LA RESPONSABILIDAD DE LOS INTERMEDIARIOS EN INTERNET ¿PUERTOS SEGUROS A PRUEBA DE FUTURO?*

LIABILITY OF INTERNET INTERMEDIARIES SAFE AND FUTURE-PROOF HARBOURS?

Esther Arroyo Amayuelas
Catedrática de Derecho Civil
Titular de la Cátedra Jean Monnet de Derecho Privado Europeo
Universitat de Barcelona
ORCID ID: 0000-0002-2466-7833

Recibido: 11.12.2019 / Aceptado: 10.01.2020
DOI: https://doi.org/10.20318/cdt.2020.5225

Resumen: Transcurridos 20 años desde la promulgación de la Directiva 2000/31, de 8 de junio de 2000, sobre comercio electrónico (DCE), parece llegado el momento de adaptar sus exenciones de responsabilidad a los nuevos modelos de negocio en internet. Todo indica que la nueva DCE no tendrá ya por finalidad preservar los puertos seguros con que ahora cuentan los prestadores de servicios de intermediación (arts. 12-14 DCE), sino prevenir que las nuevas estructuras digitales (plataformas) promuevan y difundan actividades ilícitas. En definitiva, se prevé un incremento de sus deberes de diligencia, con el riesgo de censura provocado por un exceso de celo en la búsqueda de ilegalidades y el correspondiente perjuicio para la libertad de información, expresión y empresa. La Directiva 2019/790, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital es un buen exponente de los cambios que ya se han producido y de los que se avecinan.

Palabras clave: intermediarios, plataformas, alojamiento, acceso, deber de diligencia, notificación y retirada.

Abstract: Twenty years after the enactment of Directive 2000/31 of 8 June 2000, on electronic commerce (ECD), it seems that the time has come to adapt its safe harbours regulatory framework to the new internet business models. All the signs are that the purpose of the new ECD will no longer be to preserve the safe harbours now available to providers of intermediation services (arts. 12-14 ECD), but to prevent new digital structures (platforms) from promoting and disseminating illicit activities. In short, it is foreseen an increase in their duties of diligence, with the risk of censorship caused by an excess of zeal in the search for illegalities and the corresponding damage to the freedom of information, expression and enterprise. Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market is just a good example of the changes that have already taken place and those that are still to come.

Keywords: intermediaries, platforms, hosting, access, duty of care, notice and take down.

*Este trabajo tiene su base en la ponencia expuesta en el Congreso Internacional El Derecho privado en el nuevo paradigma digital (Colegio Notarial de Cataluña, Barcelona, 3 y 4 de octubre de 2019). Forma parte de las actividades de la Cátedra Jean Monnet de Derecho privado europeo y también se enmarca en el Proyecto DER2017-82129-P y los estudios llevados a cabo en el seno del Grupo consolidado de investigación de la U. Barcelona (2017 SGR 151).

III. El control editorial. IV. El conocimiento de la ilicitud. 1. La diligencia del operador económico. 2. La notificación. 3. La ilicitud manifiesta. V. El control del tráfico de internet. 1. Alcance de las órdenes judiciales. 2. La iniciativa del intermediario. VI. Los procedimientos de moderación de contenidos. VII. Reflexiones finales.

I. Introducción

1. Hace tiempo que en Europa se cuestiona el rol y las responsabilidades de los intermediarios, o prestadores de servicios de internet, por los contenidos ilícitos que circulan o se alojan en la red. Por el momento, la política de la Comisión Europea, respaldada por parte de la doctrina,[1] ha sido no derogar la Directiva 2000/31, de 8 de junio, sobre comercio electrónico (DCE). [2] Con todo, la Estrategia del Mercado Único Digital (2015-2018) ha ido acompañada de una notable suavización de los efectos del puerto seguro tal y como se encuentra regulado en los arts. 12-14 DCE.

Como es sabido, la DCE no armoniza los distintos sistemas de responsabilidad de los Estados miembros (Cdo 40), a pesar de que el mosaico heterogéneo que estos ofrecen sin duda obstaculiza la consecución del mercado interior. A semejanza de la americana *Digital Millenium Copyright Act*,[3] que es su modelo, la DCE solo prevé algunos supuestos que nunca pueden dar lugar a esa responsabilidad.[4] Esos puertos seguros o *safe harbours* abarcan todo tipo de infracciones y, por consiguiente, además de la civil, también la responsabilidad penal o administrativa. Solo quedan a salvo los ámbitos expresamente excluidos en el art. 3 DCE.

Una vez perdido el puerto seguro, el intermediario solo será responsable de la infracción si se cumplen las condiciones previstas en el respectivo Estado Miembro para ello. Por consiguiente, la falta de exoneración no equivale a una correlativa y automática imputación de responsabilidad;[5] en defecto de normativa específica se exigirá, de acuerdo con las normas generales, una acción u omisión, culpa, causación de un daño y relación de causalidad (art. 1902 CC).[6] Ocurre, sin embargo, que el hecho de perder la inmunidad puede ser considerado un indicio a partir del cual deducir que el prestador tenía conocimiento o contribuyó de alguna manera al ilícito, que es, a la vez, un indicio de que no existió la diligencia debida y, por tanto, un elemento que permitiría imputarle la responsabilidad:[7] una suerte de culpa indirecta o por

[1] J. B. Nordemann, "Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?. In-Depth Analysis for the IMCO Committee", Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy: Brussels, 2018, pp. 1-28.

[2] DO L 178, de 17.07.2000. Para el detalle, A. L. Lodder, "Directive 2000/31/EC on certain legal aspects of information society services in particular electronic commerce, in the internal market", en A. Lodder – A.D. Murray (eds.), *EU-Regulation of E-Commerce. A Commentary*, Edward Elgar, Chelterham (UK) - Northampton (MA, USA), 2017, [pp. 15-58], pp. 16-17.

[3] *Digital Millenium Copyright Act*, de 28 de octubre de 1998. §§ 201-203, Public Law No. 105-304, 112 Stat. 2860. Para la comparación, M. Peguera, "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems", *Columbian Journal of Law and the Arts* (Colum.J.L.&Arts), 2009, 32, pp. 481-512. De nuevo, M. Peguera Poch, "La exoneración de responsabilidad por infracción directa en la Directiva de Derechos de autor en el mercado único digital", *Actas de Derecho Industrial* (ADI), 2018-2019, 39, [pp. 229-249], pp. 232-240. Para la evolución paralela de la interpretación jurisprudencial de las respectivas normas, en América y Europa, R. Petruso, "Responsabilità degli intermediari di internet e nuovi obblighi di conformazione: robo-takedown, policy of termination, notice and take steps", *Europa e Diritto Privato*, 2017, 2, pp. 451-510.

[4] *Vid*. Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce (Brussels, 18.11.1998, COM (1998) 586 final), p. 27; Primer Informe sobre la aplicación de la Directiva 2000/31, COM(2003) 702 final, p. 15. Además, STJUE C-236/08 – C-238/08, de 23 de marzo de 2010, *Google France* v *Vuitton et al*. (ECLI:EU:C:2010:159) (§ 107); STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§ 107). Es el modelo en el que luego se inspiraría la Member States of the Council of Europe Declaration on freedom of communication on the Internet. *Vid*. Declaración adoptada por el Consejo de Ministros (Committee of Ministers) on 28 May 2003 at the 840th Meeting of the Ministers' Deputies, especialmente el Principio 6.

[5] R. Yanguas, *Contratos de conexión a Internet, Hosting y Búsqueda*, Madrid, Civitas, 2012, pp. 369-370.

[6] Sobre los distintos tipos de responsabilidad que pueden imputarse al intermediario, G. Sartor, "Providers Liability: From the eCommerce Directive to the future", In-Dept Analysis for the IMCO Committee, IP/A/IMCO/2017-07, October 2017, p. 27. Desde un punto de vista de análisis económico, A. De Streel – M. Buiten – M. Peitz, "Liability of Online Hosting Platforms. Should Exceptionalism End?", Centre on Regulation in Europe, 2018, pp. 33 ss (disponible en: https://www.cerre.eu/sites/cerre/files/180912_CERRE_LiabilityPlatforms_Final_0.pdf).

[7] Yanguas, *Contratos...*, p. 431.

contribución a la causación del daño. Por lo general, la doctrina entiende que el estándar de conducta fijado en las normas de exclusión de responsabilidad se generaliza como paradigma de diligencia mínimo.[8]

2. La política de la Comisión Europea saliente ha sido, por un lado, fomentar la autorregulación de las empresas en la lucha contra los contenidos ilegales y, por el otro, adoptar legislación específica en áreas especialmente sensibles, como las falsificaciones, el *copyright*, el terrorismo, la incitación al odio, la pornografía infantil u otros contenidos audiovisuales nocivos.[9] Sin embargo, tras las elecciones de 2019, a la nueva Comisión Europea le parece ya llegado el momento de sustituir la norma por una moderna *Digital Services Act* o Ley de Servicios Digitales (en adelante, DSA) que, además de prescindir de la obsoleta denominación de la expresión "servicios de la sociedad de la información", lleve a cabo la necesaria actualización del régimen jurídico de los puertos seguros (*safe harbours*) o exenciones de responsabilidad de los prestadores de servicios de internet.[10]

3. Con el fin de señalar qué cambios son necesarios o por qué lo son y hasta qué punto comportan riesgos, las páginas que siguen abordan cómo hacer efectiva la responsabilidad que cabe esperar de unos intermediarios que, desde hace tiempo, se conocen ya con otro nombre: las plataformas.[11] El análisis se hace eco de los retos que la nueva economía y las modernas formas de relación social plantean al Derecho y, en particular, al Derecho privado.[12] Por eso la representación inicial, que sustentaba el desarrollo de la industria gracias a reconocer el papel neutral de los intermediarios, ha dado paso, una vez consolidada esa industria, a un nuevo régimen de imputación de responsabilidad, que exige a las empresas intervenir preventivamente para impedir el ilícito.[13]

---

[8] Entre muchos, *vid*. M. Peguera Poch, "Los prestadores de servicios de internet y la normativa sobre responsabilidad", en A. López Tarruella (dir.), *Derecho TIC. Derecho de las tecnologías de la información y de la comunicación*, Valencia, Tirant lo Blanc, 2016, pp. 77-101; J. Busto Lago, "La responsabilidad civil de los prestadores de servicios de la sociedad de la información", en L. F. Reglero Campos – J. M. Busto Lago (coords), *Tratado de Responsabilidad Civil*, Cizur Menor, Thomson-Aranzadi, 2004, 5ª ed, [pp. 597-747], p. 702.

[9] Con detalle, A. Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards*, Cambridge-Antwerp-Chicago, Intersentia, 2019, pp. 75-83. Entre los documentos, *vid*. SWD (2016)172 final, p. 7; COM (2017) 555 final; C(2018) 1177 final; SWD (2018) 408 final. Además, Recomendación 2018/334 de la Comisión de 1 de marzo de 2018 sobre medidas para combatir eficazmente los contenidos ilícitos en línea (DO L 63, de 6.3.2018). En general, *vid*. https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption.

[10] *Vid*. Orientaciones políticas para la próxima Comisión Europea 2019-2024, p. 14, presentadas por la candidata a la Presidencia de la Comisión Europea, Ursula von der Leyen: "Una nueva norma sobre servicios digitales mejorará nuestras normas de responsabilidad y seguridad para las plataformas, los servicios y los productos digitales y completará el mercado único digital". Programa disponible en: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_es.pdf (última consulta: 8.11.2019).

[11] Expresamente aludidas en la Directiva 2011/83, de 25 de octubre de 2011, sobre derechos de los consumidores (Cdos 20, 24) (DO L 304, de 22.11.2011). También se refiere a las plataformas de intercambio de vídeos el nuevo art. 1.1 a) bis de la Directiva 2010/13, de servicios de comunicación audiovisual (en adelante, DSCA), tal y como ha sido modificado por la Directiva 2018/1808 (DO L 303, de 28.11.2018). Y están ampliamente aludidas en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (DO L 186, de 11 de julio de 2019).

[12] D. Wielsch, "Private Law Regulation of Digital Intermediaries", *European Review of Private Law* (ERPL), 2019, 2, pp. 197-220. Para las transformaciones en torno a la libertad de expresión, A. Boix Palop, "La construcción de los límites a la libertad de expresión en las redes sociales", *Revista de Estudios Políticos* (REP), 2016, 173, pp. 55-112.

[13] Kuczerawy, *Intermediary...*, p. 79: "The current policy discourse is steadily shifting from intermediary liability to intermediary responsibility"; G. Frosio, "Why keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility", *International Journal of Law & Information Technology* (IJLIT), 2018, 1, [pp. 1-33], p. 8; G. Frosio, "Reforming Intermediary Liability in the Platform Economy: A European Digital Market Strategy", *Northwestern University Law Review* (NULR), 2017, 19 (112), [pp. 19-46], p. 25 (disponible en: SSRN: https://ssrn.com/abstract=2912272); A. Savin, "EU Regulatory Models for Platforms on the Content Carrier Layers: Convergence and Changing Policy Patterns", *Nordic Journal of Commercial Law*, 2018, 7, pp. 9-37; De Streel – Buiten - Peitz, "Liability of Online …", pp. 10-32 (disponible en: https://www.cerre.eu/sites/cerre/files/180912_CERRE_LiabilityPlatforms_Final_0.pdf); G. Frosio – M. Husovec, "Accountability and Responsibility of Online Intermediaries", en G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability, Oxford University Press*, 2019 (en prensa), pp. 1-17 (disponible en SSRN: https://ssrn.com/abstract=3451220).*Vid*. también M. Taddeo – L. Floridi (eds), *The Responsibilities of Online Service Providers*, Springer, Switzerland, 2017.

Las reformas a que aquí se haga referencia se explicarán a medida que se señalen las deficiencias que cabe achacar a la actual DCE; en parte, vienen anunciadas en un escueto documento de la Comisión Europea que oficialmente todavía no existe[14] y sus líneas generales han sido recientemente presentadas al Grupo de trabajo sobre telecomunicaciones y sociedad de la información en el Consejo.[15]

II. Los servicios digitales en la actualidad

4. En la DCE, la única actividad de los intermediarios que merece ser tenida en cuenta es la de quienes transmiten o alojan contenidos de terceros; se trata de las actividades de acceso, memoria tampón (*caching*) y almacenamiento (*hosting*), que pueden o no ser desarrolladas por proveedores de intermediación distintos. En particular, la actividad de acceso facilita al usuario el enlace a la red mediante la conexión inalámbrica o el cable y el otorgamiento de una IP y tiene una función meramente técnica de transmisión de información (art. 12 DCE). El almacenamiento automático, intermediario y temporal de la información transmitida (memoria tampón o *caching*) persigue reducir el tiempo de transmisión y evitar que internet se sature como consecuencia de una elevada demanda del mismo material (art. 13 DCE). El *hosting* de los datos facilitados por el destinatario del servicio en los servidores del proveedor conectados a internet permite su almacenamiento permanente (art. 14 DCE).

5. No siempre ha sido fácil encajar en algunas de esas categorías otras actividades que han ido surgiendo con posterioridad. Algunos servicios que permiten cargar *software*, gráficos y música o intercambiar información *online*, como chats o plataformas de videos o comercio electrónico, las redes sociales, los servicios peer-2-peer, los blogs o los fórums de discusión y aun otros que, sobre la base de procesos técnicos, procesan y gestionan la información y la indexan, han ido recibiendo protección específica en los Estados miembros dentro de la actividad de *hosting*, a pesar de no encontrar un anclaje claro en la DCE, donde esa función estaba reservada inicialmente al alojamiento inerte de otro tipo de datos, como páginas web, email o grupos de noticias.[16] Otras veces ha sido la jurisprudencia europea la que ha aclarado que un proveedor de acceso a una red *wifi* debía recibir la protección del art. 12 DCE siempre que el servicio constituyera una actividad económica.[17] El TJUE también ha calificado como proveedor de *hosting* a la plataforma cuyo negocio es explotar una red social en línea.[18] Sin embargo, el TJUE no ha aclarado a qué categoría se ajusta la prestación de servicios de alquiler de nombres de dominio.[19] Además, tampoco ha proporcionado soluciones unívocas para las herramientas de localización de información: a veces ha excluido la responsabilidad de los motores de búsqueda por los anuncios que enlazan con sitios web de terceros que ofrecen a la venta productos falsificados o sin el consentimiento del titular de la marca,[20] y otras veces no ha excluido la de otros proveedores de enlaces a los que, en cambio, ha considerado responsables de un acto ilícito de comunicación pública o de explotación de derechos de autor;[21]

---

[14] Documento de la DG Connect filtrado disponible en: https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/ Además, *vid*. https://euinternetpolicy.wordpress.com/2019/07/30/the-eu-digital-services-act-what-it-is-and-why-it-shouldnt-happen/ (última visita: 17.10.2019); https://www.inlinepolicy.com/blog/towards-an-enhanced-responsibility-of-online-platforms-the-eu-digital-services-act (última visita: 17.10.2019).

[15] https://www.euractiv.com/wp-content/uploads/sites/2/2019/11/DSA.pdf (última visita: 15.11.2019).

[16] *Vid.* SEC(2011) 1640/2, pp. 26-30; P. van Eecke – M. Truyens (DLA Pipper UK LLP), *EU Study on the Legal Analysis of a Single Market for the Information Society. New Rules for a New Age?. Report Study*, Smart 2007/0037, 2009, Chapter 6: Liability for online intermediaries, pp. 16-17; T. Verbiest – G. Spindler, *et al*., *Study on the Liability of Internet Intermediaries*, Markt 2006/09/E. Service Contract ETD/2006/IM/E2/69, november 2007, pp. 84 ss.

[17] STJUE C-484/14, de 15 de septiembre de 2016, *Tobbias MacFadden* (ECLI:EU:C:2016:689). Con todo, en ese caso el servicio no se proporcionaba a distancia. Llama la atención sobre ese extremo, antes de la sentencia, J. Riordan, *The Liability of Internet Intermediaries*, Oxford, Oxford University Press, 2016, p. 393. Para la discusión sobre la necesidad o no de prescindir del requisito, Lodder, "Directive 2000/31/EC...", en Lodder – Murray (eds.), *EU-Regulation...*, pp. 23-24.

[18] STJUE C-360/10, de 16 de febrero de 2012, *Netlog* (ECLI:EU:C:2012:85) (§ 27).

[19] STJUE C-521/17, 7 de agosto de 2018, *SNB-REACT* (ECLI:EU:C: 2018:639) (§§ 40 ss).

[20] STJUE C-236/08–C-238/08, de 23 de marzo de 2010, *Google France* v *Vuitton et al*. (ECLI:EU:C:2010:159).

[21] STJUE C-160/15, de 8 de septiembre de 2016, *GS Media BV* (ECLI:EU:C:2016:644); STJUE C-527/15, de 26 de abril de

y a quienes también ha juzgado infractores de la privacidad por indexar y listar información que contenía datos personales.[22]

6. Tampoco los ordenamientos jurídicos nacionales se han servido de argumentos idénticos a la hora de trazar la frontera entre los proveedores de acceso y los de alojamiento. Así, en algunos países, los motores de búsqueda reciben el mismo tratamiento que los proveedores de *hosting* (España, Portugal, Hungría) pero en otros son protegidos de manera semejante a los de acceso (Austria).[23] Para justificar esto último se argumenta que, más que en la actividad de indexación y almacenamiento, debe ponerse el énfasis en la publicación misma surgida del acto de transmisión desde el motor de búsqueda hasta terceras personas.[24] Otras veces la equiparación con los proveedores de almacenamiento se niega porque los motores de búsqueda generalmente no editan el contenido que muestran en los resultados, no son la fuente de la información a la que enlazan y no están en condiciones de eliminarla de la web.[25] Una adecuada distinción es importante ya que no se exige al proveedor de acceso que remueva el ilícito tan pronto como tenga conocimiento del mismo, como requisito para gozar de la exención de responsabilidad.[26] Ocasionalmente, y en el contexto específico del terrorismo, el Consejo Económico y Social Europeo ha llegado a sugerir la necesidad de introducir para ellos la nueva categoría de "proveedores de información".[27]

7. Adicionalmente resulta que la DCE no establece si la exclusión de responsabilidad debe aplicarse a aquellos prestadores de servicios intermediarios que, siendo a su vez destinatarios del servicio de *hosting*, permiten a sus propios usuarios crear sus contenidos, por lo menos siempre que la actividad pueda considerarse un servicio de la sociedad de la información. Inicialmente la doctrina negó esa posibilidad,[28] pero mayoritariamente no ha sido así. Normalmente se entiende que, si son ilegales los contenidos alojados en el servidor que aloja la página web de quien, a su vez, presta un servicio a sus clientes (*e.g.* el titular del sitio web que acoge el foro de discusión), a este prestador intermediario también se le deberá aplicar la exención de responsabilidad si concurren los requisitos para ello.[29] En España, por lo general, los comentarios de terceros en un blog y los mensajes en un foro o chat han sido

2017, *Stichting Brein Jack v Frederik Wullems* (ECLI:EU:C:2017:300); STJUE C-610/15, de de 14 de junio de 2017, *Stichting Brein v Ziggo BV* (ECLI:EU:C:2017:456). Pero *vid*. STJUE C-466/12, Nils Svensson (ECLI:EU:C 2014:76).

[22] STJUE C-131/12, de 13 de mayo de 2014, *Google Spain* (ECLI:EU:C:2014:317) y, en aplicación de su doctrina, por primera vez, con carácter retroactivo, SAP Barcelona (Sección 16ª) de 17 de julio de 2014, con comentario de I. Garrote Fernández-Díez, "Indemnización por daños morales derivados de la publicación de resultados en buscadores que afectan al derecho al honor e intimidad y a la protección de datos personales", *Revista de Derecho Privado* (RDP), 2015, 2, pp. 3-23. De todos modos, la protección de datos es un tema que tradicionalmente ha quedado excluido de la aplicación de la DCE (Cdo 14 y art. 1.5 letra b) DCE). Sin embargo, *vid*. ahora Cdo 21 y art. 2.4 del Reglamento 2016/679, de 27 de abril de 2016, sobre datos personales (DOU L 119, de 4.5.2016).

[23] *Vid*. las referencias que proporciona el juez Eady [2009] EWHC 1765 (QB), de 16 de julio de 2009, *Metropolitan International Schools Limited* v *Design Technica Corporation et al.* (§§ 90, 100-106). Además, J. van Hoboken, "Legal space for innovative ordering: on the need to update selection intermediary liability in the EU", *International Journal of Communications Law & Policy* (IJCL&P), 2009, 13, [pp. 1-21], pp. 8-9 y COM (2003) 702, p. 14, nota 69. Para la jurisprudencia, *vid*. SEC(2011) 1640/2, p. 27.

[24] *Vid.* Riordan, *The Liability…*, p. 397.

[25] A propósito de la regulación austríaca, Van Hoboken, "Legal space...", p. 9.

[26] Es la diferencia con respecto a los proveedores de *hosting*. *Vid.* STJUE C-484/14, de 15 de septiembre de 2016, *Tobbias MacFadden* (ECLI:EU:C:2016:689) (§§ 62-63, 65). Antes, Yanguas, *Contratos…*, pp, 255-260 y allí más bibliografía. Además, Peguera Poch, "Los prestadores de servicios…", en López-Tarruella Martínez (dir.), *Derecho TIC…*., p. 93. De acuerdo, I. Garrote Fernández-Díez, "Comentario a la STJUE, Sala 3ª, de 15 de septiembre 2016 (Asunto C-484/14)", *Cuadernos Cívitas de Jurisprudencia Civil* (CCJC), 2017, 103, [pp. 499-524], p. 517. Pero *vid*. Savin, *EU Internet Law*…, p. 155.

[27] EESC Opinion Proposal on Terrorist Content, COM(2018) 640 final-2018-0331 (COD), § 4.2 "Information providers": search engines that enable identification of and access to content. En esa línea, más genéricamente para cualquier *host*, Kuczerawy, *Intermediary...*, p. 294.

[28] A. Strowel – N. Ide – F. Verhoestraete, "La Directive du 8 Juin 2000 sur le Commerce Electronique: un Cadre Juridique pour l'Internet", *Journal des Tribunaux* (JT), 2001, [pp. 133-145], Rn. 29, p. 141.

[29] E. Staudegger, "Haftungsprivilegierung des Hostproviders oder Medieninhaberschaft – tertium non datur", *Austrian Law Journal* (ALJ), 2015, 1, [pp. 46-66], p. 46 (disponible *online* en: www.austrian-law-journal.at); Sartor, "Providers Liability…", p. 27; S. Cavanillas Múgica, "La responsabilidad de los proveedores de información en la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico", en S. Cavanillas Múgica *et al.*, *Responsabilidades de los proveedores de información en internet*, Granada, Comares, 2007, [pp. 1-39], pp. 38-39; Peguera Poch, Miquel, *La exclusión de responsabilidad de los intermediarios de internet*, Granada, Comares, 2007, pp. 274-277.

supuestos subsumidos en las normas sobre exclusión de responsabilidad del prestador de servicios de *hosting* o, a veces, estas normas se les han aplicado por analogía.[30]

8. Aun habría que saber si la exención se extiende a quienes realizan actividades puramente gratuitas que ni siquiera se financian mediante banners publicitarios (*vgr.* wikis, blogs personales o impulsados por Administraciones públicas). Si se considera que esos prestadores quedan al margen de la definición de "servicios de la sociedad de la información" entonces no gozarían del privilegio,[31] porque la DCE solo se aplica a los prestadores de servicios de la sociedad de la información y este es todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de esos servicios.[32] La definición solo incluye a los prestadores de servicios que realizan una actividad económica, aunque el servicio que prestan no sea remunerado por sus destinatarios, como sucede con el suministro de información en línea o las comunicaciones comerciales.[33] En consecuencia, solo esos prestadores gozarían del puerto seguro aunque, a veces, ha sido precisamente el ánimo de lucro lo que ha servido para endurecer los requisitos que les permitían beneficiarse del mismo.[34] La DCE deja desprotegidas frente a demandas de responsabilidad a entidades cuyo servicio no es remunerado y que económicamente no son solventes. Eso no tiene mucho sentido si, al fin y al cabo, lo que hacen unos y otros intermediarios es facilitar la comunicación al o entre usuarios.[35] Por eso algunos Estados Miembros sí aplican la exención cuando el servicio se presta con carácter gratuito.[36] También

[30] *Vid*. jurisprudencia en Peguera, *La exclusión*..., pp. 284-285; J. López Richart, "Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", *Derecho Privado y Constitución* (DPyC), 2012, 26, [pp. 143-201], pp. 162-165. En relación con los foros, STS de 7 de enero de 2014 (ECLI:ES:TS:2014:68); SAP Lugo de 9 de julio de 2009 (ECLI:ES:APLU:2009:611). A propósito de los chats, SAP Barcelona de 3 de marzo de 2010 (ES:APB:2010:2964); sobre blogs, *vid*. STS de 12 de diciembre de 2013 (ECLI:ES:TS:2013:6385); SAP A Coruña de 18 de abril de 2013 (ECLI:ES:APC:2013:1298), SAP Madrid de 31 de diciembre de 2012 (ECLI:ES:APM:2011:2467) y, por analogía, SAP Las Palmas de 5 de noviembre de 2011 (ECLI:ES:APGC:2010:2228). También en Austria, según Staudegger, "Haftungsprivilegierung...", pp. 55 ss, con argumentos críticos.

[31] Pero *vid*. recientemente la petición de decisión prejudicial planteada por el Conseil d'État (Francia), C-512/18, de 3 de agosto de 2018 — French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à internet associatifs / Premier ministre, Garde des Sceaux, ministre de la Justice. Entre nosotros, admite la exención de responsabilidad de la Administración, A. Galán Galán, "La responsabilidad por la actividad informativa de la Administración en el marco de los servicios de la sociedad de la información", *Estudios de Juventud*, 2003, 61, [pp. 17-41], p. 38.

[32] Para la definición, *vid.* art. 2 letra a) DCE, que se remite al art. 1 (2) de la Directiva 98/34, recientemente reemplazada por la Directiva 2015/1535, de 9 de septiembre de 2015 (*vid*. art. 1 (d) y Anexo I y II) (DOUE L 241, de 17.09.2015). Para un análisis global, Riordan, *The Liability*..., pp. 387-394; Lodder, "Directive 2000/31/EC ...", en Lodder – Murray (eds.), *EU-Regulation...*, pp. 22-26.

[33] Cdo 18 DCE. Además, STJUE C-291/13, de 11 de Septiembre de 2014, *Papasavvas* (ECLI:EU:C:2014:2209) (§ 30): "[…] el artículo 2, letra a), de la Directiva 2000/31 debe interpretarse en el sentido de que el concepto de «servicios de la sociedad de la información», definido en dicha disposición, incluye los servicios que ofrecen información en línea y por los cuales el prestador del servicio obtiene su remuneración, no del destinatario, sino de los ingresos generados por la publicidad que figura en una página de internet. También, STJUE C-484/14, de 15 de septiembre de 2016, *Tobbias MacFadden* (ECLI:EU:C:2016:689) (§ 41): "[…] no puede deducirse que una prestación de naturaleza económica realizada con carácter gratuito no pueda constituir en ningún caso un «servicio de la sociedad de la información» en el sentido del artículo 12, apartado 1, de la Directiva 2000/31. En efecto, la remuneración de un servicio efectuado por un prestador en el marco de su actividad económica no es necesariamente abonada por las personas que disfrutan de él". Además, STJUE C-339/15, de 4 de mayo de 2017, *Luc Vanderborght* (ECLI:EU:C:2017:335) (§ 36): "El Considerando 18 de la Directiva 2000/31 precisa que el concepto de «servicios de la sociedad de la información» cubre una amplia variedad de actividades económicas que se desarrollan en línea y que dichos servicios no se limitan únicamente a servicios que dan lugar a la contratación en línea, sino también, en la medida en que tales servicios representan una actividad económica, son extensivos a servicios no remunerados por sus destinatarios, como aquellos que consisten en ofrecer información en línea o comunicaciones comerciales". En la doctrina, *vid*. Riordan, *The Liability*..., pp. 389-390; Lodder, "Directive 2000/31/EC ...", en Lodder – Murray (eds.), *EU-Regulation...*, p. 23, p. 25. Entiende que la remuneración no tiene que ser un requisito que necesariamente deba concurrir siempre y que las actividades privadas o no empresariales no dejan por ello de ser consideradas servicios de la sociedad de la información, Garrote Fernández-Díez, "Comentario a la STJUE, Sala 3ª, de 15 de septiembre 2016…", pp. 515-516.

[34] *Vid*. STEDH 16 de junio de 2015, *Delfi AS* v *Estonia* (§§ 116, 117) [pero *vid.* el voto disidente de los jueces Sajó y Tsotsorias (§§ 44-45)]; STEDH de 2 de febrero de 2106, *Magyar Tartalomszolgaltatok Egyesülete* e *Index.hu ZRT* v *Hungary* (§ 82); STEDH de 9 de marzo de 2017, *Pihl* v *Sweden* (§ 31).

[35] Sartor, "Providers Liability…", pp. 13-14, 27; De Streel - Buiten - Peitz, "Liability of Online…", pp. 51-52; López Richart, "Difamación…", pp. 160-161.

[36] Peguera, *La exclusión*..., pp. 218, 274; P. De Miguel Asensio, *Derecho privado de internet*, Madrid, Civitas, 2015, 5ª ed., p. 258; Van Eecke - Truyens (DLA Pipper UK LLP), 'Chapter 6: Liability for online intermediaries', en EU Study on the

podría pensarse que, por lo menos alguna actividad, como la referida a los blogs personales, no es tan claro que no constituyan un servicio de la sociedad de la información porque, en realidad, no constituyen una actividad puramente privada o personal, por lo menos si se tiene en cuenta la repercusión pública y los beneficios reputacionales que se traducen en contactos en redes y seguidores. Seguramente, desde ese punto de vista, sí que existen algunos efectos económicos indirectos.[37]

9. En la Directiva 2019/790, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital (en adelante, Directiva sobre *Copyright* en el Mercado Único Digital, DCMUD), los prestadores de servicios como las plataformas para desarrollar y compartir *software* o programas informáticos de código abierto (*vgr*. GitHub), los repositorios científicos o educativos sin fines lucrativos y las enciclopedias en línea, así mismo sin fines lucrativos, no son considerados "prestadores de servicios para compartir contenidos en línea" (eventualmente responsables por la realización de actos de comunicación pública sin la pertinente licencia o autorización), pero quizás tampoco podrían ser considerados prestadores de la sociedad de la información, de acuerdo con la definición tradicional, que la Directiva no modifica (Cdo 62 y art. 2.5 y 6 DCMUD). Ocurre entonces que la aplicación del puerto seguro del art. 14 DCE no es, en realidad, segura, a pesar de la generalidad con la que se expresa el art. 17.3 II DCMUD.

El caso de los *influencers* es distinto. No cabe duda de que realizan un servicio de la sociedad de la información y de que su actividad es remunerada por las empresas para las que trabajan (aunque a veces ese dato se silencie). Sin embargo, la DCMUD establece que la licencia que obtenga la plataforma solo puede cubrir una finalidad no lucrativa; cuando no sea así, aquella será responsable, sin que pueda operar el puerto seguro (Cdo 69).[38]

10. En definitiva, es tarea del legislador europeo en el futuro aclarar qué servicios digitales merecen ser tenidos en consideración en una nueva directiva o reglamento; en particular, le corresponde decidir si es preciso un puerto seguro para las herramientas de recuperación de información (motores de búsqueda) y los puntos de acceso WiFi en cafeterías y hoteles y los servicios en la nube, las redes de entrega de contenidos, o los servicios de nombres de dominio, por citar algunos ejemplos ya mencionados en el documento filtrado sobre la DSA.[39]

1. La neutralidad de los intermediarios

11. El Cdo 42 DCE establece una distinción entre prestadores activos y pasivos. Así, solo pueden gozar de la exención de responsabilidad los prestadores que lleven a cabo una actividad meramente técnica, automática y pasiva. Eso excluye a los intermediarios cuya función no sea neutral sino "activa".

2. Proveedores activos/pasivos

12. La distinción que efectúa el Cdo 42 DCE entre prestadores activos y pasivos solo se refiere a los intermediarios de acceso y de memoria tampón (*caching*). A los prestadores de *hosting* (almace-

Legal Analysis…., p. 39. Expresamente, en Austria: § 19 (2) E-Commerce-Gesetz: "Abs. 1 sowie die §§ 13 bis 18 sind auch auf Anbieter anzuwenden, die unentgeltlich elektronische Dienste bereitstellen" (Versión de 13.11.2018). En Francia: art. 6 (2**)** Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[37] Riordan, *The Liability*…, p. 390.

[38] G. Spindler, "Responsabilidad civil y diligencia de los intermediarios desde la perspectiva de la propiedad intelectual", *LaNotaria*, 2019, 2 (en prensa).

[39] Ampliamente, sobre la tipología de intermediarios de *hosting*, sus funciones, los modelos de negocio que se desarrollan en la actualidad y los incentivos que pueden existir para combatir según qué ilícitos dependiendo de la empresa y los beneficios que se obtengan, J. Van Hoboken – J. P. Quintais – J. Poort – N. Van Eijk, "Hosting Intermediary Services and Illegal Content Online", Final Report. A Study prepared for the European Commission DG Communications Networks, Content and Technology, 2018. Smart number 2018/0033, pp. 9 ss.

namiento), de acuerdo con el art 14.1 DCE, les resultaría aplicable el Cdo 46. Sin embargo, aquellos requisitos se han extendido a estos últimos prestadores, cosa que ha sido juzgada incorrecta por buena parte de la doctrina.[40] Esa extensión fue obra de la STJUE C-236/08 – C-238/08, de 23 de marzo de 2010, *Google France* v *Vuitton*,[41] a propósito de *AdWords Google service,* que permitía a los anunciantes seleccionar una o varias palabras clave para que, en el caso de que coincidieran con las introducidas por los usuarios en el motor de búsqueda, se mostrara un enlace promocional a la página web del anunciante. Este enlace promocional aparecía bajo la rúbrica "enlaces patrocinados" e iba acompañado de un breve mensaje comercial. Los enlaces llevaban a sitios que ofrecían imitaciones de los productos de *Vuitton* -porque, junto con la marca, *Google* permitía seleccionar palabras como "imitación" o "copia"- y a productos de otros competidores. Se trataba de saber si ello suponía una infracción del derecho del titular de la marca y si *Google* gozaba del privilegio de la exención de la responsabilidad.

13. El TJUE consideró probado que el motor de búsqueda procesaba los datos proporcionados por los anunciantes y que la visualización de los anuncios se realizaba en condiciones que *Google* controlaba; ahora bien, también concluyó que la concordancia entre la palabra clave seleccionada y el término de búsqueda introducido por un internauta no bastaba por sí sola para justificar que *Google* tuviera conocimiento o control sobre los datos introducidos en su sistema por los anunciantes y almacenados en la memoria de su servidor. Por el contrario, parece que podía ser relevante el papel desempeñado por *Google* en la redacción del mensaje comercial que acompañaba al enlace promocional, o en el establecimiento o la selección de palabras clave. Desgraciadamente, el TJUE deja sin responder qué conducta se requiere para que pueda decirse que esta es algo más que meramente técnica, automática y pasiva y deja a los jueces nacionales esa tarea.[42] Lo que sí que deja claro es que el proveedor de enlaces patrocinados perdería el puerto seguro si, tras llegar a su conocimiento la ilicitud de las actividades del anunciante, no actuara con prontitud para retirar los datos o hacer que el acceso a ellos fuera imposible. Es decir, que respondería por no mantener una actitud colaborativa.

14. El anterior no es un caso aislado. A propósito de *eBay*, y en contra de la Opinión del Abogado General,[43] el TJUE también ha considerado que la plataforma de comercio electrónico juega un papel activo y, por tanto, deja de ser neutral, cuando asiste a los vendedores y promociona y fomenta las ventas de productos falsificados o que se comercializan sin el consentimiento del titular de la marca. Para el TJUE puede suponerse que esa promoción conlleva un rol activo (de distribución) que le proporciona el conocimiento o el control de las ofertas ilícitas de venta que almacena, aunque esa es una cuestión que deberá analizar el juez nacional.[44]

---

[40] Así, Riordan, *The Liability*..., no 12.119, p 402; Giovanella, Federica, "Online Service Providers' Liability, Copyright Infringement, and Freedom of Expression: Could Europe Learn from Canada?", en Taddeo - Floridi (eds), *The Responsibilities*..., [pp. 221–240], p. 231; Peguera Poch, "Los prestadores de servicios…", en López-Tarruella (dir.), *Derecho TIC*...., pp. 92-93; de nuevo, Peguera Poch, "La exoneración…", p. 239, nota 49; Kuczerawy, *Intermediary*..., pp. 97, 294. El propio Abogado General Jääskinen advertía de la incorrección. Lo recuerda ahora López Richart, Julián, "Un nuevo régimen de responsabilidad para las plataformas de almacenamiento de contenidos generados por los usuarios en el mercado único digital", *Pe.i. revista de propiedad intelectual*, 2018, 60, [pp. 67-126], pp. 83-84.

[41] ECLI:EU:C:2010:159 (§§ 113 y 116).

[42] La UK High Court no tuvo que decidir porque los litigantes llegaron a un acuerdo en 2014. Referencias en U. Carsten, "Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective", *Journal of Intellectual Property, Information Technology and Electronic* (JIPITEC), 2017, 8, [pp. 111-127], p. 115, nota 35. En el contexto del Derecho de la competencia, la SAP Madrid (Sección 28ª) de 19 de enero de 2018 (AC\2018\496) reitera la licitud del comportamiento de *Google* (que ahora ya utiliza la marca ajena como palabra clave en el servicio de referenciación), dado que la empresa solo trata, procesa, organiza y presenta la información y no redacta el mensaje comercial que acompaña al enlace promocional. En esa misma línea, SAP Alicante (Sección 8ª) de 10 de octubre de 2017 (AC\2018\25).

[43] Conclusiones del Abogado General Jääskinen en el asunto C-324/09, *L'Oréal* v *eBay*, presentadas el 9 de diciembre de 2010 (ECLI:EU:C:2010:757) (§§ 140-142, 146).

[44] STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§ 116). En esa línea, *vid.* recientemente conclusiones del Abogado General M. Campos Sánchez-Bordona, de 28 de noviembre de 2019, en el Asunto C-567/18, *Coty Germany GmbH* v *Amazon* (ECLI:EU:C:2019:1031) (§§ 56-63, 82, 84), a propósito de la implicación activa de las empresas de Amazon en la distribución de productos que infringen el derecho de marca mediante el programa "Logística de Amazón".

15. Parece claro que el criterio de la neutralidad que maneja el TJUE exige no tener el control del negocio, lo cual equivaldría a no tener participación en la creación o distribución de los contenidos.[45] Sin embargo, si incluso asuntos que tienen que ver con la infracción de la marca arrojan resultados dispares en los Estados miembros,[46] mucho más difícil puede ser establecer qué criterios llevan a perder la neutralidad en otros casos. Lo demuestra la contradictoria jurisprudencia en distintos países y aun dentro de cada país.[47] Así, mientras que en Alemania el BGH considera que un mercado en línea desempeña un papel activo cuando ofrece directamente la posibilidad de comprar desde los vínculos de la publicidad en línea,[48] en circunstancias idénticas otro tribunal había entendido antes, en los Países Bajos, que ese mercado en línea no desempeña un papel activo, sino neutro, entre sus clientes-vendedores y los compradores potenciales, de manera que debe beneficiarse del puerto seguro propio de los servicios de alojamiento.[49] En un asunto relativo a un sitio web de comparación de precios que ofrecía clasificar en los primeros puestos los productos de los comerciantes que pagaban una tasa adicional, la *Cour de Cassation* francesa constató que, al clasificar los productos en los primeros puestos y cobrar una remuneración de terceros comerciantes, la plataforma estaba promocionando indirectamente esos productos y, por tanto, actuaba como proveedor activo de un servicio comercial.[50] Por el contrario, el BGH consideró que un sitio web de valoración de hoteles no era el responsable de una opinión publicada por un usuario en la que indicaba que, en determinado hotel, «cobraban 37,50 EUR por persona y noche y había chinches», porque el sitio web no había fomentado ni difundido activamente esa opinión.[51] Con buen criterio, para saber si el prestador juega o no un rol activo, el BGH discrimina en función de si los contenidos son ajenos o pueden considerarse propios del prestador. Y, naturalmente, no es esto último lo que acaece cuando lo único que sucede es que las valoraciones otorgadas por los usuarios se evalúan estadísticamente mediante la indicación de valores medios o una "tasa de recomendación". No habría, en tal caso, tratamiento de la información o de los datos alojados y, por tanto, tampoco existiría un rol activo.[52]

16. Es evidente que aferrarse al rol activo para eliminar la exención de responsabilidad perjudica enormemente a los prestadores de servicios de internet que explotan su negocio con actividades esencialmente dinámicas que no existían cuando se aprobó la DCE y que consisten, precisamente, en optimizar la presentación de las obras o prestaciones cargadas por los usuarios y/o promocionarlas. Se diría que esos son hoy la mayoría.[53] La propia DSCA advierte que la responsabilidad de las plataformas de intercambio de videos por no proteger al público, en general, o a los menores, en particular, frente a los contenidos que inciten a la violencia o el odio, existiría como consecuencia de una mala organización (presentación, etiquetado, secuenciación, etc.) de esos contenidos. Es decir que esa "actividad" sería totalmente compatible con la exención de responsabilidad por causa de la ilicitud de los contenidos si se dieran las condiciones para que esa exención pudiera aplicarse.[54] Además, nadie diría tampoco que tiene una actitud pasiva el intermediario que, en el interés general de sus usuarios, adopta medidas de

[45] Peguera, "Los prestadores de servicios…", en López-Tarruella (dir.), *Derecho TIC*..., p. 93. Parecidamente, López Richart, "Un nuevo régimen… ", pp. 84-85.

[46] Una muestra, en relación con la jurisprudencia francesa relativa a eBay, en Carbajo Cascón, Fernando, "Sobre la responsabilidad indirecta de los agregadores de información por contribución a la infracción de derechos de propiedad industrial e intelectual en internet", ADI, 2011-2012, 32, [pp- 51-78], pp. 66-67.

[47] *Vid*. SWD (2016) 163 final, pp. 136-137. Los ejemplos de la jurisprudencia que se citan a continuación en el texto y notas que siguen se extraen de ese documento, que es una guía sobre la mejor manera de implementar la Diretiva 2005/29, sobre prácticas comerciales desleales en el nuevo contexto del e-commerce.

[48] BGH de 16 de mayo de 2013, *Stokke*/*eBay*

[49] Tribunal de Apelación de Leeuwarden, de 22 de mayo de 2012, *Stokke*/*Marktplaats B.V*.

[50] Cass. Com, de 4 de diciembre de 2012, *Publicité Sté Pewterpassion.com*/*Sté Leguide.com*.

[51] BGH de 19 de marzo de 2015, *Hotelbewertungsportal*. En la sentencia del Juzgado de Primera Instancia de Barcelona, de 18 de setiembre de 2019 (AC\2019\1201) no se duda de que Tripadvisor es un prestador de servicios de la sociedad de la información del art. 16 LSSICE, exento de responsabilidad, pero la argumentación discurre por la vía de la infracción de normas de competencia.

[52] G. Spindler,"Haftung ohne Ende? Über Stand und Zukunft der Haftung von Providern", *Multimedia und Recht* (MMR), 2018, [pp. 48-52], p. 49.

[53] Sartor, "Providers Liability…", pp. 26-27; Kuczerawy, *Intermediary...*, p. 294.

[54] Cdos 47, 48 Directiva 2018/1808 por la que se modifica la DSCA.*Vid.* el nuevo art. 1.1 a) bis DSCA.

moderación de contenidos ilícitos. Es decir que, por lo menos a los fines de que no se entienda que una política de "no tocar" contribuye a hacer posible el ilícito, se admite que el intermediario mantenga una actitud activa.[55] Con todo, esta última afirmación ha sido tradicionalmente polémica porque parece que podría chocar con los principios que inspiran la DCE y, por consiguiente, podría cuestionarse *lege lata*. No es así, pero de ello trataré con posterioridad.

17. A la vista de todo lo anterior, más que incluir a los proveedores de *hosting* activos en el ámbito de aplicación de la exención, lo mejor sería abandonar esa distinción entre "rol activo" y "rol pasivo" a la hora de calificar a los proveedores de *hosting* y reemplazar esas expresiones por otros términos más apropiados, como "grado de control", "desempeño de funciones editoriales",[56] o "conocimiento efectivo". Lo sugiere ahora el documento de la Comisión que se ha filtrado al público y al que ya he aludido con anterioridad.

3. Las plataformas colaborativas y el *copyright*

18. Antes de la promulgación de la DCMUD, en el centro de la polémica se situaba el rol de plataformas como *YouTube*, *Goear* y otras similares, porque era dudoso si la actividad de indexación y catalogación de contenidos excluía la neutralidad del prestador del servicio de alojamiento. Lo mismo cabía decir de la inserción de anuncios, la conclusión de acuerdos con quienes subían vídeos para compartir los ingresos publicitarios derivados de las visitas, o el hecho de permitir al usuario hacer el vídeo visible sólo para sus contactos y ocultar así una posible ofensa. En Italia, un tribunal entendió que nada de eso equivalía a manipular el contenido del vídeo compartido entre múltiples usuarios y, por consiguiente, aquellas actividades no afectaban a la neutralidad de la plataforma. Efectivamente, según el *Tribunale Ordinario* de Turin, 1º *Sezione Civile*, de 7 de abril de 2017:

> FJ 6.2: "[...] il Tribunale ritiene che il punto di discrimine fra fornitore neutrale e fornitore non neutrale debba essere individuato nella manipolazione o trasformazione delle informazioni o dei contenuti trasmessi o memorizzati, come peraltro suggerito (sebbene con riferimento alle attività di "mere conduit" e "caching") dal considerando n. 43 della Direttiva 2000/31/CE, estensibile, per analogia, anche al caso dell'*hosting*, nonché come anche chiarito dai successivi considerando n. 44 e 46 che richiamano l'intenzionalità e l'inerzia di fronte a specifiche informazioni dell'avvenuto illecito quali momenti di discrimine per il venir meno dell'operatività delle deroghe di responsabilità".[57]

19. También otros tribunales en Francia[58] o en España[59] han rechazado que *YouTube* desempeñara un rol activo por el hecho de tener firmados contratos con entidades de gestión de derechos de propiedad intelectual, que suponían el otorgamiento de una licencia global sobre los derechos por ellas gestionados; o por exigir una licencia de uso para subir contenidos a la plataforma; o porque en los términos de utilización del servicio se establecieran las directrices para la retirada de archivos que no se correspondieran con los términos del servicio. Tampoco les confería ese rol activo, según algunos

[55] Sartor, "Providers Liability…", p. 29: "In general, we might say that the exemptions from secondary liability should not apply when the provider contributed to the unlawful behaviour of its user by failing to exercise due care, namely, to adopt reasonable measures that could have prevented that behaviour or mitigate its effects […]"; Lodder, "Directive 2000/31/EC...", en Lodder – Murray (eds.), *EU-Regulation...*, p. 51. Por eso mismo, Kuczerawy, *Intermediary...*, p. 308, sugiere la necesidad de eliminar la diferencia entre "activo" y "pasivo".

[56] *Vid*. ya el nuevo art. 1.1 a) bis DSCA, a propósito del "servicio de intercambio de vídeos a través de plataforma" o "plataforma de intercambio de vídeos", que define como "un servicio [...] cuya finalidad [...] consiste en ofrecer al público en general programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma...".

[57] Texto completo disponible en https://www.laleggepertutti.it/wp-content/uploads/2017/04/sentenza_1928_17.pdf.

[58] Tribunal Grand d'Instance de Paris (3è Ch, 1ère Section), de 29 de mayo de 2012, *TF 1 et autres* v *Youtube*, disponible en https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-3eme-chambre-1ere-section-jugement-du-29-mai-2012/

[59] JUR 2014\36900. *Vid*. FJ 15-17.

jueces, que el personal de *YouTube* seleccionara determinados vídeos de entre los popularizados por los usuarios del sistema, o los hiciera figurar en la sección de videos destacados, según las sugerencias que estos últimos les hicieran llegar. Según la SAP Madrid de 14 de enero de 2014 (Sección 28ª), ninguna de esas actividades determina la existencia de conocimiento o control:

> "La índole de tales labores, frente a lo que se nos quiere hacer ver por las recurrentes, no resiste la menor comparación con la de las que fueron objeto de consideración en las sentencias Google France y L'Oreal" (FJ 17).

20. Sin embargo, es evidente que otros casos se han resuelto de manera distinta, fruto de la percepción que el modelo de negocio se basaba esencialmente en la violación de derechos de autor.[60] En el contexto de los hipervínculos que proporcionan enlaces a obras protegidas sin autorización de su autor, el TJUE ha establecido una presunción *iuris tantum* de conocimiento del ilícito cuando esa actividad se realizaba con ánimo de lucro y ha entendido que no operaba la exención de responsabilidad, por considerar que existía una intervención activa de puesta a disposición de la obra.[61] Las hipotéticas infracciones también alcanzan a la publicación gratuita de contenidos de audio en internet, a los reproductores multimedia con hipervínculos preinstalados que permiten acceder en *streaming* a obras ilegalmente publicadas en internet y a intercambios de ficheros protegidos sin autorización del titular mediante redes p2p.[62]

21. Todo ello ha llevado a los legisladores nacional[63] y europeo a replantear el rol de los intermediarios de internet y, en particular, las grandes plataformas sin cuya colaboración los terceros no podrían llevar a cabo actos ilícitos contrarios a la propiedad intelectual de los autores. Precedida de la jurisprudencia del TJUE que, con argumentos más o menos convincentes, ha tratado de combatir la piratería,[64] ahora la DCMUD pretende que los proveedores de servicios de la sociedad de la información cuyo negocio sea reproducir o referenciar de forma automática cantidades significativas de obras visuales protegidas por derechos de autor (*Youtube*, *Facebook*, *DailyMotion*, etc.) concluyan acuerdos con todos los titulares de derechos, con el fin de garantizar la remuneración equitativa de los mismos ("*value gap*"). Así que esas plataformas que permiten cargar contenidos no autorizados son responsables, por el mero hecho de almacenar y facilitar el acceso a los contenidos almacenados por otros, de un acto de comunicación pública de obras protegidas por derecho de autor.[65]

---

[60] LG Hamburg (310 O 461/10), de 20 de abril de 2012, *GEMA* v *Youtube*.

[61] Para el análisis, *vid*. I. Garrote Fernández-Díez, "El concepto autónomo de «comunicación al público» en la jurisprudencia del TJUE", *Pe. i. revista de propiedad intelectual,* 2019, 61, pp. 13-67; A. Rubí Puig – P. Rivas, "El nuevo derecho de acceso (Evolución de la jurisprudencia del TJUE en materia de comunicación al público en relación con las actividades que facilitan el acceso a obras protegidas)", *Pe. i. revista de propiedad intelectual*, 2018, 58, pp. 13-86. Analizan -y afirman- la compatibilidad de la jurisprudencia del TJUE con la DCE, Nordemann, "Liability of Online Services..", pp. 22-24; Rubí Puig – Rivas, "El nuevo derecho de acceso…", pp. 79-81.

[62] A propósito del prestador que permite compartir archivos protegidos por derechos de autor sin autorización de sus titulares mediante redes p2p, *vid.* STJUE C-610/15, de 14 de junio de 2017, *Stichting Brein* v *Ziggo BV* (ECLI:EU:C:2017:456) (§§ 26, 29 36-37). En España, hay un antes y un después, que viene marcado por la L. 2/2014. Para las sentencias más recientes, *vid*. SAP Madrid (Sección 28º) de 4 de diciembre de 2017 (AC 2017/1593), sobre enlaces "e2dk" (a las redes de pares); sobre la actividad infractora de "Roja Directa", *vid*. Juzgado de lo Mercantil de A Coruña de 1 de febrero de 2017 (AC/2017/306) y SAP La Coruña (Sección 4ª) de 28 de diciembre de 2018 (AC/2019/194); en relación con *Goear*, *vid.* STS (Sala 3ª) de 27 de junio de 2019 (RJ\2019\2604). En cuanto a las páginas para subir enlaces, *vid*. todavía la sentencia del Juzgado de lo Penal nº 4 de Murcia, de 21 de junio de 2019 (ARP\2019\930), que absuelve a los intermediarios demandados. *Vid*. recientemente, M. Orozco González, *Nuevos retos de los derechos de autor en la sociedad digital*, Cizur Menor, Aranzadi, 2019, pp. 224 ss.

[63] En Alemania, *vid*. el nuevo § 8 (1) TMG, que exige intencionalidad. En España, *vid*. art. 138.2, 195.2 letra b) TR-LPI.

[64] Fundamentalmente, STJUE C160/15, de 8 de septiembre de 2016, *GS Media BV* (ECLI:EU:C:2016:644); STJUE C-527/15, de 26 de abril de 2017, *Stichting Brein Jack* v *Frederik Wullems* (ECLI:EU:C:2017:300); STJUE C-610/15, de 14 de junio de 2017, *Stichting Brein* v *Ziggo BV* (ECLI:EU:C:2017:456).

[65] Aunque en relación con la Propuesta DCMUD, señala el apartamiento que supone de la jurisprudencia del TJUE, que siempre había exigido el conocimiento, López Richart, "Un nuevo régimen…", p. 124. Sobre los niveles de conocimiento, Rubí Puig – Rivas, "El nuevo derecho de acceso…", pp. 63-66.

22. Inicialmente la Propuesta de DCMUD, de 14 de septiembre de 2016, iba más allá de la STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay*, al excluir de la exención de responsabilidad a todos los "*hosting* activos", sin importar en absoluto la manera en que se pudiera llevar a cabo la optimización de los contenidos.[66] La expresión "*hosting* activo" ha desaparecido en la DCMUD finalmente aprobada pero, seguramente, eso ha sido a costa de eliminar la cualificación como intermediario de las grandes plataformas de difusión de música y videos (art. 17.3 I DCMUD).[67] Con todo, no puede desconocerse que su condición de prestadores de *hosting* no desaparece si se trata de juzgar infracciones distintas de la vulneración de derechos de autor, incluso cuando este último tipo de infracciones también concurra (Cdo 65, art. 17.3 II DCMUD).[68] Puesto que en esos casos sí que puede regir el puerto seguro del art. 14 DCE, algún autor ha concluido que lo único que sucede es que estas plataformas ya no gozarán de exención cuando cometan una infracción directa.[69] Efectivamente, parece que la calificación como *hosting* para un mismo proveedor no puede depender de que se cometan unos u otros ilícitos. Ahora bien, no es descartable que sea eso exactamente lo que ocurra, si se admite que la calificación puede estar en función de la directiva que en cada caso se declare aplicable. Puede ser argumento que refuerce la condición de intermediaria de la plataforma que el Cdo 66 afirme que no es ella la que carga los contenidos y que, a pesar de que no exista una mención explícita al art. 15 DCE, la referencia a ese artículo esté implícita en el art. 17.8 DCE.[70] La DCMUD se aprueba mientras están pendientes de resolución dos cuestiones prejudiciales que, entre otras demandas, precisamente tratan de aclarar eso mismo.[71]

23. En cualquier caso, es significativo el cambio de perspectiva: a diferencia del art. 14 DCE, que se pronuncia en términos de exención (condicionada) de responsabilidad -a partir del conocimiento y retirada o *take down*-, la DCMUD se expresa en términos de responsabilidad directa de las empresas que, a su vez, también se presenta condicionada a una serie de requisitos: que obtengan licencias, o que filtren y bloqueen contenidos (Cdo 66 I-IV y art. 17.4 DCMUD). Dejando de lado las limitaciones aplicables a empresas más jóvenes o de menor tamaño (art. 17.6 DCMUD), no cabe duda de que la norma perjudica la difusión de contenidos generados por los usuarios que son, generalmente, obras compuestas o derivadas en los que se integran contenidos de terceros (*e.g*. música, fotos) que no necesariamente encontrarán acomodo en las excepciones.[72] Se trata de excepciones que, por lo demás, no queda claro que sean obligatorias en todos los Estados.[73] Además, si la licencia no ha sido concedida previamente por el

[66] Cdo 38 y art. 13 COM(2016) 593 final. Muy críticos, Carsten, "Standarts for Duty of Care?...", p. 116; S. Stalla-Bourdillon, "Des intermédiaires de l'Internet aux plateformes en ligne en passant par les fournisseurs d'hébergement: repenser le paradigme «de la neutralité» à l'aune des droits fondamentaux", en J. Sénéchal – S. Stalla-Bourdillon (dirs.), *Rôle et responsabilité des opérateurs de plateforme en ligne: aproche(s) transverale(s) ou aproches sectorielles ?*, Paris, Institut de Recherche Juridique de la Sorbonne, 2018, [pp. 61-86], pp. 73-74. Entre nosotros, López Richart, "Un nuevo régimen… ", pp. 94-98.

[67] Cdos 62, 63 y arts. 2.6, 17.3 DCMUD.

[68] Orozco González, *Nuevos retos*..., p. 187. Antes, en relación con la Propuesta de Directiva, López Richart, "Un nuevo régimen…", pp. 97-98.

[69] Que las infracciones directas están amparadas por el puerto seguro no es afirmación unánime, pero lo sostiene Peguera Poch, "La exoneración…", pp. 237-241.

[70] Peguera Poch, "La exoneración…", p. 241, nota 57; p. 245, nota 86.

[71] Petición de decisión prejudicial planteada por el Bundesgerichtshof (Alemania), C-682/18, de 6 de noviembre de 2018 — LF / Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH; Petición de decisión prejudicial planteada por el Bundesgerichtshof (Alemania), C-683/18, de 6 de noviembre de 2018 — Elsevier Inc. / Cyando AG.

[72] Para la definición y problemática que encierran esos contenidos, *vid.* R. Evangelio Llorca – J. López Richart, "El derecho de autor en el entorno digital", en López-Tarruella (dir.), *Derecho TIC*...., [pp. 163-208], pp. 169-172. Con más detalle, a propósito de la posibilidad de salvar los límites establecidos en la Directiva 2001/29, *vid*. I. Garrote Fernández-Díez, "¿Puede crearse un nuevo límite en la ley de propiedad intelectual española para dar cobertura a los contenidos generados por los usuarios?", en J. J. Marín López – R. Casas Vallès – J. C. Sánchez Aristi (coords.), *Estudios sobre la ley de propiedad intelectual: últimas reformas y materias pendientes*, Madrid, Dyckinson, 2016, pp. 257-295.

[73] Compárese el Cdo 70 DCMUD: "Esas excepciones y limitaciones deben por lo tanto ser obligatorias a fin de garantizar que los usuarios reciban una protección uniforme en toda la Unión", con el art. 17.7 DCMUD: "Los Estados miembros garantizarán que los usuarios en cada Estado miembro puedan ampararse en cualquiera de las siguientes excepciones o limitaciones vigentes". Lo advierte Peguera Poch, "La exoneración…", p. 246. Sin embargo, puede que "vigentes" no se refiera las efectivamente existentes en los Estados Miembros, sino a las existentes ya en la Unión Europea (en el art. 5 Directiva InfoSoc). Para esa consideración y aun otras que tratan de asegurar una recta aplicación del art. 17 DCMUD, *vid*. J. Quintais – G. Frosio – S.

autor será difícil obtenerla cuando quien suba los contenidos sea persona distinta y ello induce a pensar que solo se cargarán los contenidos que hayan sido previamente autorizados.[74] Es problemática también la manera prevista para detectar las ilegalidades. A ello se aludirá más adelante.

III. El control editorial

24. Uno de los criterios que tradicionalmente se ha hecho servir para considerar que los intermediarios no merecen el puerto seguro al que pretenden acogerse es el del control editorial o, lo que es lo mismo, la "selección" o "modificación" de contenidos. En particular, el art. 12 DCE solo permite a los proveedores de acceso manipulaciones técnicas en el contenido transmitido (Cdo 43). Aunque en ningún lugar la DCE explica lo que eso significa, cabe entender incluidas en la expresión actividades como la compresión de datos para reducir el tamaño de un fichero,[75] la fragmentación de los ficheros o el añadido de una información de cabecera,[76] e incluso la eliminación automática de virus o spam de los correos electrónicos.[77] Por su parte, el proveedor de *hosting* pierde el privilegio si aloja contenido ilegal bajo la dirección o control del intermediario (art. 14.2 DCE). En tal caso, el contenido ya no puede tratarse como si proviniera de terceros, sino del propio prestador que, en consecuencia, dejaría de comportarse como mero intermediario.[78] Tanto el art. 12 como el art. 14 DCE son problemáticos.

25. El art. 12 DCE es problemático porque, como ya se ha dicho, no explica en qué consisten las "modificaciones técnicas" y, por consiguiente, se han planteado interrogantes en torno a si actividades voluntarias distintas de las mencionadas con anterioridad de filtrado de tráfico, inserción de anuncios en páginas web, o el filtrado textual de conversaciones de chat pueden entrar en esas categorías.[79] La limitación voluntaria del acceso a ciertos contenidos que pueden ser considerados ilícitos o perjudiciales, como la pornografía, la pedofilia, el abuso sexual o la incitación al odio no debería estar penalizado, no solo porque ese actuar beneficia a todos los usuarios, sino porque claramente el intermediario no hace suyo el contenido que transmite al impedir su circulación.[80] Sin embargo, qué duda cabe de que *lege lata* existe el riesgo de que esa actuación pudiera ser cualificada de control editorial.[81] Además, los intermediarios no son jueces y un exceso de celo podría comportar una censura indebida, que es todo lo contrario a la finalidad perseguida con la instauración del puerto seguro.

26. La situación descrita en el art. 14.2 DC, que establece que la exención no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios, concurre

---

Van Gompel – P. B. Hugenholtz – M. Husovec – B. J. Jütte – M. Senftleben, "Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics" (November 11, 2019), p. 3 (en SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3484968) (última consulta: 12.11.2019).

[74] Peguera Poch, "La exoneración…", p. 246.

[75] Ahora lo prevé expresamente el Cdo 11 Reglamento 2015/2120, por el que se establecen medidas en relación con el acceso a una internet abierta (DO L 310, de 26.11.2015).

[76] UK Department of Trade and Industry, A Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013), p. 25, Regulation 17 (1): "Manipulations of a technical nature that take place in the course of the transmission (*e.g.* the automatic adding of headers) [...] do not fail this test if they do not alter the integrity of the information contained in the transmission" (disponible en: https://webarchive.nationalarchives.gov.uk/20121212135622/http:/www.bis.gov.uk/files/file14635.pdf) (última visita: 7.12.2019).

[77] UK Department of Trade, A Guide…, p. 25, Regulation 17 (1): "[...] the automated removal of viruses from emails do not fail this test if they do not alter the integrity of the information contained in the transmission".

[78] M. Clemente Meoro, "La responsabilidad civil de los prestadores de servicios de la sociedad de la información", en M. Clemente Meoro – S. Cavanillas Múgica, *Responsabilidad civil y contratos en internet*, Granada, Comares, 2003, [pp. 1-116], p. 98; M. Tescaro, "Die zivilrechtliche Haftung von Internet-Providern in Italien: Umsetzung der E-Commerce-Richlinie gegen Tendenzen der Rechtsprechung", *Zeitschrift für das Privatrecht der Europäischen Union* (GPR), 2014, 5, [pp. 270-277], p. 271.

[79] Van Eecke -Truyens (DLA Pipper UK LLP), 'Chapter 6: Liability for online intermediaries', en EU Study on the Legal Analysis…, p 14.

[80] Peguera, *La exclusión*..., pp. 247-248.

[81] Savin, *EU Internet Law*..., p. 155.

cuando el destinatario del servicio trabaja (elabora contenidos) para el prestador, que actúa como su empleador o supervisor.[82] El control no se ejerce sobre la información, sino sobre la actuación del destinatario del servicio.[83]

Sin embargo, se ha afirmado que el contenido generado por el usuario puede entenderse creado bajo el control del prestador cuando el intermediario especifica, en los términos y condiciones para el acceso, qué puede o no ser publicado en la plataforma participativa (*e.g*. *Facebook*) y también cuando se reserva la facultad de editar los contenidos generados por el usuario (*e.g*. Wikipedia).[84] También a veces se entiende que el prestador tiene control sobre el usuario mediante el moderador del foro o grupo de noticias.[85] En particular, la STEDH de 16 de junio de 2015, *Delfi AS* v *Estonia*, equipara al editor de prensa el intermediario que gestiona un portal de noticias de Internet que permite a sus lectores introducir comentarios (aunque es así solo porque estima que en ambos casos se trata de una gestión profesional que tiene carácter comercial).[86]

27. El control que ejercen los intermediarios en todas esas situaciones nunca puede equipararse a un control editorial por varias razones: son los usuarios quienes eligen al intermediario y no al revés, no es posible identificar a los destinatarios del servicio, y es muy dificil moderar en tiempo real; esto último debe entenderse como imposibilidad de llevar a cabo una censura previa, a diferencia de lo que sucede con las cartas de los lectores en un diario.[87] Tampoco la moderación *a posteriori* podría ser un indicio de que esos contenidos son introducidos a instancias del proveedor de servicios o de que este los selecciona y -aunque este ya es otro tema- mucho menos puede entenderse que el hecho de moderar le proporciona un conocimiento del ilícito que le hace perder la exención.[88]

Hay que asumir, en favor de la libertad de expresión y en pro de la innovación, que lo mejor que pueden hacer los prestadores de servicios de internet es facilitar canales para que fluya la información. Con esa finalidad, también la *Communications Decency Act* americana protege tanto a los proveedores de servicios de internet como a los que permiten interactuar a sus usuarios gracias a la publicación de sus contenidos.[89]

---

[82] Lodder, "Directive 2000/31/EC...", en Lodder – Murray (eds.), *EU-Regulation...*, p. 52; M. Barrio Andrés, *Fundamentos del Derecho de internet*, Madrid, CEPC, 2017, p. 381; Kuczerawy, *Intermediary...*, pp. 62-63.

[83] *Vid*. COM (1998) 586 final, p. 30: "It should be stressed that the relevant control is the control of the recipient's acts and not the control over the information as such"; Lodder, "Directive 2000/31/EC...", en Lodder – Murray (eds.), *EU-Regulation...*, p. 52. Por el contrario, P. Baistrocchi, "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce", *Santa Clara HTLJ,* 2003, 19, [pp. 111-130], p. 123: "[...] the ISPs may be held liable if they have some form of "control" over the information"; Savin, *EU Internet Law*..., p. 162: "The presence of such editing potentially removes liability protection and turns intermediaries into editors who bear primary or secondary liability".

[84] Barrio, *Fundamentos*..., p. 381. Por el contrario, *vid.* Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries [Marzo 2018]. Apéndice 1.3.3: "When intermediaries remove content based on their own terms and conditions of service, this should not be considered a form of control that makes them liable for the third party content for which they provide access".

[85] Para la discusión en los distintos derechos nacionales, Verbiest - Spindler *et al.*, *Study on the Liability*..., p. 47.

[86] STEDH de 16 de junio de 2015, *Delfi AS* v *Estonia* (§§ 115-116).

[87] *Vid.* el voto particular disidente de los jueces Sajó y Tsotsorias en la STEDH de 16 de junio de 2015, *Delfi AS* v *Estonia* (§ 47): "[…] in normal circumstances the active intermediary has no personal control over the person who posts the message. The commenter is not the employee of the publisher and in most cases is not known to the publisher. The publication occurs without the decision of the editor. Hence, the level of knowledge and control differ significantly"; (§ 48): "Control *presupposes* knowledge. In this regard the difference between the editor/publisher and the active intermediary is obvious." Sobre la aplicación del art. 65 de la Ley de Prensa en internet, con opiniones no coincidentes con las expresadas en el texto, *vid*. P. Grimalt Servera, "La responsabilidad de los proveedores de información en internet y la Ley 14/1966, de Prensa e Imprenta", en Cavanillas Múgica *et al*, *Responsabilidades...*, [pp. 41-81], pp. 68 ss.

[88] Cavanillas Múgica, "La responsabilidad...", en Cavanillas Múgica *et al*, *Responsabilidades...,* p. 37; López Richart, "Difamación…", pp. 187-188, con crítica a jurisprudencia nacional contraria. Recientemente, a partir de exigir el control del moderador sobre la información publicada en el foro con contenidos patentemente ilícitos, STS de 26 de febrero de 2013 (RJ2013\2580); STS de 5 de mayo de 2016 (RJ 2016\2451).

[89] 47 U.S.C. § 230 (c) (1) Communication Decency Act. Sobre la misma, Kuczerawy, *Intermediary...*, pp. 67-73, esp. pp. 70-73 y pp. 268 ss.

IV. El conocimiento de la ilicitud

28. Los arts. 13-14 DCE establecen la exención de responsabilidad para la actividad de *caching* (copia temporal) y *hosting* (almacenamiento), siempre que el proveedor elimine el contenido ilegal tan pronto como tenga conocimiento de la ilicitud. En relación con la actividad de *hosting*, el art. 14.1 a) DCE recalca que puede tratarse de un conocimiento presunto o indiciario, pero esto último solo si se pretende reclamar daños y perjuicios; es decir, solo si se exige responsabilidad civil.[90] Por otro lado, ya se ha dicho que el art. 12 DCE no exige el conocimiento de la infracción a los proveedores de acceso.

29. La DCE no aclara si el conocimiento efectivo o presunto de la ilicitud debe referirse a informaciones ilícitas concretas o si basta con un conocimiento general de que el proveedor puede albergar contenidos ilícitos. Desde luego, esto último pondría mucha más presión sobre el intermediario y por eso debe rechazarse. [91] La cuestión ha sido sometida a la consideración del TJUE aunque, en relación con el *copyright*, la respuesta tendrá poco recorrido, una vez aprobada la DCMUD.[92]

30. Cómo adquiere el prestador conocimiento de que aloja contenidos ilícitos ha sido resuelto por la STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay*. En esa sentencia, el TJUE decidió que, para que se le niegue al prestador de un servicio de la sociedad de la información la posibilidad de acogerse a la exclusión de responsabilidad prevista en el art. 14 DCE, basta con que aquél haya tenido conocimiento de hechos o circunstancias a partir de las que un operador económico diligente hubiera debido deducir ese carácter ilícito. Según el TJUE serviría cualquier situación mediante la cual el prestatario en cuestión adquiera conocimiento, de una forma o de otra, de tales hechos o circunstancias. Esto comprende su propia investigación, la notificación de terceros, o la evidencia de la ilegalidad. En España los tribunales han declarado reiteradamente que no es preciso esperar a obtener una resolución judicial o administrativa.[93] Aunque, desde luego, el único medio seguro para hacer adquirir conocimiento de la infracción al prestador intermediario es la sentencia o resolución del organismo competente (*vgr*. la Comisión para la Defensa de los Derechos de Propiedad Intelectual; la Agencia de Protección de Datos), si estas fueran la única fuente de conocimiento, probablemente llevaría demasiado tiempo dar satisfacción a las víctimas y no evitaría que en el ínterim se cometieran nuevas infracciones. Si, además, la infracción fuera evidente, la necesidad de obtener una resolución no haría más que incrementar el perjuicio.[94]

1. La diligencia del operador económico

31. El deber de diligencia o *duty of care* es un concepto vago, cuya definición la DCE abandona a los Derechos nacionales, que son los que deberían concretar las medidas que lo ejemplifican. El dato

[90] Contra esa interpretación, *vid*. las conclusiones del Abogado General Jaäskinen, de 9 de diciembre de 2010, en el Asunto C-324/09 (*L'Oréal*) (§§ 162-163) (ECLI:EU:C:2010:757).

[91] Contra esa posibilidad, Giovanella, "Online Service Providers' Liability…", en Taddeo-Floridi (eds), *The Responsibilities…*, p. 231; López Richart, "Un nuevo régimen…", pp. 76-77. En esa línea, sentencia del Juzgado de lo Mercantil núm. 7 de Madrid de 20 de septiembre de 2010 (AC 2010/1462), en cita e interpretación de A. Rubí Puig, "Derecho al honor *online* y responsabilidad civil de los ISPs", *InDret*, 2010, 4, [pp. 1-20], pp. 17-18.

[92] *Vid.* Petición de decisión prejudicial planteada por el Bundesgerichtshof (Alemania), C-683/18, de 6 de noviembre de 2018 — Elsevier Inc. / Cyando AG. Además, Petición de decisión prejudicial planteada por el Bundesgerichtshof (Alemania), C-682/18, de 6 de noviembre de 2018 — LF / Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH.

[93] Sobre el particular, Rubí Puig, "Derecho al honor…", esp. pp. 12 ss; Carbajo, "Sobre la responsabilidad…", pp. 56-57.

[94] STS de 7 de enero de 2014 (ECLI:ES:TS:2014:68): "[...] es claro que, en el actual mundo de las telecomunicaciones, caracterizado por la facilidad y rapidez de difusión de los datos, remitir al perjudicado a la previa obtención de una declaración formal de ilicitud, cuando la intromisión en el derecho fundamental al honor es tan notoria como en el caso que nos ocupa [...] multiplicaría los perjuicios ocasionados, hasta el extremo de que, cuando obtuviese respuesta a la tutela judicial pretendida, aquellos perjuicios pudieran ser ya irreparables". Idem, STS de 5 de mayo de 2016 (RJ 2016\2451). Se hace eco, Juzgado de Primera Instancia e Instrucción de Purchena (Almería), de 18 de septiembre de 2018 (JUR\2018\96977). En la doctrina, De Miguel, *Derecho privado…*, p. 261; Sin embargo, el Juzgado de lo Penal nº 4 de Murcia, de 21 de junio de 2019 (ARP\2019\930), en el famoso caso "Serieyonkis", interpreta literalmente el art. 16 LSSICE y exige una sentencia para que el intermediario pueda conocer la ilictud.

cierto es que el prestador infringe ese deber siempre que conociera o debiera haber conocido la actividad ilegal y, sin embargo, no hubiera hecho nada por bloquearla o removerla.[95] Es decir que la diligencia exigiría una actuación reactiva. La cuestión es si, además, obliga a tomar medidas voluntarias y preventivas, proactivas, para impedir que la ilicitud tenga lugar. Parece que sí, que los intermediarios deberían adoptar especiales deberes de cuidado, a la vista de la exigencia prevista en el Cdo 48, que permite a los Estados miembros exigir a los prestadores de servicios de *hosting* la diligencia que razonablemente pudiera esperarse para detectar y prevenir determinados tipos de actividades ilegales. Ahora bien, por un lado, ese Cdo 48 al que se acaba de aludir preceptúa que tal deber de diligencia venga concretado legalmente ("*que esté especificado en el Derecho nacional*"). Esto no solo se refiere a los ámbitos concretos de actuación en relación con "casos específicos" (Cdo 47) -por ejemplo, ante ilegalidades manifiestas, como pornografía infantil, incitación al odio o enaltecimiento del terrorismo-, sino que, seguramente, se refiere también a las medidas que los prestadores deberían adoptar.[96] Por otro lado, existe el límite del art. 15.1 DCE, que prohíbe el control general de todos los contenidos y no permite que pueda obligarse a los intermediarios a buscar hechos ilícitos "en general". Un control general es difícil por la cantidad de contenidos que circulan por internet[97] y seguramente exigiría costes excesivos a las empresas que, de esta manera, perderían incentivos para invertir en el negocio; además, se pondría en riesgo la libertad de expresión e información de los usuarios. Con todo, eso es así, en teoría; en la práctica, las cosas han ido por otros derroteros. De ello se tratará más adelante.

32. El deber de diligencia no puede equivaler a un deber de vigilancia permanente, porque eso equivaldría a establecer la responsabilidad objetiva del intermediario por el mero hecho de poner a disposición del público herramientas y espacios que faciliten las actividades ilegales.[98] El mismo Cdo 48 DCE alude a la diligencia, que "cabe esperar razonablemente" de los prestadores. Por el contrario, la solución que finalmente ofrece la DCMUD es la de exigirles "los mayores esfuerzos" por garantizar la indisponibilidad de obras sin licencias de acuerdo con normas sectoriales *estrictas* de diligencia profesional y los desarrollos (incluso futuros) de la industria (Cdo 66 II, art. 17.4 letra b). La diligencia tiene que adaptarse a la tecnología y el modelo de las empresas, pero la amenaza de imputación de responsabilidad que, a su vez, viene determinada por el nivel de actividad de esas empresas, les obliga a crear esa tecnología y, por consiguiente, a incrementar su nivel de control.[99]

33. Todavía existe el peligro de que la adopción voluntaria de medidas para prevenir el ilícito se identifique con un conocimiento de la ilegalidad que acabe terminando por calificar al proveedor de "activo". Llama mucho la atención la insistencia con que la Comisión Europea reitera que las medidas voluntarias adoptadas para aumentar la confianza y ofrecer un servicio más competitivo no deben interpretarse automáticamente en el sentido de que el funcionamiento de la plataforma ya no es meramente técnico, automático y pasivo.[100] La objeción no es muy razonable si, a fin de cuentas, ese conocimiento sirve para eliminar el ilícito.[101] Pero insiste en ello, recientemente, la Recomendación 2018/334, relativa

[95] STJUE C160/15, de 8 de septiembre de 2016, *GS Media BV* (ECLI:EU:C:2016:644) (§ 49) (ECLI:EU:C:2016:644); STJUE C-236/08 – C-238/08, de 23 de marzo de 2010, *Google France* v *Vuitton et al*. (ECLI:EU:C:2010:159) (§ 120); STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§§ 120, 124).

[96] La cuestión es discutida. *Vid*. Van Hoboken – Quintais – Poort – Van Eijk, "Hosting Intermediary Services….", pp. 43-45.

[97] Savin, *EU Internet Law...*, pp. 161–162.

[98] *Vid*. la opinión disidente conjunta de los jueces Sajó y Tsotsorias en STEDH 16 de junio de 2015, *Delfi AS v Estonia* (§ 51); STEDH de 2 de febrero de 2106, *Magyar Tartalomszolgaltatok Egyesülete* e *Index.hu ZRT* v *Hungary* (§ 83); STEDH de 9 de marzo de 2017, *Pihl* v *Sweden* (§ 31). Además, Opinión del Abogado General Szpunar, de 4 de junio de 2018, en el Asunto C-18/18, *Glawischnig-Piesczek* (ECLI:EU:C:2019:458) (§§ 36–39, 51).

[99] *Vid*. COM (2017) 555 final, p. 14, en cuanto a la imposición de desarrollar tecnología adecuada: "La Comisión insta a adoptar nuevos enfoques de investigación e innovación que vayan más allá del estado actual de la técnica con el fin de mejorar la exactitud de los medios técnicos de identificación de contenidos ilícitos. Asimismo, insta al sector a que introduzca de forma efectiva innovaciones que contribuyan a incrementar la eficiencia y eficacia de los procedimientos de detección automáticos."

[100] COM(2016) 356 final, p. 8; COM (2017) 555 final, pp. 12-13. Crítica con ese razonamiento, Kuczerawy, *Intermediary...*, pp. 293-294.

[101] En otro orden de consideraciones, pero en una línea parecida a lo que aquí se discute, también el art. 20.2 RD 1889/2011,

a las medidas para combatir eficazmente los contenidos ilícitos en línea, que además considera esencial que todas ellas sean proporcionadas y estén sujetas a salvaguardias efectivas y adecuadas.[102] Lo que, sorprendentemente, ninguno de esos documentos aclara es qué consecuencias tendría que, a pesar de actuar de buena fe y con todas las garantías y salvaguardias, los proveedores no eliminasen los contenidos que resultaran ser ilícitos o impidieran el acceso a otros que no lo fueran.[103] El documento que contiene las líneas generales con el contenido de una futura DSA se propone clarificar esa ausencia de responsabilidad. Con buen criterio, la *House of Lords* ya ha sugerido que la acción de responsabilidad contra los proveedores solo debería tener lugar ante fallos sistémicos.[104]

34. Por lo general, los Estados miembros han fomentado la cooperación entre los intermediarios y las autoridades y han sugerido que se adopten voluntariamente medidas para prevenir la ilegalidad y su repetición. A ello me referiré con posterioridad.

2. La notificación

35. Si no media resolución judicial o administrativa, será la víctima quien notifique la ilicitud al intermediario, pero nada impide que los notificantes sean terceros a quienes, en definitiva, también les interesa velar por la limpieza de los contenidos en línea, *e.g.* con el fin de que se borren los datos personales de una víctima de violación, o se bloquee la difusión de material pornográfico infantil en la red.[105] Ese es precisamente el papel de los llamados *trusted flaggers* o notificantes fiables.[106] Por otra parte, está claro que no pueden existir límites a la legitimación para efectuar esa notificación si se recomienda o permite que esta se lleve a cabo anónimamente.[107]

36. La DCE no establece cómo deben identificarse los hechos ilícitos. Algunos tribunales europeos son muy rigurosos con los requisitos que debe reunir la notificación de terceros para que pueda entenderse que, efectivamente, existe conocimiento. En Francia no solo se exige el detalle de la identificación del notificante, sino también una descripción de los hechos controvertidos y su localización precisa; las razones por las que debe suprimirse el contenido, incluida una referencia a las disposiciones legales y la prueba de los hechos; una copia de la correspondencia dirigida al autor o al editor de la información o de las actividades controvertidas en la que se solicite su interrupción, supresión o modificación, o la prueba de que no se pudo contactar con el autor o el editor.[108] En Alemania, la notificación debe estar redactada de manera tan concreta que el destinatario de la misma debe poder determinar fácilmente la

---

de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual, admitía que la interrupción del servicio o retirada voluntaria [*atendiendo al requerimiento de la Comisión de Propiedad Intelectual*] tenía el valor de reconocimiento implícito de la referida vulneración. Lógicamente, el precepto fue declarado nulo por la STS (Sala 3ª) de 31 de mayo de 2013.

[102] Recomendación 2018/334, Cdos 24-27, §§ 18-20, 36-37.

[103] *Vid*. Kuczerawy, *Intermediary...*, p. 295, que señala las diferencias con la auténtica cláusula del buen samaritano americana (cfr. pp. 70-71, 295-296); Van Hoboken – Quintais – Poort – Van Eijk, "Hosting Intermediary Services….", p. 42; De Streel - Buiten - Peitz, "Liability of Online…", pp. 45, 53.

[104] House of Lords. Select Committee on Communications. 2nd Report of Session 2017-2019, "Regulating in a digital world" (printed 26 February and published 9 March 2019), pp. 53-54, 55.

[105] COM(2017) 555 final, p. 10: "debe facultarse a los usuarios corrientes para que llamen la atención de las plataformas sobre contenidos ilícitos en linea […]". En el contexto de las redes sociales, Soler Presas, Ana, "Am I in Facebook?", *InDret*, 2011, 3, [pp. 1-44], pp. 28 ss, admite que la legitimación para solicitar la remoción de contenidos y, en general, exigir deberes de cuidado pueda corresponder a cualquier usuario de la red, por razón de la relación contractual que mantiene con el prestador, aunque no sea él la víctima. Los usuarios de Internet que se encuentren con material pornográfico infantil en línea también deben poder denunciar,*vid*. COM(2016) 872 final, p. 5. Sin embargo, el art. 17.9 II DCMUD solo se refiere a los titulares de derechos: "Cuando los titulares de derechos soliciten que se inhabilite el acceso a obras u otras prestaciones específicas suyas o que se retiren tales obras o prestaciones…".

[106] Recomendación 2018/334, Cdos 29, 34, § 4 letra g), §§ 25-27. Antes, COM(2017) 555 final, pp. 9-10.

[107] Sobre el anonimato y la legitimación de cualquier persona, *vid*. Cdos 16, 18, § 4 letras e), f), § 7 Recomendación 2018/334.

[108] Cass. Civ. I, de 17 de febrero de 2011, *Dailymotion*; Cass. Civ. I, de 17 de febrero de 2011, *Amen*. *Vid*. art. 6 I 5 Loi n° 2004-575 de 21 de junio de 2004.

violación de la ley, sin un examen legal o real detallado. La medida en que el operador de una plataforma está obligado a llevar a cabo dicho examen depende de las circunstancias del caso concreto, en particular del peso de las infracciones notificadas, por una parte, y de la capacidad del operador para identificarlas, por otra.[109] En Inglaterra, los jueces coinciden en la necesidad de especificar en cualquier notificación el nombre completo y la dirección del remitente de la notificación, los detalles de la ubicación de la información en cuestión y los detalles de la naturaleza ilegal de la actividad o información en cuestión. Además, aun sería preciso examinar y considerar, con conocimiento de causa, la validez o la solidez de los medios de defensa disponibles.[110]

Entre nosotros, la doctrina ha sugerido propuestas similares, al amparo de lo dispuesto en la *Millenium Copyright Act* (DMCA).[111] De momento, alguna sentencia ha exigido adjuntar copia de la resolución que acreditaba que la información a la que remitía el motor de búsqueda era falsa y no ha estimado suficiente poner en conocimiento del prestador de servicios el inicio de acciones civiles; por supuesto, los hechos relatados deben sean ciertos.[112] A pesar de que se debería exigir un particular deber de cuidado en la identificación de esos hechos,[113] en algunos casos que han llegado a los tribunales el notificante ni siquiera explicaba qué comentarios eran los que consideraba ofensivos, aunque al final el dato no ha acabado siendo muy relevante a la vista de unos daños que se deducían *ex re ipsa*.[114]

37. Si se trata de infracciones de derechos de propiedad intelectual, parece evidente que la notificación debe permitir identificar exactamente la actividad ilícita, la obra o prestación, el titular de los derechos correspondientes y, al menos, una ubicación donde la obra o prestación es ofrecida. La DCMUD todavía alude a conceptos vagos como la "información pertinente y necesaria" y "motivada" o "debidamente justificada" de los titulares de derechos (art. 17.4 letras b) y c), art. 17.9 II DCMUD).[115] Algo más explícita, la Comunicación de la Comisión Europea sobre la lucha de los contenidos en línea admitía que debían justificarse las razones y localizar los contenidos potencialmente ilícitos, que es algo que luego ha traslucido en la Recomendación 2018/334.[116]Puesto que los Estados miembros pueden realizar ulteriores concreciones y, quizás, establecer requisitos distintos en función de los tipos de contenidos (eg. la identificación del notificante), sería deseable confeccionar una "hoja de notificación europea", en su caso adaptada a distintas posibles infracciones, que pudiera aplicarse uniformemente en todos los países de la UE.

3. La ilicitud manifiesta

38. El conocimiento de la manifiesta ilicitud puede venir proporcionado, además de por una orden judicial, por la previa notificación de un tercero; ahora bien, la propia evidencia puede servir también para que el operador económico conozca por sí mismo. La STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay*, no distingue. El problema es que, a falta de indicaciones legales claras, no siempre será fácil determinar cuando el ilícito es evidente, en particular cuando sea necesario tener

[109] BGH de 17 de agosto de 2011, *Stiftparfum* (§ 31).

[110] EWHC 449 (QB), de 2 de marzo de 2012, *Tamiz* v *Google Inc.* (§ 59) y The Electronic Commerce (EC Directive) Regulations 2002: Regulation 22 [Notice for the purposes of actual knowledge].

[111] 17 USC § 512 c) 3. *Vid*. Rubí Puig, "Derecho al honor *online*....", pp. 16-17.

[112] STS de 4 de marzo de 2013 (RJ 2013\3380).

[113] Rubí Puig, "Derecho al honor *online*…", 14 ss.

[114] STS de 26 de febrero de 2013 (RJ/2013/2580).

[115] STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§ 122): "suficientemente fundamentada". *Vid*. también Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries [Marzo 2018]. Apéndice 1.3.7: "sufficient information".

[116] COM(2017) 555, p. 11; Cap. II § 6 Recomendación 2018/334: "notificaciones que sean suficientemente precisas y estén debidamente fundamentadas [...] [y mecanismos que faciliten] la comunicación de notificaciones que expliquen las razones por las que el notificante considera que esos contenidos son ilícitos y una indicación clara de su localización". No aporta mayor luz la definición de "notificación" contenida en el Cap. I, § 4 letra e): "comunicación dirigida a un prestador de servicios de alojamiento de datos por un notificante en relación con contenidos almacenados por dicho prestador que el notificante considere que constituyen contenidos ilícitos y con respecto al cual solicite al prestador su retirada o el bloqueo del acceso sobre una base voluntaria".

en cuenta los diversos ámbitos o escenarios en que puede cometerse la infracción.[117] Ese riesgo no ha desaparecido en relación con las infracciones de *copyright*, aunque la nueva directiva exija licencia de uso de los contenidos que carguen los usuarios, porque todavía pueden considerarse lícitas comunicaciones que no necesitan licencia. Es lo que sucederá si la obra ya ha entrado en el dominio público o los contenidos están amparados por las excepciones previstas en la propia norma. Eso es algo que el prestador puede no conocer y que las técnicas automáticas de filtrado -cuando sean aplicables- pueden muy bien no detectar, sobre todo si se tiene en cuenta que estas se activan según la información proporcionada por los titulares de derechos y estos pueden muy bien (voluntariamente o no) no decir la verdad (art. 17.7 y 9 II y III DCMUD). Muy complicado puede resultar también valorar lo ilícito de un comentario en un foro o blog, especialmente si resulta que su carácter ilegal depende de que la información difundida sea verdad.[118] En definitiva, puede ser difícil establecer cuál es la línea que separa la infracción, constitutiva de una verdadera lesión, de lo que puedan ser declaraciones ofensivas de mal gusto o mala educación.[119]

39. Un botón de muestra de la dificultad a la que se acaba de aludir es la STEDH de 16 de junio de 2015, *Delfi AS* v *Estonia*, que condena a un portal de noticias por no haber retirado a tiempo comentarios de los lectores a un artículo allí publicado. La sentencia afirma que los comentarios de terceros que implican odio y amenazas contra la integridad personal de los individuos justifican imponer responsabilidad al portal de noticias que no retira inmediatamente los que son claramente ilícitos o ilegales, incluso sin necesidad de que nadie lo notifique.[120] Sin embargo, el voto disidente de los jueces Sajó y Tsotsorias hacen notar que el mismo Tribunal Supremo de Estonia calificaba dichos comentarios de forma imprecisa, a veces como un discurso de incitación al odio, otras como una lesión al honor;[121] y otros votos particulares a esa misma sentencia, de los jueces Raimondi, Karakaş, De Gaetano y Kjølbro, aun manifestándose partidarios de lo decidido por la mayoría, reconocían que para poder afirmar que el portal de noticias debía tener conocimiento de comentarios claramente ilícitos, como insultos, amenazas o expresiones de odio, el Tribunal debía fijar claramente qué parámetros debían tomarse en consideración: no solo la naturaleza del comentario, sino también el contexto en que se publicaba, el tema del artículo que generaba esos comentarios, la envergadura o finalidad del portal del noticias en cuestión, su historia, el número de comentarios generados por el artículo publicado, la actividad del portal y cuánto tiempo los mismos permanecían visibles.[122]

En otro caso en que un tribunal nacional húngaro consideraba que una injuria en absoluto venía avalada por la libertad de expresión, la STEDH de 2 de febrero de 2106, *Magyar Tartalomszolgaltatok Egyesülete e Index.hu ZRT* v *Hungary* entendió que no existe esa interferencia cuando lo único que se expresan son opiniones o juicios de valor; esto es, cuando el ataque a la reputación de la persona no reviste gravedad y, como mucho, es simplemente ofensivo o vulgar. Y, a la hora de valorarlo, no solo

[117] Son algunos de los problemas que se achacan a la ley alemana NetzDG (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (*Netzwerkdurchsetzungsgesetz*), de 1 de septiembre de 2017, disponible en: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Para la crítica, G. Spindler, "Internet Intermediary Liability Reloaded. The New German Act on Responsibility of Social Networks and its (In-) Compatibility with European Law", JIPITEC, 2017, 8, pp. 166-179.

[118] *Vid*. STS de 4 de diciembre de 2013 (RJ 2013\195) que, a propósito del uso de la expresión "ladrón", da preferencia a la libertad de expresión frente al derecho al honor, precisamente porque estaba pendiente una sentencia que podía dar la razón a quién de aquella manera se expresaba. El Juzgado de Primera Instancia e Instrucción de Purchena (Almería), de 18 de septiembre de 2018 (JUR\2018\96977) no condena a Google porque su buscador autocomplete la búsqueda asociada al nombre de una persona jurídica con la expresión "blanqueo de dinero", por existir indicios de veracidad de la sugerencia, además de entender que *Google* había actuado diligentemente al comprobar esa posible veracidad y concluir que debía prevalecer la libertad de expresión.

[119] Cavanillas Múgica, "La responsabilidad…", en Cavanillas Múgica *et al*, *Responsabilidades...,* p. 30. Contrastar la STEDH de 16 de junio de 2015, *Delfi AS* v *Estonia* con STEDH de 9 de marzo de 2017, *Pihl* v *Sweden* y STEDH de 19 de marzo de 2019, *Høiness* v *Norway*.

[120] STEDH de 16 de junio de 2015, *Delfi AS* v *Estonia* (§ 159).

[121] Voto disidente de los jueces Sajó y Tsotsorias, en TEDH de 16 de junio de 2015, *Delfi AS* v *Estonia* (§§ 28; además, §§ 29-31).

[122] Voto concurrente de los jueces Raimondi, Karakaş, De Gaetano y Kjølbro en TEDH, de 16 de junio de 2015, *Delfi AS* v *Estonia* (§ 12, además §§ 11, 13-15).

cuenta el contexto en que son proferidas esas opiniones, sino también el estilo de comunicación propio de internet.[123] En esa misma línea se pronuncia la reciente STEDH *Høiness* v *Norway*.[124]

40. En España, admitir como indicio de conocimiento efectivo lo patente o evidente de la lesión ha dado pie a los tribunales a exigir al intermediario "extremar las precauciones y ejercer mayor control sobre las opiniones y comentarios alojados [en el foro]".[125] Con ello se podría estar sugiriendo que al moderar, el administrador del foro hace suyos los contenidos de terceros -interpretación que convendría evitar- o, más claramente, se estaría afirmando que es necesario introducir un control general de vigilancia antes de proceder a la publicación del (de cualquier) comentario que es lo que, precisamente, la ley expresamente prohibe (art. 15 DCE).

41. El documento filtrado que contiene el borrador con las líneas básicas para la actualización de la DCE solo contiene la noción "actual knowledge" y no se refiere ya al conocimiento presunto. Sin embargo, eso no debe llevar a engaño porque la contrapartida es el incremento de las medidas de control y prevención que deben llevar a obtener ese conocimiento.

V. El control del tráfico de internet

42. De acuerdo con el art. 15 DCE, no existe un deber general de controlar la información que los intermediarios transmiten o almacenan, ni tampoco una obligación de buscar hechos o circunstancias que indiquen que tiene lugar una actividad ilegal. En 1998, la Propuesta de DCE admitía que los jueces pudieran imponer actividades de vigilancia selectiva y temporal, para salvaguardar la seguridad nacional y para la prevención, investigación, detección y enjuiciamiento de delitos, de acuerdo con la legislación nacional, por razones de seguridad pública,[126] pero lo único que queda de esa regla es el mucho más genérico Cdo 47, que permite las "órdenes formuladas de acuerdo con la legislación nacional". El Reglamento por el que se establecen medidas sobre el acceso a una red abierta recuerda que las medidas de gestión del tráfico que adopten los intermediarios no deben poder supervisar el contenido específico y que no se deberán poder mantener por más tiempo del necesario.[127]

43. Además, el art. 15.2 DCE permite a los Estados miembros exigir que comuniquen con prontitud a las autoridades competentes los presuntos datos o actividades ilícitas llevadas a cabo por destinatarios de su servicio o comunicarles, a solicitud de aquellas, información que les permita identificar a aquellos con los que hayan celebrado acuerdos de almacenamiento. La Recomendación 2018/334 insiste en la necesidad de que los Estados miembros hagan uso de la posibilidad que ofrece ese artículo a efectos de la prevención, investigación, detección o enjuiciamiento de delitos.[128] Se trata, pues, de que las empresas hagan de espías de sus usuarios para los Estados.[129] Aun así, la STJUE C-275/06, de 29 de enero de 2008, *Promusicae* afirmó que esta disposición -al igual que otras, en diferentes Directivas- no obliga a los Estados miembros a establecer una obligación de comunicar datos personales de los presuntos infractores de los derechos de autor en el contexto de un procedimiento civil; más bien se requería una evaluación equilibrada de todos los derechos fundamentales en juego.[130] Otra reciente cuestión prejudicial ofrece una nueva posibilidad de pronunciamiento.[131] De momento, la DSA guarda silencio sobre

[123] STEDH de 2 de febrero de 2106, *Magyar Tartalomszolgaltatok Egyesülete* e *Index.hu ZRT* v *Hungary* (§§ 74-77). Kuczerawy, *Intermediary...*, p. 175.

[124] STEDH de 19 de marzo de 2019, *Høiness* v *Norway* (§§ 67, 69).

[125] STS de 26 de febrero de 2013 (RJ 2013\2580); STS de 5 de mayo de 2016 (RJ 2016\2451).

[126] COM (1998) 586 final, p. 47.

[127] Art. 3.3 Reglamento 2015/2120.

[128] Recomendación 2018/334, Cdo 28, Capítulo II, § 24.

[129] Savin, *EU Internet Law…*, p. 162.

[130] ECLI:EU:C:2008:54 (§§ 59, 61–70); Auto TJUE, C-557/07, de 19 de febrero de 2009, *LSG* v *Tele 2* (ECLI:EU:C:2009:107) (§§ 29, 47).

[131] Cuestión prejudicial planteada por el *Conseil d'État* (Francia) el 3 de agosto de 2018: C-512/18 *La Quadrature du Net*

este punto, pero no es verosímil que no se incorpore este mandato del actual art. 15 DCE en la norma que en el futuro reemplace a la actual DCE.

1. Alcance de las órdenes judiciales

44. El art. 15.1 DCE es una norma dirigida a los Estados miembros, que limita la responsabilidad de los intermediarios y desempeña un papel crucial a la hora de determinar el alcance de su responsabilidad. Por consiguiente, los jueces que conocen de las reclamaciones de las víctimas y ordenan medidas para el cese de la infracción deben ajustarse a lo dispuesto en ese precepto. En la STJUE C-70/10, de 14 de noviembre de 2011, *Sabam* v *Starlet*, el TJUE confirmó, igual que ya hiciera en la STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay*, que el art. 15.1 DCE prohibe una orden judicial que exija que el proveedor de servicios de internet instale un sistema de filtrado que le obligue a controlar activamente todos los datos relativos a cada uno de sus clientes para evitar futuras infracciones de los derechos de propiedad intelectual. En particular, no admitió un sistema de filtrado que suponía que el prestador de servicios de internet identificara, en primer lugar, de entre el conjunto de las comunicaciones electrónicas de todos sus clientes, los archivos correspondientes al tráfico «peer-to-peer»; que identificara, en segundo lugar, en el ámbito de dicho tráfico, los archivos que contuvieran obras sobre las que los titulares de derechos de propiedad intelectual tuvieran supuestamente derechos; que determinara, en tercer lugar, cuáles de esos archivos se intercambiaban de un modo ilícito; y que procediera, en cuarto lugar, a bloquear los intercambios de archivos que considerara ilícitos. En el caso concreto, proteger a los titulares de los derechos de propiedad intelectual no debía ir en detrimento de la libertad de empresa de los intermediarios, ni del derecho a la protección de datos de los clientes de los intermediarios o su libertad de recibir o comunicar informaciones, que son derechos salvaguardados por los arts. 8 y 11 de la Carta de Derechos fundamentales de la Unión Europea. El TJUE trae a colación el caso *Promusicae* para recordar que la protección del derecho fundamental de propiedad, del que forman parte los derechos vinculados a la propiedad intelectual, debe ponderarse con respecto a la protección de otros derechos fundamentales. Los intermediarios quedan eximidos de una carga que puede ser imposible de cumplir o solo mediante costes que podrían menoscabar el desarrollo del negocio, lo cual atentaría contra la libertad de empresa, y en aras del respeto de los derechos fundamentales de los usuarios de internet, como la libertad de expresión o de información y la privacidad.

> STJUE C-70/10, de 14 de noviembre de 2011, *Sabam* v *Starlet* : (§ 50) […] los efectos de dicho requerimiento judicial no se limitarían al PAI afectado, ya que el sistema de filtrado litigioso también puede vulnerar los derechos fundamentales de los clientes de ese PAI, a saber, su derecho a la protección de datos de carácter personal y su libertad de recibir o comunicar informaciones, derechos que se encuentran protegidos por los artículos 8 y 11 de la Carta (§ 51). En efecto, consta en autos, por un lado, que el requerimiento judicial por el que se ordena establecer el sistema de filtrado litigioso implicaría un análisis sistemático de todos los contenidos y la recopilación e identificación de las direcciones IP de los usuarios que hayan originado el envío de contenidos ilícitos en la red, dándose la circunstancia de que dichas direcciones son datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios (§ 52). Por otro lado, dicho requerimiento judicial podría vulnerar la libertad de información, dado que se corre el riesgo de que el citado sistema no distinga suficientemente entre contenidos lícitos e ilícitos, por lo que su establecimiento podría dar lugar al bloqueo de comunicaciones de contenido lícito. En efecto, es incontrovertido que el carácter lícito de una transmisión depende igualmente de la aplicación de excepciones legales a los derechos de autor que varían de un Estado miembro a otro. Además, en determinados Estados, ciertas obras pueden pertenecer al dominio público o los autores afectados pueden ponerlas gratuitamente a disposición pública en internet (§ 53). Por consiguiente, procede declarar que, si adoptara el requerimiento judicial por el que se obliga al PAI a establecer el sistema de filtrado litigioso,

(DO C 392, 29.10.2018, p. 7–8). En particular, se pregunta si es compatible con los arts. 6-8, 11 y 52.1 de la Carta de Derechos Fundamentales de la Unión Europea la obligación de conservar los datos que puedan permitir la identificación de quien haya contribuido a la creación del contenido o de alguno de los contenidos de los servicios de comunicación al público prestados por empresas, o personas que los almacenen, incluso de forma gratuita, con el fin de que la autoridad judicial pueda requerir, en su caso, la comunicación de los mismos para que se respeten las normas en materia de responsabilidad civil o penal.

el órgano jurisdiccional nacional en cuestión no respetaría el requisito de garantizar un justo equilibrio entre, por un lado, el derecho de propiedad intelectual y, por otro, la libertad de empresa, el derecho a la protección de datos de carácter personal y la libertad de recibir o comunicar informaciones".[132]

45. En la STJUE C-314/12, de 27 de marzo de 2014, *Telekabel*, se confirmó la necesidad de preservar ese equilibrio de derechos entre proveedores de contenidos, titulares de derechos e intermediarios;[133] sin embargo, más que especificar qué medidas concretas podían adoptarse, el TJUE puso el acento en que esas medidas debían ser las que mejor se adapten a los recursos y capacidades de que disponga el intermediario y que sean compatibles con las demás obligaciones y retos a que deba hacer frente en el ejercicio de su actividad; admitió que este no debe hacer sacrificios insostenibles, teniendo en cuenta que él no es el autor de la vulneración del derecho fundamental de propiedad intelectual. Por otra parte, reconoce que no cabe excluir que no exista técnica alguna que permita poner fin por completo a las violaciones del derecho de propiedad intelectual, o que dicha técnica no sea realizable en la práctica, lo que tendría como consecuencia que determinadas medidas adoptadas podrían, en su caso, eludirse de uno u otro modo.[134]

En cualquier caso, añade que las medidas adoptadas por el destinatario de un requerimiento judicial deben ser suficientemente eficaces para garantizar una protección efectiva del derecho fundamental de que se trata, es decir que deben tener como efecto impedir o, al menos, hacer difícilmente realizable, el acceso no autorizado a las prestaciones protegidas y disuadir seriamente a los usuarios de internet que recurran a los servicios del destinatario de dicho requerimiento de acceder a esas prestaciones puestas a su disposición en violación del mencionado derecho fundamental.[135]

46. En la STJUE C-484/14, de 15 de septiembre de 2016, *Tobbias MacFadden*, tras recordar de nuevo que el control de todos los datos transmitidos debe ser excluido,[136] el TJUE no admitió la medida que consiste en cerrar completamente la conexión a Internet; consideró que medidas menos coercitivas son más respetuosas con la actividad económica que consiste en facilitar acceso a internet y, por consiguiente, declaró que el remedio a la infracción del derecho de autor no debía comportar una restricción absoluta de la libertad de empresa.[137] Señaló que la solución que consiste en proteger la conexión a internet mediante una contraseña sirve para disuadir a los usuarios de esta conexión de vulnerar un derecho de autor o un derecho afín a un derecho de autor siempre que dichos usuarios estén obligados a revelar su identidad para obtener la contraseña requerida y no puedan actuar anónimamente.[138] A su vez, consideró que así no afectado ni el derecho a la libertad de empresa del prestador que facilita un servicio de acceso a una red de comunicaciones, ni el derecho a la libertad de información de los destinatarios de ese servicio.[139]

47. En la reciente STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek*, el TJUE se ha apartado de la jurisprudencia anterior.[140] En un caso de difamación, el TJUE admite que el art. 15.1 DCE no resulta violado cuando un tribunal exige al prestador de servicios de alojamiento de datos "que bloquee el acceso a los datos almacenados cuyo contenido sea idéntico al que se ha declarado ilícito con anterioridad, o retire esos datos, sea quien fuere el autor de la solicitud de su almacenamiento."[141] El TJUE admite asimismo que es posible "obligar a un prestador de servicios de alojamiento de datos a suprimir los datos que almacene, y cuyo contenido sea similar al de una información declarada ilícita con

[132] Además, §§ 47-49, 52 (ECLI:EU:C:2011:771). Antes, STJUE C-360/10, de 16 de febrero de 2012, *Netlog* (ECLI:EU:C:2012:85) (§§ 45–52).

[133] ECLI:EU:C:2014:192 (§§ 46-47).

[134] ECLI:EU:C:2014:192 (§§ 49-56).

[135] ECLI:EU:C:2014:192 (§ 63).

[136] ECLI:EU:C:2016:689 (§ 87).

[137] ECLI:EU:C:2016:689 (§ 88)

[138] ECLI:EU:C:2016:689 (§ 96).

[139] ECLI:EU:C:2016:689 (§§ 91, 92, 100).

[140] ECLI:EU:C:2019:821. Para una valoración provisional, *vid.* L. Woods en: http://eulawanalysis.blogspot.com/2019/10/facebooks-liability-for-defamatory.html (última visita: 24.10.2019).

[141] STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek* (ECLI:EU:C:2019:821) (§§ 37, 53).

anterioridad, o a bloquear el acceso a ellos, siempre que la supervisión y la búsqueda de los datos a los que se refiere tal medida cautelar se limiten a aquellos datos 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 la medida cautelar acordada" y 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".[142] El TJUE parece ignorar deliberadamente que tal búsqueda de información requiere necesariamente la supervisión de los datos almacenados de todos los usuarios y que ello puede repercutir negativamente en la privacidad. La sentencia también es problemática porque no ofrece orientación sobre cómo analizar la similitud o equivalencia de los contenidos. Además, el TJUE legitima el uso de técnicas de filtrado automático que no tienen en cuenta el contexto en el que se reproducen las palabras ofensivas, pero no parece aceptar la posibilidad de una revisión humana para contrarestar los efectos de un filtrado y bloqueos inadecuado. Sin duda, analizar contenidos similares sería mucho más fácil si se tratara de identificar imágenes y/o si dependiera del conocimiento que el operador pudiera tener de las circunstancias. La sentencia tampoco excluye el efecto mundial de la orden de bloqueo y retirada, si eso no está excluido en el marco del derecho internacional de cada Estado Miembro.[143]

48. Resumidamente, puede decirse, pues, que, en los casos de infracción de los derechos de propiedad intelectual, el TJUE acepta órdenes para evitar nuevas infracciones, [144] del mismo tipo y por el mismo infractor, aunque no necesariamente contra las mismas marcas,[145] y añade que dichas medidas preventivas pueden consistir en suspender las cuentas de los usuarios infractores o en proporcionar información que contribuya a identificarlos.[146] Además confirma que otras medidas más agresivas, como la inspección general y permanente de todo el contenido, no son aceptables. Sin embargo, la doctrina del caso *Glawischnig*, dictada en un caso de difamación, en una plataforma de redes sociales -aunque podría generalizarse a otras hipótesis- admite que pueda controlarse el contenido de todos los usuarios y no solo en la búsqueda de ilícitos ya declarados, sino también de otros parecidos.

2. La iniciativa del intermediario

49. Muy frecuentemente la Comisión Europea ha fomentado la autorregulación y ha alentado a los intermediarios a que voluntariamente adoptaran medidas que impidieran la transmisión o almacenamiento de contenidos ilícitos.[147] Entre los códigos de conducta promovidos por la Comisión Europea puede contarse el Código de conducta para la lucha contra las declaraciones de incitación al odio en línea,[148] el Memorándum de Acuerdo sobre la falsificación de mercancías,[149] o el Foro de Internet de la

[142] STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek* (ECLI:EU:C:2019:821) (§§ 41-47, 53).

[143] STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek* (ECLI:EU:C:2019:821) (§§ 50-52, 53). *Vid*. STJUE C-507/17, de 24 de septiembre de 2019, *Google LLC* (ECLI:EU:C:2019:772).

[144] STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§§ 131, 144); STJUE C-70/10, de 24 de noviembre de 2011, *Scarlet Extended* (ECLI:EU:C:2011:771) (§ 31); STJUE C-360/10, de 16 de febrero de 2012, *Netlog* (ECLI:EU:C:2012:85) (§ 29).

[145] STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§ 141): "para evitar que el mismo comerciante vuelva a cometer infracciones de esta naturaleza en relación con las mismas marcas"; STJEU C-494/15, de 7 de julio de 2016, *Tommy Hilfiger* (ECLI:EU:C:2016:528) (§ 34): "se puede obligar al intermediario a que adopte medidas que contribuyan a evitar que se produzcan nuevas infracciones de la misma naturaleza por parte del mismo comerciante". La idea de que las futuras infracciones deberían referirse a las mismas marcas no se refleja en la segunda sentencia.

[146] STJUE C-324/09, de 12 de julio de 2011, *L'Oréal* v *eBay* (ECLI:EU:C:2011:474) (§§ 141-142); STJUE C-484/14, de 15 de septiembre de 2016, *Tobbias MacFadden* (ECLI:EU:C:2016:689) (§ 96).

[147] COM(2017) 555 final, pp. 11-13; Cdos 24, 26 y Cap. II §§ 18, 28 y Cap. III §§ 36-37 Recomendación 2018/334. A propósito de los códigos de conducta, *vid*. antes Cdos 32, 49, art. 16 DCE.

[148] Code of conduct for countering illegal hate speech online, disponible en: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300

[149] *MoU on Counterfeit Goods*, disponible en: https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_es

UE.[150] Otros tratan de prevenir los contenidos audiovisuales nocivos.[151] Esa estrategia ha permitido a los gobiernos eludir la prohibición de control general (que se dirige exclusivamente a los Estados Miembros) y delegar la vigilancia de internet en operadores privados. Es una práctica censurable, porque deja en manos de estos últimos decidir como debe ser el comportamiento de los usuarios en internet.[152] Por eso es un paso en la buena dirección que, desde el año 2015, el Reglamento 2015/2120, por el que se establecen medidas en relación con el acceso a una internet abierta, no permita la adaptación de medidas restrictivas del tráfico si no existe fundamento jurídico para ello.[153]

50. Sin embargo, son cada vez más las normas que imponen a los intermediarios el deber de tomar la iniciativa y adoptar medidas en ámbitos específicos, e.g. en relación con las plataformas de intercambio de videos nocivos,[154] o a propósito del enaltecimiento del terrorismo.[155] A veces se permite incluso a los Estados miembros imponer medidas más detalladas o estrictas que las previstas por el legislador europeo. Así sucede en relación con los servicios de comunicación audiovisual o las plataformas de comercio electrónico.[156] Se advierte que todas esas medidas deben ser viables y proporcionadas y no discriminatorias y que deben tener en cuenta, por un lado, la categoría de personas que deben protegerse, el tamaño y la naturaleza del servicio que se presta, la viabilidad económica para la empresa y la forma en que tales medidas pueden afectar a los derechos e intereses de los destinatarios del servicio (principio de proporcionalidad).[157] Eso significa que la pertinencia y adecuación de las que deban adoptarse concretamente (*e.g.* filtrado automatizado de palabras clave o contenidos infractores; bloqueo de sitios web, URLs y clientes; mecanismos de revisión humana; y eliminación de contenidos ilícitos mediante sistemas de notificación y retirada, etc.) deberá juzgarse caso por caso.

51. Ahora bien, puesto que la DCE carece de claridad sobre cómo esa prohibición de control general es compatible con las obligaciones de diligencia de los proveedores de alojamiento, es difícil definir el alcance de las medidas a adoptar y, por consiguiente, también el de las órdenes judiciales a que se refiere el art. 15.1 DCE.

El resultado ha sido sentencias contradictorias en los Estados Miembros, si bien muchos jueces nacionales han acabado imponiendo la obligación de actuar en función de la capacidad técnica de las grandes empresas a la luz de los programas ya existentes (por ejemplo, PhotoDNA, iWatch, Content-ID) aunque también se les ha obligado a crear otros para remover ilícitos idénticos o similares.[158] Un ejemplo claro es la saga de sentencias en el asunto *Max Mosley* v *Google*, de los tribunales francés,[159] alemán,[160] e inglés,[161] que obligaron al intermediario a tomar medidas para que fotografías tomadas ilegalmente

---

[150] *EU Internet Forum*, disponible en: https://www.eif*online*.org/about-us/about-eif.html

[151] Art. 4 bis, art. 28 ter 2 IV DSCA, según modificacion de la Directiva 2018/1808.

152 *Vid.* Recommendation CM/Rec (2018) 2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries. Apéndice 1.1.1: "States should not exert pressure on internet intermediaries through non-legal means". En la doctrina, G. Frosio – S. Mendis, "Monitoring and Filtering: European Reform or Global Trend?" (September 9, 2019), en G. Frosio (ed), *The Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2019 (en prensa), pp. 13-14 (disponible en SSRN: https://ssrn.com/abstract=3450194 or http://dx.doi.org/10.2139/ssrn.3450194 .

[153] Cdos 11, 13 y art. 3.3 letra a), art. 10.3 Reglamento 2015/2120.

[154] Art. 28 *ter* 3 DSCA, tal y como han sido incorporado por la Directiva 2018/1808.

[155] COM(2018)640 final, en particular art. 6. Pero *vid*. Parlamento Europeo, Enmiendas 85-88. La Propuesta, tras la Primera lectura llevada a cabo por el Parlamento y tras la aceptación de enmiendas por el Consejo puede leerse en https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8663_2019_INIT&qid=1573035054776&from=ES

[156] Art. 28 ter 6 DSCA, tal y como han sido incorporados por la Directiva 2018/1808; Cdos 28-29, art. 6 bis 2 Directiva 2019/2161, sobre la mejora de la aplicación y modernización de las normas de protección de los consumidores de la UE.

[157] Sartor, "Providers Liability…", pp. 29-31; Carsten, "Standards for Duty of Care?...", pp. 119-120.

[158] Muy crítico, Frosio, Giancarlo, "The Death of "No Monitoring Obligations" A Story of Untameable Monsters', JIPITEC, 2017, 8, [pp. 199–215], pp. 203-211. Frosio, "Reforming Intermediary Liability…", pp. 38-40. También Frosio-Mendis, "Monitoring and Filtering….", en Frosio (ed), *The Oxford Handbook...*, pp. 4-6, 8-12.

[159] Tribunal Grand d'Instance de Paris (17ª Ch), de 6 de noviembre de 2013 (RG 11/07970), *Max Mosley* v *Google Inc*/*Google France*.

[160] LG Hamburgo (AZ: 324 O 264/11), de 24 de enero de 2014.

[161] [2015] EWHC 59 (QB), de 15 de enero de 2015, *Max Mosley* v *Google Inc/Google UK Limited* (§ 54), en un caso de protección de datos en el que ni siquiera era posible la monitorización.

que afectaban a la intimidad del demandante no volvieran a aparecer en el motor de búsqueda, lo cual incluía la obligación de aplicar y/o desarrollar *software* específico para borrar, detectar y bloquear esos contenidos. Así, según el tribunal alemán:

> "[Al demandado] le correspondía tomar las precauciones necesarias para evitar nuevas infracciones similares después de las correspondientes quejas del demandante o hacer esfuerzos, por ejemplo, utilizar programas informáticos para detectar y eliminar o bloquear este contenido o desarrollar dichos programas informáticos. Esto es razonable. Las imágenes contienen graves violaciones de la ley que pueden ser detectadas sin mucho esfuerzo. El demandante ha tomado medidas contra operadores de sitios web individuales o autores antes de presentar una demanda contra el demandado, pero esto no ha dado lugar a una solución adecuada en lo que respecta la búsqueda de imágenes. Habida cuenta de la gravedad de la infracción y de sus esfuerzos anteriores, no estaba obligado a tomar medidas contra todas las grandes empresas de medios de comunicación -posiblemente de todo el mundo- que distribuyen estas imágenes en sus propios sitios web. Hay que tener en cuenta que el motor de búsqueda de imágenes del demandado busca regularmente en toda Internet y, por lo tanto, encuentra e incluye repetidamente en su índice páginas que contienen las imágenes correspondientes, aunque no se trate de publicaciones de empresas de medios de comunicación de renombre. La invasión de la esfera privada protegida no es menos sustancial para el demandante en este caso, sin embargo, si la imagen se indica en los resultados de la búsqueda con la URL de una página de Internet menos conocida. También hay que tener en cuenta la posición del demandado y el tamaño y la reputación del motor de búsqueda que explota. El hecho de que estas imágenes puedan difundirse a través de otros motores de búsqueda, pero en particular a través de las redes sociales, incluso si el demandado las bloquea, no exime al demandado de su obligación."[162]

52. En defintiva, la ampliación de los deberes de diligencia del intermediario, a veces *ex ante* voluntariamente asumidas y otras *ex post* judicialmente impuestas, ilustra la paulatina erosión que desde hace tiempo viene sufriendo la prohibición de control general establecida en el art. 15 DCE. Los pasos que modernamente está dando el legislador europeo todavía van más lejos y llegan incluso a prescindir abiertamente del art. 15 DCE. Es un ejemplo la Propuesta para combatir el terrorismo, que justifica ese proceder ante el "riesgo particularmente grave impuesto por la difusión de contenidos terroristas en línea", aunque el Parlamento Europeo ha reaccionado con la derogación de esa regla y ha introducido otras cautelas.[163] Otro ejemplo, mucho más cercano, es el art. 17 DCMUD aunque el legislador no tiene empacho en afirmar que el filtrado generalizado en busca de violaciones del *copyright* no da lugar a ninguna obligación general de supervisión (art. 17.8 DCMUD). Todos sabemos, por el contrario, que eso es exactamente lo que sucederá.[164] Ni siquiera las excepciones (art. 17.7 DCMUD), que tratan de maquillar la regulación propuesta, podrían evitar ese control general de los contenidos. La República de Polonia ha solicitado la anulación del art. 17.4 letras b) y c) DCMUD, por violación del derecho a la libertad de expresión y de información garantizado por el art. 11 de la Carta de los Derechos Fundamentales de la Unión Europea.[165] La norma constituye además un claro apartamiento de jurisprudencia del TJUE, por lo menos la dictada hasta ahora en el ámbito de la propiedad intelectual.

---

[162] LG Hamburgo (AZ: 324 O 264/11), de 24 de enero de 2014 (§ 137).

[163] *Vid*. Parlamento Europeo, Enmienda 22 al Cdo 19 y enmiendas 61-64 a un nuevo art. 3 e introducción de un nuevo art. 3 bis. La Propuesta, tras la Primera lectura llevada a cabo por el Parlamento y tras la aceptación de enmiendas por el Consejo puede leerse en https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8663_2019_INIT&qid=1573035054776&from=ES Antes, *vid*. *Opinion of the European Union Agency for Fundamental Rights*, 39), disponible en: https://fra.europa.eu/en/publications-and-resources/opinions.

[164] Remarca la sorpresa que causa ese art. 17.8 DCMUD, Peguera Poch, "La exoneración…", p. 245. La generalidad de la doctrina denuncia la imposibilidad de escapar de la responsabilidad sin llevar a cabo ese control general. Entre muchos, Frosio-Mendis, "Monitoring and Filtering...", en Frosio (ed), *The Oxford Handbook…*, pp. 18-20, que también apunta a su adopción voluntaria, ex art. 17.10 de la Directiva. *Vid*. Spindler, "Responsabilidad civil y diligencia…", *LaNotaria*, 2019 (en prensa); el mismo autor, "¿Compartir contenidos en línea o no? Un análisis del artículo 17 de la Directiva sobre propiedad intelectual en el mercado único digital", *Cuadernos de Derecho Transnacional* (CDT), 2020, 1, núm. 63.

[165] *Vid*. el recurso interpuesto el 24 de mayo de 2019 - República de Polonia contra Parlamento Europeo y Consejo de la Unión Europea (Asunto C-401/19) (DO L 130, de 12.8.2019).

53. La DCMUD también plantea dudas sobre el grado de sofisticación que es preciso para detectar los contenidos exceptuados y, por consiguiente, también la accesibilidad a los mismos por parte de solo pocas empresas. Podrá decirse que la prohibición general de control se respeta siempre que exista la tecnología adecuada y que, por eso mismo, la norma prevé excepciones.[166] Esa es, por lo menos, la premisa de la que parte el documento que recoge las líneas básicas de la futura DSA que, a la vez que pretende imponer la puesta en práctica obligatoria de medidas *ex ante*, como contenido del deber de diligencia de los intermediarios, pretende dejar intacto el art. 15 DCE.

Ese borrador que contiene las líneas de una futura DSA valida el enfoque de la DCMUD, que legitima el uso de la inteligencia artificial para detectar contenidos ilícitos. Efectivamente, como ya se ha visto, las técnicas automáticas de filtrado y bloqueo adquieren carta de naturaleza en el art. 17.4 letras b) y c) DCMUD, salvo para las plataformas nuevas con un volumen de negocios y una audiencia reducidos (Cdo 67, art. 17.6 DCMUD). La técnica ya aparece contemplada en el Cdo 40 DCE y solo recientemente ha sido considerada la mejor práctica por la Comisión Europea.[167] El citado documento también admite que deben introducirse disposiciones específicas que regulen los algoritmos para las tecnologías automatizadas a fin de garantizar la transparencia y la responsabilidad.

VI. Los procedimientos de moderación de contenidos

54. Una de las carencias más destacadas de la DCE es la no inclusión de regla alguna sobre el procedimiento de aviso (de la comisión de un ilícito) y retirada (de los contenidos que contravienen los derechos de terceros). Este es un procedimiento estrictamente privado en virtud del cual las personas que se consideran víctimas de la infracción lo notifican al intermediario que aloja el contenido ilícito o dañoso, y/o que enlaza con él, para que lo elimine. La Comisión Europea se reservaba regular esos procedimientos en el futuro (art. 21.2 DCE) y, por eso, de momento, el art. 14.3 DCE se limita a advertir que la exclusión de responsabilidad no afecta a la posibilidad de que los Estados Miembros desarrollen esos procedimientos. El Cdo 40 y el art. 16 DCE añaden que tal desarrollo puede llevarse a cabo sobre la base de acuerdos voluntarios entre todas las partes interesadas.

La ventaja de tales procedimientos es que no es preciso esperar a que una orden judicial autorice la retirada o el bloqueo; eso es beneficioso porque, en la mayoría de casos, los costes de litigación serán elevados y, además, la obtención de una sentencia puede tomar más tiempo del deseable para reparar a la víctimas.

Sin embargo, qué duda cabe de que tales procedimientos, que dejan en manos de los privados cómo debe ser el comportamiento de los usuarios, solo pueden ser satisfactorios si ambas partes pueden acceder fácilmente a procedimientos judiciales o extrajudiciales de resolución de litigios.[168] Por otra parte, se diría que para determinados contenidos dañosos (*e.g. fake news*) el procedimiento de notificación (y consiguiente retirada) no es plenamente satisfactorio. Para esos supuestos, el documento filtrado que contiene ideas para una nueva DSA confia en los códigos de conducta –previa aprobación de un regulador- y en el empoderamiento del usuario en la elección de las fuentes, lo cual sugiere la necesidad de mejorar la educación de los ciudadanos.[169]

---

[166] Cfr. art. 17.5 DCMUD. Para el argumento, Sartor, "Providers Liability…", p. 26, p. 29. Lo mismo parece desprenderse ahora de la STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek* (ECLI:EU:C:2019:821) cuando afirma que no es preciso un ulterior control humano de los resultados que arroje el sistema automáticamente (§§ 44-47).

[167] En general, para los pros y contras del filtrado, *vid*. SEC(2011) 1641/2, 50–51. *Vid*. ahora COM(2017) 555 final, pp. 13-15.

[168] *Vid.* ahora el Cdo 70 y el art. 17.9 II DCMUD. Antes, Cdo 22 y § 14 Recomendación 2018/334.

[169] A nivel nacional, contra la desinformación, *vid*. en Francia Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information; en el Reino Unido, UK Online Harms White Paper de 9.4.2019 (modificado por última vez, 26.6.2019); en Alemania, *vid*. la *Staatsvertraglicher Neuregelungen zu Rundfunkbegriff / Zulassungspflicht, Plattformregulierung und Intermediäre* ("Medienstaatsvertrag"), que probablemente entrará en vigor en septiembre de 2020 (https://www.tagesschau.de/inland/medienstaatsvertrag-rundfunkstaatsvertrag-101~amp.html) (última consulta : 7.12.2019).

55. Los Estados miembros han puesto en marcha procedimientos de notificación y retirada a través de líneas telefónicas directas nacionales que permiten a los usuarios de internet denunciar, *e.g.* los contenidos de pornografía infantil que encuentren en línea.[170] A veces esos procedimientos son fruto de la autoregulación, que más que el acuerdo con las partes interesadas (*stakeholders*) reflejan la política individual de las empresas (*vgr*. la política de protección de marcas que, por lo general, no se refiere solo a los contenidos ilegales).[171] En este último caso, el riesgo es no ofrecer la necesaria transparencia. La posibilidad de retirar contenidos que solo son presuntamente ilegales, ante la dificultad de conocer la verdadera naturaleza de determinado tipo de infracciones, aumenta cuanto más opacos sean los criterios que hacen servir los prestadores para determinar las razones por las que los contenidos deben ser eliminados en las cláusulas de exención de responsabilidad. Ello ha alimentado la censura del intermediario frente al proveedor de contenidos lícitos indebidamente retirados o bloqueados sin, aparentemente, el riesgo de tener que soportar una demanda de responsabilidad contractual.[172] Es una situación intolerable que exige analizar cuidadosamente la licitud o ilicitud de los acuerdos que permiten filtrar o bloquear contenidos porque, más allá de las legítimas decisiones sobre la política de la empresa, podría suceder que algunas condiciones generales de los contratos de acceso a las plataformas fueran abusivas: e.g. si una cláusula dijera, sin ulterior precisión, que la plataforma se reserva el derecho de eliminar los contenidos que considere "objetables" sin la necesaria trasparencia sobre los criterios que hace servir; o, por poner otro ejemplo, si dijera que se reserva el derecho a suspender las cuentas sin aviso. Los derechos fundamentales deben prevalecer sobre las condiciones generales y cláusulas como las acabadas de mencionar limitan la libertad de expresión. Tras la entrada en vigor del Reglamento sobre una intermet abierta se prohibe, salvo contadas excepciones, el bloqueo no exigido por ley y, por supuesto, el bloqueo voluntario de contenido lícito.[173]

56. En el Primer Informe sobre la aplicación de la DCE,[174] Finlandia aparecía como el único país que había adoptado una regulación sobre *notice-and-take down* en materia de *copyright*, pero la lista de los Estados que han regulado ese mismo procedimiento u otros que permiten el bloqueo (*notice-and-stay down*), ya en un ámbito sectorial, ya con alcance horizontal, se ha ampliado muy considerablemente en nuestros días.[175] En España, en el ámbito de la propiedad intelectual, el art. 195 TR-LPI regula un procedimiento administrativo para hacer cesar el ilícito. A pesar de esa teórica evolución, o precisamente por ello, no existe un criterio unánime en relación con el contenido que deberían tener las notificaciones, el marco temporal dentro del cual deberían actuar los intermediarios, o la necesidad de prever un contra-aviso o contra-notificación que permita defender la legalidad de la información alojada, así como la posibilidad de control judicial posterior.[176]

57. La Recomendación 2018/334 trata de establecer los criterios por los que deberían regirse los procedimientos de moderación de contenidos de las empresas intermediarias aunque, en realidad, el documento se dirige fundamentalmente a las plataformas que hoy se reparten el mercado. En general, la Recomendación es muy laxa en sus términos, porque parte de la base de la existencia de códigos de con-

[170] *Vid*. COM(2016) 872 final, pp. 7-9.

[171] SEC(2011) 1640/2, pp. 40-41; Giovanella, "*Online* Service Providers' Liability….", en Taddeo-Floridi (eds), *The Responsibilities…*, pp. 232-233 y pp. 234 ss, donde propone un modelo al estilo del que existe en Canadá.

[172] G. N. Yannopoulos, 'The Immunity of Internet Intermediarie Reconsidered?', en Taddeo-Floridi (eds), *The Responsibilities...* [pp. 43-59], p. 50. Con matices, Rubí Puig, "Derecho al honor *online*...", p. 15, nota 21. Recientemente, J. Venturini *et al.*, "Terms of Service and Human Rights: an Analysis of *Online* Platform Contracts, 2016 (disponible en: http://bibliotecadigital.fgv.br/dspace/handle/10438/18231).

[173] Cdos 11, 13 y art. 3.3 letra a) Reglamento 2015/2120. H. W. Micklitz – P. Pałka, "Algorithms in the Service of the Civil Society", EuCML, 2019, 1, [pp. 1-3], p. 2, explican su implicación en el desarrollo de un programa algorítmico que permitirá detectar cláusulas potenciamente abusivas y que verificarán el cumplimiento del Reglamento 2016/679, de protección de datos.

[174] Primer Informe sobre la aplicación de la Directiva 2000/31 (COM(2003) 702 final, Bruselas, 21.11.2003), pp. 14-16.

[175] *Vid*. SEC(2011) 1641/2, pp. 42-43 y Annex II, pp. 137–140; SWD (2018) 408 final, Annex 7, pp. 122-125.

[176] *Vid.* SEC(2011) 1640/2, pp. 43-46; Verbiest-Spindler *et al.*, *Study on the Liability*..., pp. 41-46; Van Eecke -Truyens (DLA Pipper UK LLP), 'Chapter 6: Liability for online intermediaries', en EU Study on the Legal Analysis…, pp. 19-20; SWD (2018) 408 final, Anexo 7, pp. 125-129 y Anexo 8, en relación con la autoregulación. Sobre la bondad de cada uno de esos sistemas, con detalle, Kuczerawy, *Intermediary...*, pp. 203 ss., pp. 331 ss.

ducta –en los que se inspira- donde se desarrollan los detalles. De entrada, y sin perjuicio de las especificidades que puedan existir en relación con determinados contenidos terroristas, el documento no impone ni la forma ni el contenido de las notificaciones, ni obliga al notificante a identificarse.[177] Prevé, además, la posibilidad de que el proveedor de contenidos se oponga a la decisión de bloquear o retirar los materiales (*counter-notice*) –algo que la DCE no precisa- lo cual es, sin duda, un acierto. La contra notificación se hace con vista a la anulación de la decisión de retirada, pero la Recomendación advierte que eso es "en su caso", esto es, no prejuzga que, tras recibirla, el prestador esté necesariamente obligado a reponer los contenidos antes suprimidos. Por otra parte, se deduce que la retirada es automática, tras la notificación, lo cual indica que ni siquiera se da la ocasión al prestador de valorar la posible ilegalidad del contenido.

En realidad, la facultad de oponerse solo existe si el afectado solicita ser informado de la retirada o bloqueo de los contenidos y no podrá hacer uso de la misma cuando exista una evidencia manifiesta de la ilicitud y/o de que los hechos son constitutivos de delitos graves que suponen un peligro para la vida o la seguridad de las personas, o cuando así lo solicite la autoridad competente por razones de orden y seguridad públicas. En el primer caso, la carga para las empresas es evidente, si resulta que estas tienen que juzgar sobre la base de unos hechos que, en definitiva, no siempre quedará claro que sean ilegales o cuya naturaleza delictiva no tienen por qué conocer. La Recomendación parece conjurar el riesgo de error exigiendo que las notificaciones sean suficientemente precisas y bien fundadas y con el fomento de la colaboración entre prestadores de servicios y notificantes fiables, a pesar de que no se sabe bien quienes lo son o porqué lo son, sino solo que lo serán según las condiciones que establezca la empresa. En esta última hipótesis –la de los notificantes fiables- se establece la necesidad de poner en marcha procedimientos acelerados que tramiten más rápidamente sus notificaciones. Una medida adicional, para evitar la indebida retirada de contenidos lícitos, es que los intermediarios deben contar con la intervención de expertos que garanticen una actuación proporcionada por parte de los intermediarios.[178] Además, se recomienda adoptar medidas para prevenir la existencia de notificaciones o contra notificaciones realizadas con abuso o mala fe, lo cual sugiere la necesidad de imponer algún tipo de sanción pecuniaria (o la responsabilidad por la pérdida de ingresos mientras dura la retirada), pero no se explica quién debería pechar con esa carga.[179] Se recalca que todo ello debe realizarse con el debido respeto a los derechos fundamentales y que en modo alguno queda vedado el acceso a ulteriores procedimientos de resolución extrajudicial y, por supuesto, tampoco judicial.

58. El procedimiento de notificación y retirada obliga a los titulares de derechos defraudados a estar pendientes de que el ilícito no vuelva a repetirse. Al amparo de la DCE, la *Cour de Cassation* impidió a *Google France* perder el puerto seguro por el hecho de que reaparecieran los vídeos/películas cuestionadas tras haberlas suprimido efectivamente, por entender que lo contrario hubiera exigido una vigilancia continua.[180] Sin embargo, recientemente, en un caso de difamación, la STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek* parece legitimar que el bloqueo pueda tener alcance mundial. Es una decisión que contrasta con la STEDH de 9 de marzo de 2017, *Pihl* v *Sweden*, que no

[177] En la misma línea, el art. 17.9 III DCMUD establece que: "no conducirá a identificación alguna de usuarios concretos, ni al tratamiento de sus datos personales".

[178] *Vid* ahora art. 17.9 II DCMUD.

[179] Cap. II, § 21 Recomendación 2018/334.

[180] Cass. Civ. I, de 12 de julio de 2012, *Aufeminin.com / Google France et autres*; Cass. Civ. I, de 12 de julio de 2012, *Google France et autre / société Bac films et autres*: «En se prononçant ainsi, quand la prévention imposée aux sociétés Google pour empêcher toute nouvelle mise en ligne des vidéos contrefaisantes, sans même qu'elles en aient été avisées par une autre notification régulière pourtant requise pour qu'elles aient effectivement connaissance de son caractère illicite et de sa localisation et soient alors tenues d'agir promptement pour la retirer ou en rendre l'accès impossible, aboutit à les soumettre, au-delà de la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause, à une obligation générale de surveillance des images qu'elles stockent et de recherche des mises en ligne illicites et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps». Por el contrario, *vid.* BGH de 12 de julio de 2012, *Alone in the Dark* (resumen en Kur, Annette, "Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU", Colum.J.L.&Arts, 2014, 37, [pp. 525-540], pp. 537-538). Ampliamente, sobre la distinta aproximación al problema en Francia y Alemania, Kuczerawy, *Intermediary...*, pp. 234 ss, y allí la valoración crítica del régimen alemán que, en opinión de la autora, comporta un control general de los contenidos que contraviene el art. 15.1 DCE. Además, pp. 357 ss

considera responsable de la violación de la vida privada al intermediario *online* que, tras haber borrado del servidor un comentario ultrajante, a requerimiento del ofendido, sin embargo no había impedido que este pudiera localizarse en otros lugares.[181] Precisamente para contrarestar decisiones de ese tipo, la Comisión Europea ve ahora factible el desarrollo de procedimientos de *notice and staydown* (bloqueo) en su Recomendación. Con todo, cualquier bloqueo del contenido *online* debe haber sido previamente previsto en la ley, estar claramente justificado, ser proporcionado, y no ir más allá de lo necesario para conseguir esa finalidad.[182]

59. La DCMUD permite utilizar tecnología de reconocimiento de contenidos, tanto para filtrar como para bloquear. Sin embargo, si esta tecnología no está bastante desarrollada, o bien la empresa no puede permitirse el coste de su implementación, la revisión manual, en su caso previa notificación, será el único instrumento para evitar la disponibilidad de contenidos protegidos (o no) por derechos de autor (Cdo 66 II DCMUD). Para uno y otro caso se han previsto mecanismos de reclamaciones, a las que deberán atender personas expertas (este último calificativo no aparece expresamente, pero cabe presumirlo), antes de dar paso a la resolución (judicial o extrajudicial), con el fin de atenuar resultados indeseados cuando se haga un uso legítimo (Cdo 70 II, art. 17.7 DCMUD). Estos últimos serán frecuentes si se observa que a las plataformas se las obliga a actuar "de modo expeditivo" para retirar y bloquear el acceso (art. 17.4 letra c) DCMUD). Eso facilita la existencia de falsos positivos y/o una inadecuada reacción frente a notificaciones falsas, ante las cuales solo quedará recurrir al juez u otro mecanismo extrajudicial de resolución. Eso va a promover la inacción de muchos usuarios que no conocerán las complejidades legales o no considerarán que vale la pena invertir tiempo y dinero en ello.

VII. Reflexiones finales

60. Existe una creciente necesidad de regular el comportamiento de los prestadores intermediarios y la información que se aloja en páginas web, redes sociales, blogs o foros, en relación con la incitación al odio, la exaltación del terrorismo, la difamación, o la propagación de pornografía infantil, por citar solo algunos ejemplos. El legislador debería ser capaz de proteger a las víctimas, sin incurrir en el riesgo de dañar a los creadores, perjudicar la libertad de expresión, o hundir el negocio de internet. De momento, la tendencia es ampliar las obligaciones de control preventivo, siguiendo la estela de decisiones (contradictorias) de los tribunales nacionales que han contribuido a la confusión sobre el nivel de diligencia que debían tener para proteger su puerto seguro. Es, también, la tendencia que observa el legislador en algunos Estados Miembros a la hora de combatir la piratería[183] o los contenidos ofensivos.[184]

---

[181] STEDH de 9 de marzo de 2017, *Pihl* v *Sweden* (§ 33). El Tribunal tiene en cuenta, además, el carácter no lucrativo de la asociación que gestionaba el bloc, así como su reducido tamaño (§ 31).

[182] Cdos 11, 13 y art. 3.3 letra a) Reglamento 2015/2120; art. 25.1 Directiva 2011/93/UE, contra los abusos y explotación sexual de menores; Cdo 22-23 y art. 21.2 y 3 de la Directiva 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo (DO L 88, de 31.03.2017); art. 17.4 letra c) y 5 DCMUD. En relación con la interpretación que merece el Reglamento citado en primer lugar, *vid*. Council of Europe, Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2017, pp. 24-26 (disponible en https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html) (última visita: 7.12.2019).

[183] En Francia, *vid*. N. Lucchi, "Regulation and Control of Communications: the French Online Copyright Infringement Law (hadopi)", 2011, 7 Max Planck Institute for Intellectual Property and Competition Law Research Paper (MPI IPCL RP), pp. 1-28, en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1816287 (última consulta: 12.11.2019). La suspensión del acceso al prestador de internet fue abrogada en 2013. Alemania también ha modificado la Ley de Telecomunicaciones (*Telemediengesetz* - TMG) con el fin de excluir del privilegio a las plataformas cuya actividad incluye la violación de los derechos de autor (por ejemplo, "The Pirate Bay"). *Vid*. Spindler, "Haftung ohne Ende?...", pp. 48-52.

[184] En Alemania, *vid*. *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Netzwerkdurchsetzungsgesetz – NetzDG), de 1.9.2017. Para la crítica, G. Spindler, "Internet Intermediary Liability Reloaded. The New German Act on Responsibility of Social Networks and its (In-) Compatibility with European Law", 2017, 8, JIPITEC, pp. 166-179. Además, *vid.* UK Online Harms White Paper of 9.4.2019 (modificado por última vez, 26.6.2019). Recientemente, en Francia, *vid*. la *Proposition de loi adoptee par l'Assemblée Nationale visant à lutter contre les contenus haineux sur internet* de 9.7.2019.

Los riesgos de internet son evidentes y conocidos, pero tampoco duda nadie de las enormes ventajas que trae aparejadas. Sorprende, pues, que 20 años después de la promulgación de la DCE, internet parece ser percibida más como una amenaza que como una oportunidad. Seguramente por eso nuevas directrices políticas para la próxima Comisión Europea 2019-2024 anuncian la derogación de la DCE y la promulgación de otra que la sustituya. Según ya se ha explicado, los planes consisten en ampliar las actividades de acceso, caché y alojamiento, para incluir explícitamente otros servicios; reescribir la regulación sobre exenciones de responsabilidad; y exigir un papel activo de los distintos servicios digitales y, en particular, para las plataformas en línea. Ese enfoque es mucho más gravoso para las empresas y presenta mucho mayor riesgo de limitar la libertad de expresión y de información.

En particular, cobra particular importancia en la detección de contenido ilegal el filtrado preventivo y el subsiguiente bloqueo, a los que se concede el privilegio de ser el modo de detección habitual y, según parece, no solo en el combate contra la detección de ilícitos en el *copyright* o contra el honor. La utilización de herramientas automatizadas trae consigo el riesgo de aumento de la censura y cerrado de cuentas porque la tecnología no siempre puede detectar correctamente las ilegalidades (¿cómo percibir los matices de la comunicación humana?); aun peor, puede tener efectos discriminatorios entre distintos grupos sociales. Si se admite, porque sin duda se ha revelado eficaz, es preciso introducir precauciones y, por de pronto, prever mecanismos de revisión humana. Es sorprendente que eso sea lo que descarte, precisamente, la STJUE C-18/18, de 3 de octubre de 2019, *Glawischnig-Piesczek*.

El documento que se ha filtrado con las notas para una futura DSA se refiere específicamente a la necesidad de establecer medidas que permitan conocer la transparencia del algoritmo -es decir, que permitan saber porqué el contenido se ha borrado-, pero es verosímil pensar que ello requerirá la adopción de legislación específica adicional y *ad hoc*, según evolucionen los debates que sobre inteligencia artificial tienen lugar en la actualidad.[185] Ese será el tema a estudiar en los próximos años y ya veremos como lidia con él la próxima DSA.

[185] COM(2018) 237 final. Micklitz – Pałka, "Algorithms in the Service...", pp. 1-3; M. Kolain, "Artificial Intelligence, Robotics and the Law: Current Research Projects and Unsolved Legal Questions – Report of the first RAILS-Conference on 23 March 2018 in Hannover", ERPL, 2019, 3, pp. 647–656. *Vid*. además el "Algorithmic Awareness-Building Project", en https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building (última consulta: 3.12.2019).