CAPÍTULO V
Datos personales, relaciones jurídico privadas y jurisprudencia europea

Dolores Palacios González
Profesora titular de derecho civil de la Universidad de Oviedo[1]

1. INTRODUCCIÓN

Según la más reciente definición de datos personales, recogida en el artículo 14 del Reglamento UE 2016/687 del Parlamento Europeo y del Consejo de 27 de abril de 2017 (en adelante, el Reglamento), constituyen datos personales "toda información sobre una persona física identificada o identificable", considerándose persona física identificable "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". La definición es muy similar, aunque no idéntica, a la que proporcionaba la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, reconducida en el artículo 3 de nuestra primera Ley de protección de datos, la Ley Orgánica 15/1999, a "cualquier información concerniente a personas físicas identificadas o identificables".

Aunque la protección específica de este tipo de datos es relativamente reciente, ya con anterioridad sus titulares pudieron defenderse frente a algunas utilizaciones que entendían lesivas, debido a la conexión de esos datos referidos a una persona identificable con otros bienes jurídicos que sí estaban tutelados como el honor, la intimidad o la imagen.

[1] Miembro del Grupo Consolidado de Investigación del Principado de Asturias "EURODER-UNIOVI-IDI/2018/000187". Este trabajo está vinculado al Proyecto DER2017-86017-R, "Obstáculos a la movilidad de personas en los nuevos escenarios de la UE", concedido por el Ministerio de Economía, Industria y Competitividad, en los términos del artículo 37 de la Ley 14/2011, de 1 de junio (*BOE* nº 131, 2-VI-2011).

La Ley 1/1982 de 5 de mayo, desarrollo del artículo 18 de la Constitución, no define el honor, la intimidad o la imagen personal pero de ella puede deducirse, como así lo han hecho la jurisprudencia y la doctrina posteriores, que de acuerdo con el precepto constitucional nos encontramos con tres derechos diferentes. En primer lugar, el derecho a no ser escarnecido ni humillado, ni desmerecido en la consideración que una persona se tiene a sí misma y la que nos tienen los demás; en segundo lugar, y por lo que se refiere a la intimidad, el derecho a controlar la parcela más íntima de nuestra vida, sin perjuicio de las limitaciones establecidas en la ley; por último, el derecho a la imagen supone la autodeterminación de la proyección pública de nuestros rasgos físicos, la voz y el nombre. Es evidente que la utilización de los datos de una persona por un tercero puede también lesionar alguno o algunos de estos derechos.

Cuando el incumplimiento de la normativa de protección de datos dé lugar a una lesión en el honor, la intimidad o/y la imagen del titular de los mismos caben distintas posibilidades. Es posible reclamar exclusivamente sobre la base de la regulación que tutela los datos o el otro u otros derechos afectados pero también es posible superponer ambas regulaciones, lo que ha dado lugar a que en la práctica la situación se presente, a veces, confusa. Así vemos que la sentencia de la Sala de lo Contencioso Administrativo del Tribunal Supremo de 11 de enero de 2019 (núm. 12/2019) fija como jurisprudencia que "la persona afectada por una supuesta lesión del derecho al honor, a la intimidad personal y familiar y a la propia imagen está legitimada para fundamentar válidamente una acción de reclamación ante la entidad proveedora de los servicios de motor de búsqueda en Internet o ante la Agencia Española de Protección de Datos, cuando los responsables del motor de búsqueda ofrezcan datos sustancialmente erróneos o inexactos que supongan una desvalorización de la imagen reputacional que se revele injustificada..."; la normativa aplicada es la normativa de protección de datos –concretamente el artículo 6.4 de la Ley 15/1999, que recogía el derecho de oposición al tratamiento– en relación con el artículo 20 de la Constitución.

En la actualidad, nuestra norma interna para la protección de los datos personales es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de los Datos Personales y garantía de los derechos digitales, que se remite al Reglamento en gran parte de su articulado.

2. EL RÉGIMEN INTERDISCIPLINAR DE LA PROTECCIÓN DE LOS DATOS PERSONALES DE LAS PERSONAS FÍSICAS

La artificiosidad que supone compartimentar actualmente cualquier ordenamiento jurídico, incluso en relación con la más antigua y aparentemente clara distinción entre Derecho público y Derecho privado, es algo muy evidente desde hace tiempo. Si nos centramos en el Derecho privado general, el Derecho civil, observamos que cada vez resulta más extraño encontrar un ámbito de relaciones en que las entidades públicas no intervengan en mayor o menor medida[2]. Esta evidencia no debe, sin embargo, llevarnos a inútiles disquisiciones acerca de si el Derecho privado se está administrativizando o no, o de si el Derecho privado gana o pierde terreno como si de una competición se tratara, sino a plantearnos la necesidad de armonizar, en la medida de lo posible, los principios que tradicionalmente vienen inspirando ambas categorías de normas.

En el mismo orden de cosas, si observamos el sistema normativo a aplicar desde la óptica del haz de relaciones a regular, nos encontramos con que muchas veces no solo no es posible subsumirlas en una de las ramas tradicionales del Derecho sino tampoco decidir siquiera si nos encontramos ante una relación de Derecho público o de Derecho privado. La razón al fin es bien sencilla, la complejidad de las relaciones actuales debe llevar, muchas veces, a una regulación interdisciplinar.

En el ordenamiento jurídico español la perspectiva constitucional de la protección de datos personales está fuera de toda duda. El Tribunal Constitucional ya manifestó en su sentencia de 30 de noviembre de 2000 (STC 292/2000) que sobre la base del artículo 18.4 de la Carta Magna, el derecho a la autodeterminación de los datos en relación con una persona física constituye un derecho fundamental derivado de la dignidad humana que va más allá de la intimidad[3]. Así, el artículo 1 de la Ley Orgánica 3/2018 de 5 de diciembre, alude expresamente al "derecho fundamental" a la protección de las personas físicas en lo que respecta a la protección de datos[4].

---

[2] Pueden ser paradigmáticas en este sentido las relaciones de consumo, la defensa de la propiedad intelectual o, como vamos a comentar seguidamente, la protección de datos personales.

[3] Se refiere el Tribunal a "un derecho o libertad fundamental... frente a las potenciales agresiones a la dignidad y a la libertad de las personas provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática".

[4] A su vez el Considerando 1 del Reglamento recoge que "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

Descendiendo por el ordenamiento y dejando de lado la tutela penal prevista para las conductas que el legislador ha estimado de especial gravedad, es evidente que la más general protección de los datos le compete a la Administración. El legislador comunitario ha decidido hacer descansar la tutela de los derechos que incluye en la misma en una autoridad pública independiente (autoridad de control) que en España es la Agencia Española de Protección de Datos (AEPD).

Las resoluciones dictadas por la AEPD frente a las reclamaciones que las personas físicas presenten en defensa de esos derechos[5], cuando los responsables o encargados del tratamiento no les dan satisfacción –los primeros son quienes determinan cualquier operación que afecte a los datos y el segundo quienes se ocupan del tratamiento por cuenta del responsable– ponen fin a la vía administrativa de acuerdo con el artículo 114.1 c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, pudiendo los interesados interponer potestativamente recurso de reposición ante la Dirección de la Agencia Española de Protección de Datos en un mes desde la notificación (artículos 112 y 123 de la Ley 39/2015) o directamente recurso contencioso administrativo ante la Sala del mismo orden de la Audiencia Nacional (artículo 25 y apartado 5 de la disposición adicional cuarta de la ley 29/1998 de 13 de julio).

Por otra parte el artículo 19 de la derogada Ley 15/1999, a su vez transposición de las previsiones del artículo 23 de la Directiva 95/46/CE, establecía que si como consecuencia del incumplimiento de lo dispuesto en la misma en relación con el responsable o el encargado del tratamiento de los datos una persona sufre un "daño o lesión en sus bienes o derechos" tiene derecho a ser indemnizada. En caso de ficheros de titularidad pública se establecía expresamente que la responsabilidad habría de exigirse de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas y en el de los ficheros de titularidad privada, ante los órganos de la jurisdicción ordinaria.

La LO 3/2018 vigente no ha recogido esta regulación pero por supuesto esto no significa que haya desaparecido el derecho a la indemnización cuando se produzca un daño pues, en cualquier caso, vendría amparado por la normativa general que regula la responsabilidad patrimonial de la Administración en caso de responsabilidad pública, y en el artículo 1902 del Código civil para el caso de que el daño fuese causado como consecuencia de la actuación de una persona privada, sin perjuicio de la posibilidad, más específica pero muy habitual, de esgrimir otras previsiones como las recogidas en la Ley Orgánica 1/1982 de

[5] Tras la entrada en vigor del Reglamento UE 2016/687 los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición) se han reconducido, sin demasiadas alteraciones, a los derechos de información y acceso, rectificación, supresión (olvido), limitación del tratamiento, portabilidad y oposición.

protección del honor, intimidad personal y familiar y la propia imagen cuando se considere que también ha sido lesionado alguno de estos derechos[6].

Pero es que, además, la posibilidad en general sí viene establecida directamente en el Reglamento, que en su artículo 82 dice que "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos". La responsabilidad corresponderá a cualquier responsable que participe en la operación de tratamiento en caso de que dicha operación no cumpla lo dispuesto por el Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

Cabe exención de responsabilidad si el responsable o el encargado demuestran que no son, en modo alguno, responsables del hecho que haya causado los daños y perjuicios.

En beneficio del afectado se establece un régimen de responsabilidad solidaria para el caso de que más de un responsable o encargado, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean responsables de cualquier daño o perjuicio causado por dicho tratamiento; cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

Cuando un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su cuota de responsabilidad por los daños y perjuicios causados.

En relación con el ejercicio de las acciones judiciales para reclamar la indemnización, el último párrafo del precepto remite a los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2[7].

---

[6] Véase cómo en la Sentencia de la Sala Primera del Tribunal Supremo de 12 de noviembre de 2015 (609/2015) se concede, sobre la base de los mismos hechos, una indemnización en parte fundada en la Ley Orgánica 1/1988 y en parte en la Ley 15/1999.

[7] Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

De todo ello podemos deducir que, cuando entre en juego el Derecho español las reglas específicas de responsabilidad aquí recogidas, habrán de ser tenidas en cuenta por la jurisdicción contenciosa o por la jurisdicción civil competentes respectivamente en caso de que el responsable o encargado del tratamiento lo sea de un fichero de titularidad pública o privada.

La competencia de la jurisdicción civil no se limita a la reclamación, en su caso, de la indemnización mencionada, sino que también es factible acudir a la misma en protección del derecho fundamental al control de los datos personales, sobre la base de la legislación de protección de datos y solicitar medidas que impidan la persistencia de la intromisión[8].

Por último, procede hacer referencia aquí a la competencia de la jurisdicción social para la protección de los datos personales de los trabajadores en el ámbito laboral (art. 2 f) de la Ley 36/2011 reguladora de la jurisdicción social).

3. LA PROTECCIÓN DE DATOS FRENTE A PARTICULARES EN LA JURISPRUDENCIA DEL TJUE

Para la actividad empresarial el interés económico y estratégico del conocimiento de los datos personales de la ciudadanía es muy elevado y no solo para elaborar perfiles de potenciales clientes sino también con otros fines, más delicados incluso, como conocer determinados aspectos de la situación de cada persona e incluso decidir si se contrata con ella o no o el contenido de un eventual negocio (así, por ejemplo la situación económica de un cliente o los datos de salud para las Compañías de seguros, serían sin duda conocimientos de gran valor para la empresa). También es evidente, y la realidad lo avala, que las personas físicas tenemos actualmente un riesgo muy elevado de perder el control de nuestros datos personales por más que el ordenamiento nos la reconozca. Es de esperar que principios incorporados en el Reglamento como el de responsabilidad proactiva o el enfoque de riesgo sirvan, efectivamente, para minimizarlo.

Para concluir cómo está la situación actualmente, en el ámbito de las relaciones jurídico-privadas, procede ahora analizar los asuntos más relevantes que ha tenido que enfrentar en este ámbito el TJUE y su repercusión en la jurisprudencia de nuestro país.

[8] Por ejemplo, en la Sentencia de la Sala Primera de 12 de noviembre de 2015 (609/2015) se condena a la demandada a cancelar los datos del demandante.

3.1 Ficheros de datos, tratamiento de datos y responsabilidad del tratamiento

La sentencia del TJUE de 10 de julio de 2018 (asunto C-25/17) ha tenido que enfrentar los conceptos de "fichero de datos" y "responsabilidad del tratamiento" en relación con la actividad de recogida de datos puerta a puerta que los miembros de la comunidad religiosa de los Testigos de Jehová venía haciendo en Finlandia. Frente a la decisión de la autoridad central de ese país de someter dicha actuación a la normativa de protección de datos, la comunidad religiosa aduce que el hecho de que sus predicadores apunten en libretas cuestiones como el nombre y los apellidos de los entrevistados y también en ocasiones sus inclinaciones religiosas no supone la llevanza de un fichero ni un tratamiento de datos personales fuera de un "ámbito personal o doméstico" y, por tanto, la actividad ha de quedar excluida de la normativa protectora.

En la sentencia, por el contrario, se considera que la actuación de los predicadores no puede considerarse de ámbito doméstico ya que los datos recabados pertenecían a personas ajenas a aquellos y además alguno de esos datos era transmitido a las congregaciones de la comunidad para registrar a quienes no quisieran recibir más visitas. Además, que esa actividad constituye un tratamiento de datos desde el momento en que el hecho de que estos no se recojan por vía digital ni utilizando fichas o catálogos no excluye su consideración de fichero como conjunto estructurado de datos referidos a personas que permite su recuperación.

El TJUE concluye la responsabilidad de la Comunidad de los Testigos de Jehová respecto del tratamiento de esos datos recabados con independencia de la actuación de los predicadores, al entender que estos actúan para cumplir las finalidades de la misma, que además recibe alguno de esos datos. Se dan, por tanto, los requisitos que la normativa exige para considerar a una persona física o jurídica responsable del tratamiento: la persona que sola o con otras determina los fines y los medios del tratamiento; y ello con independencia, dice el Tribunal, de que existan o no instrucciones por escrito o de que se hayan o no impartido consignas.

Aunque en este asunto no se planteó la cuestión, podríamos preguntarnos si los predicadores habrían de ser considerados también responsables o, por el contrario, encargados del tratamiento. En nuestra opinión, la autonomía con la que funcionaban en relación con los datos permitiría calificarlos asimismo de responsables, lo que podría llevarnos a la cuestión de las consecuencias de la corresponsabilidad de un tratamiento, sin perjuicio de que también los encargados tengan sus obligaciones. La misma sentencia, en su apartado 65, señala que un tratamiento puede concernir a varios agentes "cada uno de los cuales estará por

tanto sujeto a las disposiciones aplicables en materia de protección de datos (véase, en este sentido, la sentencia de 5 de junio de 2018, Wirtschaftsakademie Scheleswig-Holstein, C-210/16, EU:C:2018:388, apartado 29) pero también (apartado 66) que "los agentes pueden estar implicados en distintas etapas del tratamiento y en distintos grados, de modo que el nivel de responsabilidad de cada uno de ellos debe evaluarse teniendo en cuenta todas las circunstancias pertinentes del caso concreto", también conforme a la sentencia dictada en el asunto C-210/26.

La última vez que el TJUE ha tenido que enfrentarse al régimen de los corresponsables del tratamiento de datos personales fue en el asunto C-47/16, Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV (sentencia de 29 de julio de 2019). El Tribunal, siguiendo las conclusiones del Abogado General, considera que si un administrador de una página web inserta el plug-in de un tercero, como en el caso el administrador de la web de moda Fashion ID insertó el botón "Me gusta" de Facebook, y este último da lugar a la recogida y tratamiento de datos –en el caso aunque el navegante no utilizase el "Me gusta" e incluso aunque no fuera usuario de Facebook –, también es responsable del tratamiento. Como consecuencia de ello, el administrador del sitio web habrá de cumplir con las obligaciones relacionadas con aquellos aspectos del tratamiento por parte de la red social, en cuya determinación haya participado. En el caso se trataría de las operaciones de recogida de datos por lo que ambos corresponsables habrán de proporcionar al usuario de la web la información necesaria acerca de la recogida y tratamiento, y de no ser necesario el consentimiento por existir un fin legítimo para el responsable de los datos, dicho interés habrá de ser probado tanto por el administrador del sitio de Internet como por el proveedor de la red[9].

Por su parte, en la sentencia de 14 de febrero de 2019 (C-345/17, asunto Buividis contra la Datu valsts inspekcija (Agencia Estatal de protección de datos de Letonia), se discute si la grabación por un particular de su propia declaración en una comisaría de policía y posterior subida a la web www.youtube.com supone un tratamiento de datos personales ajenos y, si es así, si estaría amparado por la

[9] La corresponsabilidad del tratamiento se regula ahora en el artículo 25.2 del Reglamento que pretende evitar conflictos estableciendo que cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de sus obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo habrá de reflejar debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Independientemente de los términos del mismo, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

libertad de información (fines periodísticos, a afectos del artículo 9 de la Directiva 95/46). Al respecto el tribunal concluye que la mera recogida de datos personales (imágenes y conversaciones de los policías) ya constituye tratamiento y que si además se ha difundido la información en una página web realizando las operaciones necesarias para que resulten accesibles en Internet los datos se están tratando de manera automatizada, citando en este sentido la sentencia de 6 de noviembre de 2003 (Lindqvist, C-101/01, EU:C:2003:596, apartado 26).

Por lo que se refiere a la excepción de fines exclusivamente periodísticos del artículo 9 de la Directiva el Tribunal considera, de acuerdo con su jurisprudencia, que ni el soporte en el que se transmiten los datos, clásico como el papel o las ondas de radio, o electrónico como Internet, es determinante para apreciar si se trata de una actividad «con fines exclusivamente periodísticos» (se remite a la sentencia de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 60), ni tampoco lo es el hecho de que la persona que comunica hechos (información) o que expresa opiniones o ideas, no sea profesionalmente un periodista. Ahora bien, habrán de ser los tribunales nacionales los que, a la vista de las circunstancias de cada caso, valoren si la información compartida en Internet puede calificarse de exclusivamente periodística a los efectos de ser tutelada por el derecho a la libertad de información y, para ello, el TJUE se apoya en los parámetros señalados por el Tribunal Europeo de Derechos Humanos en la ponderación de los derechos a la intimidad y a las libertades de expresión e información: "concretamente la contribución a un debate de interés general, la notoriedad de la persona afectada, el objeto del reportaje, el comportamiento anterior del interesado, el contenido, la forma y las repercusiones de la publicación, la forma y las circunstancias en las que se obtuvo información y su veracidad (véase, en este sentido, la sentencia del TEDH de 27 de junio de 2017, Satakunnan Markkinapörssi Oy y Satamedia Oy c. Finlandia, CE:ECHR:2017:0627JUD000093113, apartado 165). Asimismo, deberá tomarse en consideración la posibilidad de que el responsable del tratamiento adopte medidas que permitan mitigar el alcance de la injerencia en el derecho a la intimidad".

Esta doctrina del TJUE es plenamente aplicable en la actualidad con la vigencia del Reglamento en cuyo artículo 85.2 se prevé precisamente que los Estados miembros han de conciliar por ley el derecho a la protección de datos personales del Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos. La única diferencia apreciable, que veremos si tiene alguna consecuencia práctica, es que ya no se exige que los fines limitativos de la protección de datos sean "exclusivamente" periodísticos.

3.2 El olvido digital

El llamado "derecho al olvido", no adquirió carta de naturaleza en el derecho positivo hasta la entrada en vigor del Reglamento. No obstante, la denominación era utilizada ya antes por la doctrina y por los tribunales para hacer referencia, básicamente, a la posibilidad de que los titulares de los datos obtuvieran la supresión de los que fuesen lesivos para sus derechos, sobre todo la supresión de información obsoleta de hechos que podían perjudicarlos porque socialmente son de consideración negativa (v.gr. la comisión de un delito). Su fundamento se encontraba en el principio de calidad de los datos en virtud del cual incluso si no hay problema en relación con la posibilidad de su obtención, los datos personales solo podrán ser tratados en la medida necesaria para el fin para el que son recabados y no pueden mantenerse cuando este fin ya no lo justifique. Como se establecía ya entonces, los datos tratados han de ser adecuados, pertinentes y no excesivos en relación con el fin para el que fueron obtenidos. En consecuencia, la impresión era que realmente el derecho al olvido no era nada distinto de los derechos de oposición y cancelación recogidos en la normativa entonces vigente, en nuestro país la Directiva 95/46/CE y la Ley de Protección de datos de 1999[10].

Cuando el derecho al olvido se perfila con cierta identidad propia, o en palabras de la STS de 5 de abril de 2016, se concreta en el ámbito de Internet el derecho a la calidad de los datos, es a raíz de la conocida STJUE de 13 de mayo de 2014 (Gran Sala) (Asunto Google Spain contra AEPD, C-131/12). En esta sentencia y en relación con los buscadores de Internet, particularmente Google, el TJUE, partiendo de su consideración como responsable del tratamiento de los datos que maneja, entiende adecuado al Derecho de la Unión obligarlo a evitar el acceso y desindexar los que no cumplan la normativa, concretamente por ser obsoletos incluso aunque en su momento hayan sido editados lícitamente y también aunque no se considere necesaria o pertinente la eliminación por parte de la web de origen. Se tiene en cuenta, al respecto, la altísima capacidad que tiene Internet para posibilitar la difusión de una información hacia millones de personas en todos los lugares del planeta y que mien-

[10] Derecho a oponerse al tratamiento de los datos recabados sin consentimiento, salvo que una Ley establezca otra cosa, con base en motivos fundados y legítimos relativos a una concreta situación personal (art. 6) y derecho a que se cancelen –en principio que se bloqueen– los datos que infrinjan lo establecido en la norma (art. 16) y más concretamente los inexactos o incompletos y los que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados (art. 4.4 y 4.5); en relación con estos últimos se prevé que no puedan ser conservados en forma que permita la identificación del interesado (4.5 segundo párrafo).

tras una información divulgada por un medio tradicional va perdiendo actualidad, en Internet puede permanecer siempre presente si aparece en los primeros resultados de un buscador.

Esta manera de entender el "derecho al olvido", que en algún caso ha sido vista como un mero derecho a dificultar el acceso a los datos mediante la desindexación, porque realmente no supone la cancelación de los datos, que siguen en Internet[11], ha sido posteriormente aplicada por nuestro Tribunal Supremo. Así ocurrió en la sentencia de la Sala de lo civil de 15 de octubre de 2015 (545/2015) aunque esta vez la reclamación se hizo directamente al editor de la página web de origen de la información discutida (web del diario El País). El Tribunal obliga a la web demandada a evitar técnicamente la indexación de una información muy antigua, en su momento considerada noticia por hacer referencia a la comisión de un delito, y que desde que el acceso a la hemeroteca digital se hizo público y gratuito aparecía siempre que se realizaba una búsqueda utilizando el nombre y apellidos de los demandantes, que eran personas privadas. La actuación de la editora al no limitar ese acceso cuando se le pidió no se consideró amparada por la libertad de información[12], que sin embargo sí justificaba, a juicio del tribunal, el mantenimiento de la hemeroteca digital sin necesidad de suprimir los nombres y apellidos e incluso iniciales de los demandantes, como por el contrario había considerado la Audiencia Provincial, y también la posibilidad de búsqueda sobre la base de esos datos personales en el interior de la web del editor. No obstante, como consecuencia del recurso de amparo interpuesto ante el Tribunal Constitucional, hay que entender que la difusión en estos casos ha de limitarse aún más y así, se considera que tampoco debe de poder accederse a los mismos con el buscador de la web, que el Tribunal Constitucional considera un medio de difusión muy potente aunque no sea generalista[13].

En la misma línea, la STS de 5 de abril de 2016 estima el derecho de oposición ejercido en el año 2010 por una persona que había sido indultada en 1999 por un delito cometido en 1981. Google es condenado a indemnizar por el tiempo

[11] Cfr. Ruda González, A., "Sentencia 15 de octubre de 2015. Indemnización por daños al derecho al olvido. La responsabilidad por la no exclusión de la indexación de una hemeroteca digital por los buscadores generales (Caso El País). *Cuadernos Cívitas de jurisprudencia civil*, nº 101, 2016. Aunque ciertamente con la normativa anterior la cancelación no supone exactamente supresión sino bloqueo de los datos (art. 16 Ley 15/1999).

[12] Ya la STJUE en el caso Google, párrafo 39, se había referido a la posibilidad de que los editores de páginas web utilizaran protocolos de exclusión códigos para evitar la indexación de sus informaciones por los motores de búsqueda.

[13] STC Sala Primera 58/2018, de 4 de junio. Se pondera el daño, excesivo a juicio del Tribunal Constitucional, frente al limitado interés de la noticia dado que los protagonistas no eran personajes públicos y los hechos habían sido cometidos treinta años atrás.

en que la información fue accesible desde que, en otro procedimiento, fue requerido por la AEPD para que limitase el acceso. Según el tribunal, la vulneración del derecho por parte del buscador en este caso no estuvo en la indexación inicial del BOE[14] sino en mantenerlo diez años más tarde pese al requerimiento del afectado. Distinto sería, dice el Tribunal Supremo tanto en esta sentencia como en la anterior, que el titular de los datos fuese un personaje público, pero probablemente esta afirmación, tan genérica, haya de ser matizada en función de las circunstancias de los casos concretos que pudieran plantearse.

Por el contrario, la STJUE de 9 de marzo de 2017 (C-398/2015) no considera contrario al Derecho de la Unión el mantenimiento de datos personales en un Registro de sociedades pese a haber pasado tiempo desde el cese de la actividad de la sociedad en cuestión. El demandante reclamaba porque, a su juicio, el motivo por el que sus asuntos empresariales iban mal era porque en dicho registro figuraba que había sido administrador de otra empresa que años atrás había terminado liquidada tras un concurso de acreedores. Ponderando todos los intereses en juego el TJUE considera atendible la finalidad por la que pueden mantenerse esos datos, concretamente la seguridad jurídica en las relaciones entre las sociedades de capital y terceros, de acuerdo con lo previsto en la Directiva 68/151 tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades definidas en el segundo párrafo del artículo 58 del Tratado, para proteger los intereses de socios y terceros. A la cuestión prejudicial planteada lo que responde el Tribunal es que corresponde a los Estados miembros determinar esa posibilidad de "solicitar a la autoridad responsable de la llevanza del registro central, del registro mercantil o del registro de sociedades, respectivamente, que compruebe, sobre la base de una apreciación caso por caso, si está excepcionalmente justificado, por razones preponderantes y legítimas relacionadas con su situación particular, limitar, al expirar un plazo suficientemente largo tras la disolución de la empresa de que se trate, el acceso a los datos personales que les conciernen, inscritos en dicho registro, a los terceros que justifiquen un interés específico en la consulta de dichos datos".

Por lo que se refiere a la jurisdicción Contencioso-Administrativa, la sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 11 de enero de 2019 desestima el recurso de casación interpuesto por Google frente a la sentencia de la Sala de lo Contencioso de la Audiencia Nacional de 18 de julio de 2017, que avalaba la resolución del Director de la AEPD instando a Google para que adoptara las medidas necesarias para evitar que el nombre

[14] La reclamación ante la AEPD también había sido hecha frente al BOE pero fue desestimada porque el boletín eliminó de su buscador el nombre del demandante en cuanto este se lo solicitó.

del demandante –jefe forestal y, por tanto, funcionario público– se vinculara en sendos resultados de búsqueda del diario el País y un blog. El motivo es que se considera que las noticias a las que se vinculaba contienen inexactitudes en demérito del recurrente pues en ellas se le calificaba de "furtivo" cuando la sentencia del TSJ de Galicia en la que se le sancionaba dando lugar a la noticia, solo hacía referencia a que formaba parte de una "cuadrilla autorizada para ejercer la caza" si bien al hilo de su actuación se produjeron unos "incidentes" que dieron lugar a la mencionada sanción. La fundamentación jurídica que se tuvo en cuenta, y a la que ya hemos aludido en la introducción a este trabajo para poner de manifiesto la yuxtaposición que de hecho se produce entre la tutela de los datos y la tutela del honor, intimidad e imagen, fue el artículo 6.4 de la LOPD de 1999 –derecho a oponerse al tratamiento– en relación con el artículo 20 de la Constitución. Dice el Tribunal Supremo que el derecho al olvido digital comporta otorgar al interesado la facultad de solicitar de la entidad proveedora de servicios de motor de búsqueda en Internet, ante la AEPD, que los "cancele, suprima o prohíba".

Todos estos asuntos comentados han sido resueltos de acuerdo con la legislación anterior. Ahora bien, es sobre la base de esa doctrina que se ha concretado el derecho en el Reglamento refiriéndolo a la "supresión", para los casos en que los datos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo, cuando se retire el consentimiento o se ejerza el derecho de oposición de acuerdo con la norma, cuando los datos hayan sido tratados ilícitamente, cuando deban suprimirse para el cumplimiento de una obligación legal o cuando se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1, que se refiere al consentimiento dado por niños en relación con esa oferta directa.

Es un derecho a la "supresión" que de acuerdo con lo anteriormente visto habrá que entender de manera flexible, incluyendo la desindexación. Por ejemplo, en el caso de prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda mal podrían suprimir –en el sentido de eliminar– unos datos que solo controlan en esa medida. De hecho, el Reglamento prevé que el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales "de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos"; se está previendo, por tanto, que la supresión pueda consistir en eliminar enlaces, no directamente los datos.

Este derecho no procederá cuando los datos tratados sean necesarios para el ejercicio de los derechos a la libertad de expresión e información, para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, por razones de salud pública, con fines de archivo en interés público en los márgenes previstos en el propio Reglamento o para la formulación, el ejercicio o la defensa de reclamaciones.

Dado que en el mismo Reglamento se prevé también el derecho a obtener la limitación del tratamiento[15] habrá que ver cómo se deslindan, en la práctica, ambas posibilidades.

Pese al tratamiento unificado que hace el Reglamento del derecho al olvido, sin separar el ámbito digital del resto de las posibilidades de tratamiento, el legislador español ha optado por separar los derechos de los titulares de los datos en general, cuyo ejercicio puede culminar con la supresión, consecuencia o no del ejercicio del derecho de oposición, o la limitación del tratamiento, recogidos en el Titulo III, aunque para su regulación sustantiva se remita al Reglamento, del "derecho al olvido digital", que introduce en el Título X como garantía en el ámbito digital. Este último se refiere, específicamente, a la eliminación de los datos de las listas de resultados obtenidas con los motores de búsqueda "cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieran devenido como tales por el tiempo transcurrido y la naturaleza e interés público de la información" y también cuando "las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda de internet", incluyéndose un específico derecho al olvido en redes sociales, básicamente con la misma configuración aunque

[15] El interesado tiene derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: cuando impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; cuando ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o cuando se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. Tras la limitación los datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

con la previsión específica de que hay que suprimir los datos sin condiciones tras la mera petición cuando hayan sido facilitados por el propio titular y en cualquier caso si fueron facilitados durante su minoría de edad.

4. A MODO DE CONCLUSIONES

La interpretación de la normativa europea de protección de datos, a día de hoy hasta la entrada en vigor del Reglamento, se está conformando, como no podía ser de otra manera, con el hacer del TJUE, que en los últimos años ha tenido ocasión de referirse a los conceptos de fichero de datos y responsabilidad del tratamiento, así como al régimen de corresponsabilidad de este último.

Lo más relevante en este sentido es que para ser responsable de un tratamiento lo determinante es tener algún control sobre los fines y medios del mismo, que puede realizar otra persona, también responsable –en el caso de que haya varios responsables, cada uno será tratado en función de su actuación y de las circunstancias del caso concreto– y ello con independencia de que existieran o no consignas o instrucciones por escrito a ese segundo responsable.

La existencia del tratamiento presupone un fichero de datos que, cuando corresponden a personas ajenas a quienes los recaban y tratan –como los predicadores de una comunidad religiosa– no pueden considerarse excluidos de la normativa de protección de datos como actividad personal o doméstica. Y es irrelevante que el conjunto de datos que se recaba se almacene digitalmente o que se utilicen fichas o catálogos.

Por lo que se refiere al derecho al olvido, con anterioridad a la entrada en vigor del Reglamento, donde se recoge por primera vez, el TJUE ya tuvo ocasión de perfilarlo en el ámbito digital, como el derecho a evitar el acceso a los datos de una persona cuando no se cumpla con la normativa de protección de datos, en especial cuando no se respete el principio de calidad de los datos.