir que vuelva a subirse y para cesar en la prestación del servicio al responsable o responsables. Si la persona afectada es pública pero no es tan clara la intromisión en la privacidad, la plataforma debe realizar un cuidadoso análisis de ponderación entre la libertad de expresión e información y la afectación de derechos de la personalidad y datos personales. Y cuando el afectado no tenga relevancia pública esa ponderación de derechos debe inclinarse a favor del mismo si la intromisión en su honor, intimidad o utilización de la imagen o datos personales carece de sentido para la información o contenido que se está difundiendo por los usuarios.

Ahora bien, en el caso de plataformas o motores de búsqueda de muy gran tamaño habría que valorar si la infracción de lo dispuesto en los artículos 34 y 35 RSD, al no implementar sistemas que permitan la evaluación y reducción de riesgos de infracción de derechos de terceros cuando estos son sistémicos a la vista del diseño y aplicación de su plataforma o servicio, podría derivar en una responsabilidad directa -en lugar de indirecta- por facilitar con su negligencia infracciones reiteradas de derechos de terceros, como pueden ser muy especialmente los derechos de la privacidad o personalidad en servicios de redes sociales o similares.