EL "DERECHO AL OLVIDO": DE LA STJCE DE 13 DE MAYO DE 2014 AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS [REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016]

FELISA MARÍA CORVO LÓPEZ*

Abstract: In 2014, the Court of Justice of the European Union ruled that individuals have the right -under certain conditions- to ask search engines to remove links with personal information about them. This right -known as "the right to be forgotten"- has also recently been regulated by the General Data Protection Regulation. The present work relates some of the problems raised by the application of this right, making special reference to Spanish case law.

Keywords: Data protection; privacy; Internet Search Engines; Right to erasure / "Right to be forgotten".

Palabras clave: protección de datos; derecho a la intimidad; motores de búsqueda; derecho de supresión/"derecho al olvido"

Resumen: 1. Introducción. 2. Construyendo el "derecho al olvido". 2.1. El derecho al olvido como manifestación del derecho a la autodeterminación informativa. 2.1.1. La protección de datos de carácter personal como derecho fundamental. 2.1.1.1. España. 2.1.1.2 Portugal. 2.1.2 El derecho a la protección de datos en la normativa comunitaria. 2.2. Planteamiento del problema tomando como referencia el caso Costeja. 2.3. Canalización del problema a través de los llamados derechos ARCO. 2.4. La STJUE de 13 de mayo de 2014. 2.5. Valoración doctrinal de la STJUE. 2.6. Primeras consecuencias de la STJUE. 2.6.1. Reacción de Google, la Comisión europea y las autoridades europeas de protección de datos. 2.6.2. Aplicación de la doctrina del TJUE por los órganos jurisdiccionales de los Estados miembros. El caso de España, en particular. 2.7. El Reglamento (UE) 2016/679. 2.7.1. El reconocimiento del derecho de supresión // "derecho al olvido". 2.7.2. Cuestiones a tener en cuenta en relación al responsable del tratamiento cuando se ejercita el derecho al olvido frente a los motores de búsqueda a la luz del Reglamento. 3. Las dificultades para aplicar el derecho al olvido. 3.1. Invocación de un motivo legítimo y fundado en los casos en que la publicación ha sido ordenada por la ley. 3.2. Concesión de una indemnización por incumplimiento de los deberes que derivan del ejercicio del derecho al olvido por parte del interesado. 3.3. ¿Podría ejercitar el derecho al olvido el heredero/apoderado digital? 4. Conclusiones

* Profesora Contratada Doctor. Universidad de Salamanca (España)

1. Introducción

El camino hacia la "sociedad de la información" no podría haberse iniciado sin una extraordinaria expansión de las redes de telecomunicaciones y, en particular, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Hoy por hoy, Internet constituye una herramienta que se ha ido incorporando de forma progresiva e imparable a la vida económica y social (ej. ámbito laboral, ocio, comunicación, trámites administrativos), y es utilizada por la inmensa mayoría de la población[1].

[1] Los estudios del INE español demuestran que, en 2016, el 77,1% de los hogares españoles con al menos un miembro de 16 a 74 años disponía de ordenador; ocho de cada 10 personas de 16 a 74 años habían usado Internet en los tres últimos meses y dos de cada tres lo hacían a diario; el 81,9% de los hogares españoles contaba con acceso a la Red, existiendo más de 13 millones de viviendas familiares con acceso a Internet; el 81,2% de dichos hogares utilizaba banda ancha (ADSL, red de cable,...), teniendo la banda estrecha una presencia testimonial. El 66.8 % de los usuarios de internet había usado las redes sociales en los últimos tres meses. Y, en el apartado de "privacidad, seguridad y confianza en internet", revelaban que el 73.5 % de los usuarios de Internet reconocía haber suministrado algún tipo de información personal a través de la red en los 12 últimos meses; el 65,7% hacía referencia a datos personales (nombre, fecha de nacimiento, etc.); el 65,1% aludía a datos de contacto (dirección, número de teléfono, etc.); el 45.2 %, a detalles de pago y el 31,5 %, a otra información personal. El 73,8% de los usuarios de Internet había realizado en los últimos 12 meses alguna acción dirigida a gestionar el acceso a su información personal en Internet: dichas acciones iban dirigidas normalmente a denegar el permiso del uso de la información personal para fines publicitarios (51,6%), comprobar que el sitio web donde se necesitó proporcionar información personal era seguro (50,4%) y limitar el acceso a su perfil o contenido en las redes sociales (49,6%); pero también se mencionaban acciones orientadas a restringir el acceso a su ubicación geográfica (39,6%) y leer la política de privacidad de los sitios web antes de proporcionar información personal (36,0%). El 62,9% de los usuarios de Internet en el último año declaraba conocer que las "cookies" son unos ficheros que se permiten rastrear los movimientos de las personas en Internet, a fin de hacer un perfil de cada usuario y presentarles anuncios a medida pero sólo el 31,0% de los usuarios manifestaba haber realizado modificaciones en la configuración del navegador para prevenir o limitar las cookies. Ante la posibilidad de que sus actividades online pudieran estar siendo monitorizadas para ofrecerle publicidad a medida, el 61,1% declaró sentir algún tipo de inquietud, el 17,3% declaró estar muy preocupado y el 43,8% algo preocupado; ahora bien, solo un 17,0% declaró utilizar algún software anti-rastreo para limitar la capacidad de seguimiento de sus actividades en Internet, si bien una gran mayoría (78,6%) declaró usar algún tipo de software o herramienta de seguridad informática. En cuanto a su grado de confianza en Internet, poco o nada era la respuesta para el 32,5%, bastante para el 58,5% y mucho el 9,0%. Datos extraídos de la "Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. Año 2016". Nota de prensa del INE publicada en http://www.ine.es/prensa/np991.pdf (consultado el 12 de enero de 2017). Los datos ofrecidos por el INE de Portugal no son tan exhaustivos, ni tan recientes; por comentar algunos de los más próximos en el tiempo, en 2015, el 68.6% de los individuos con edad comprendida entre 16 y 74 años utilizaron internet en los tres primeros meses del año; en 2016, el 74.1 % de los hogares con al menos una persona con edad comprendida entre 16 y 74 años disponían de acceso a la red; la inmensa mayoría de los hogares utilizaba banda ancha para acceder a internet (41.7% móvil, 38.2% cable, 31.7 fibra óptica, 26.2 % ADSL, según datos de 2015); en 2015, el 34,5 % facilitó información personal para redes sociales o profesionales; el 4,1 % experimentó problemas de violación de información personal enviada por internet o intromisión en su intimidad. Esta información, publicada por el Instituto Nacional de Estadística portugués, puede consultarse en https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_bdc_tree&contexto=bd&selTab=tab2 (consultado el 13/01/2017).

Sus ventajas son innumerables; de eso no cabe ninguna duda. Ahora bien, Internet también lleva consigo una mayor exposición (consciente o inconsciente) de nuestros datos personales, entendiendo por tales cualquier información concerniente a personas físicas identificadas o identificables[2]. En este nuevo tipo de control social digital los ciudadanos son a la vez fuente y destino de la información que se encuentra disponible en la red de redes; no resulta fácil censurar de alguna forma la actividad informativa que se desarrolla en la web "pues los parámetros de espacio y tiempo se difuminan en la misma"; y la amenaza de una potencial manipulación de la información proyecta su sombra con fuerza. La preocupación crece cuando comprobamos que la cantidad de información disponible en Internet no sólo es ingente sino que, en no pocas ocasiones, ha sido obtenida a través de aplicaciones de geolocalización, cookies, direcciones IPs... o deriva incluso de publicaciones oficiales y permanece en la red a disposición del público en general *per secula seculorum*[3]; que los motores de búsqueda permiten crear perfiles digitales individualizados de los ciudadanos – que pueden ser exactos o no- como consecuencia del tratamiento de datos que realizan[4]; que no es fácil identificar a quien difunde una determinada información, por poner sólo algunos ejemplos[5].

2. Construyendo el "derecho al olvido"

El derecho al olvido es el derecho que tiene el titular de un dato a que éste sea borrado o bloqueado, cuando se produzcan determinadas circunstancias y, en particular, que no sea accesible a través de la red Internet.

[2] Así se definen en el art. 2 a) de la Directiva 1995/46/CE y en el art. 4.1 del Reglamento (UE) 2016/679, los cuales añaden *"se considerará 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".*

[3] La perennidad de la información va ligada a su desactualización y, muchas veces también, a su descontextualización.

[4] Basta poner el nombre de una persona en un buscador para que sus datos personales aparezcan, procedentes de una web institucional, un periódico, un boletín oficial... (piénsese por ej. en los datos relativos a su puesto de trabajo, una sanción administrativa, un embargo, un indulto...)

[5] Son numerosos los autores que hacen referencia a los riesgos que entraña Internet. Sirvan como muestra: LÓPEZ PORTAS, Begoña, "La protección de datos personas en el universo 3.0: el derecho al olvido en la Unión Europea tras la Sentencia del TJUE de 13 de mayo de 2014, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 38, Mayo-Agosto 2015, pág. 272; ESTANCONA PÉREZ, Araya Lucía, "Un derecho al olvido en Europa", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 36, septiembre-diciembre 2014, pág. 468; CORREIA, Victor, *Sobre a privacidade*, Sinapis editores, 2016, pág. 87-99.

Su reconocimiento en la STJUE de 13 de mayo de 2014 y su plasmación en el Reglamento (UE) 2016/679, del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos, en adelante, RGPD) han contribuido a ponerlo de moda, mas no parece que estemos ante un derecho de nuevo cuño[6].

2.1. El derecho al olvido como manifestación del derecho a la autodeterminación informativa

2.1.1. La protección de datos de carácter personal como derecho fundamental

2.1.1.1. España

En España, el art. 18.1 de nuestra Carta Magna (en adelante, CE) establece: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*; y el art. 18.4 añade: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. De acuerdo con la doctrina de nuestro Tribunal Constitucional (TC), este último apartado impone un mandato al legislador como garantía del derecho al honor y a la intimidad pero consagra, al mismo tiempo, un derecho fundamental: "el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama «la informática»"[7].

El máximo intérprete de nuestra Carta Magna se ha encargado igualmente de diferenciar el derecho a la protección de datos de carácter personal y el derecho a la intimidad[8]. En este orden de cosas, ha señalado que el derecho a la intimidad no agota su contenido en facultades meramente negativas, de exclusión[9]. "La garantía de la intimidad, *latu sensu*", -afirma en el FJ 4 de su STC 11/1998, de 13 de enero- adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

Ahora bien, aunque el derecho a la protección de datos comparte con el derecho a la intimidad el objetivo de proteger la vida privada personal y familiar, no puede decirse que ambos derechos cumplan una misma función, tengan una misma finalidad y cuenten con un mismo contenido: todo lo contrario.

El derecho fundamental a la intimidad del art. 18.1 CE pretende proteger a la persona frente a cualquier invasión que pueda realizarse en aquel ámbito de su vida personal y familiar que desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad[10], "necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana"[11]. El derecho fundamental a la protección de datos, en cambio, persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. El derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, o dicho con otras palabras, permite resguardar la vida privada de una persona de una publicidad no querida. El derecho a la protección de datos, por su parte, garantiza a los individuos un poder de disposición sobre esos datos. "Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Pero ese poder de disposición sobre los propios

[6] Según algunos, la primera en hablar de derecho al olvido fue la Commission Nationale de l'Informatique et les libertés en Francia y lo hizo con la intención de dar un desarrollo mayor al derecho de oposición. Otros en cambio sostienen que su configuración es obra de la jurisprudencia norteamericana; concretamente, con el asunto Mevin V. Reid que en 1931 falló a favor de una mujer cuya vida fue llevada a la gran pantalla utilizándose su nombre de soltera sin su consentimiento. En tal sentido puede verse BOTANA GARCÍA, Gema Alejandra "Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea a propósito de la cuestión prejudicial planteada por la Audiencia Nacional en el Caso Google", *Práctica de Derecho de Daños*, Nº 120, 2014, (LA LEY 3941/2014). MARQUES WOHJAN, Bruna y WISNIEWSKI, Alice "Direito ao esquecimento: algumas perspectivas", disponible en http://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13227/2271 (consultado el 25/01/2017), apuntan que tiene su origen en Alemania, con el caso Lebach.

[7] Así lo afirma, por primera vez, en la STC 254/1993, de 20 de julio (FJ 6); insiste en ello en las SSTC 292/2000, de 30 de noviembre (FJ 5); 290/2000, de 30 de noviembre (FJ 7); 202/1999, de 8 de noviembre (FJ 2); 94/ 1998, de 4 de mayo (FJ 6); 143/1994, de 9 de mayo (FJ 7).

[8] En España, el TC ha incidido no sólo en la vinculación existente entre el derecho a la protección de datos frente al uso de la informática y el derecho al honor, sino también entre el derecho que nos ocupa y la libertad ideológica, sindical y religiosa, pues la utilización de medios informáticos puede poner en riesgo tales derechos y afectar a datos sensibles de la persona que pueden ser objeto de tráfico ilícito o de una utilización abusiva y distinta de la legítima finalidad para la que fueron recabados. A tal efecto pueden verse las SSTC 11/1998, de 12 de febrero y 45/1999, de 22 de marzo).

[9] Incide en esta cuestión, por ejemplo, en la STC 254/1993, de 20 de julio (FJ 5).

[10] Véase la STC 144/1999, de 22 de julio (FJ 8).

[11] Véase la STC 231/1988, de 2 de diciembre (FJ 3).

datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin"[12].

El objeto de protección, por tanto, es más amplio en el caso del derecho a la protección de datos, pues su garantía no se extiende únicamente a la intimidad (en su dimensión constitucionalmente protegida por el art. 18.1 CE) sino que comprende "la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal", como el derecho al honor, y al pleno ejercicio de los derechos de la persona (art. 18.4 CE). El derecho fundamental a la protección de datos amplía, pues, la garantía constitucional a aquellos datos "que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado. De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual" (para eso está ya la protección que confiere el art. 18.1 CE), "sino los datos de carácter personal". En consecuencia, alcanza también a aquellos datos personales públicos, que por el hecho de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado pues así lo garantiza su derecho a la protección de datos. La calificación de "carácter personal" de los datos no significa que sólo quedan amparados los relativos a la vida privada o íntima de la persona; significa que se protegen todos aquellos que contribuyan a la identificación de la persona, "pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"[13].

Distinto es también el contenido de uno y otro derecho. El derecho a la intimidad confiere a su titular el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido[14]; el derecho a la protección de datos, por su parte, "atribuye a su titular un haz de facultades consistente en diversos poderes

[12] Así lo pone de relieve la STC 292/2000, de 30 de noviembre (FJ 6).

[13] Véase, en este sentido, la STC 292/2000, de 30 de noviembre (FJ 6).

[14] Así lo ha puesto de relieve reiteradamente nuestro TC. Sirvan como muestra las SSTC 73/1982, de 2 de diciembre (FJ 5); 110/1984, de 26 de noviembre (FJ 3); 89/1987, de 3 de junio (FJ 3); 231/ 1988, de 2 de diciembre (FJ 3); 197/1991, de 17 de octubre (FJ 3); y, más en general, las SSTC 134/1999, de 15 de julio, o 115/2000, de 10 de mayo.

jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los ya mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales"[15/16].

A la vista de la jurisprudencia del TC cabe concluir, por tanto, que la protección de datos constituye un derecho fundamental, estrechamente vinculado con el derecho a la intimidad pero independiente de él, que se caracteriza por garantizar a la persona el control de sus datos personales, especialmente de su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados[17].

2.1.1.2. Portugal

El art. 26 de la Carta Magna portuguesa (en adelante, CRP) establece:

1. "*A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação*".

2. *A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.(...)*".

Y el art. 35 –relativo expresamente a la "*Utilização da informática*" y cuya reforma en 1997 fue imprescindible para trasponer la *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, al Ordenamiento de

[15] STC 292/2000, de 30 de noviembre, FJ 6; véase también la STC 254/1993, de 20 de julio (FJ 7).

[16] Un análisis detenido de la jurisprudencia dictada por el TC español sobre el derecho a la protección de datos puede verse en Hernández Ramos, Mario, "El derecho al olvido en internet como nuevo derecho fundamental en la sociedad de la información. Perspectiva constitucional española y europea", *Quid Iuris*, Vol. 21, junio-agosto 2013, pág. 120-125.

[17] Especialmente, las SSTC 254/1993, de 20 de julio; 290/2000, de 30 de noviembre; y 292/2000, de 30 de noviembre.

nuestro país vecino- reconoce el derecho a la autodeterminación informativa[18] en los términos que siguen:

> 1. *"Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.*
>
> 2. *A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.*
>
> 3. *A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*
>
> 4. *É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.*
>
> 5. *É proibida a atribuição de um número nacional único aos cidadãos.*
>
> 6. *A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*
>
> 7. *Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei"*[19][20].

[18] En palabras de Queiroz, Cristina "A protecção constitucional da recolha e tratamento de daos pessoais automatizados" en *Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles. 90 años*, Almedina, Coimbra, 2007, pág. 292, "O direito geral à auto-determinação informacional deve ser comprendido como uma especificação do disposto no art. 1º da Constituição ao postular a *dignidade da pessoa humana* como "valor fundamental" e ainda do disposto no art. 2º relativo à protecção e garantia do "respeito" e "efectivação" dos "direitos e liberdades fundamentais". Se trata de un derecho relativo (no absoluto) que guarda especial relación con el derecho al desarrollo de la personalidad y el derecho a la intimidad en la vida privada y familiar; su protección, por consiguiente, está sujeta a límites.

[19] La de 1997 no era la primera reforma que sufría el precepto (tras la aprobación de la CRP en 1976, se había modificado ya en 1982 y 1989). Un exhaustivo análisis de la evolución que ha sufrido el mismo puede verse en Pinheiro, Alexandre Sousa, *Privacy e Trotecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Ed. Associação académica da faculdade de direito de Lisboa, Lisboa, 2015, pág. 665 y ss y Lopes, Joaquim de Seabra, "Oartigo 35º da Constituição: dagénese à atualidade e ao futuro previsível", *Revista Forum de Protecçao de dados*, nº janeiro, 2016, pág. 14-49, https://www.cnpd.pt/bin/revistaforum/forum2016_2/index.html#15/z (consultado el 13/01/2017).

[20] Junto a estos preceptos debe tenerse en cuenta, por una parte, el art. 18.1 CRP relativo a la eficacia horizontal directa o inmediata de los derechos fundamentales, según el cual: *"Os preceitos constitucionais respeitantes aos dircitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas"*. Y es que, como pone de relieve Miranda, Jorge, *Manual de direito constitucional*, T. IV, 2ª ed. Coimbra editora, Coimbra, 1998, pág. 321-324, los derechos fundamentales inciden, o pueden incidir, tanto en las relaciones con entidades públicas como en las relaciones con particulares y es preciso proteger el respeto a la dignidad de la persona humana y la autonomía del individuo no sólo en el ámbito de las relaciones con el Estado sino también en el marco de las relaciones que las personas establecen entre sí. Así se desprende del art. 26.1 CRP (proteção da reserva da intimidade e da vida privada), art. 35.2 CRP (proibição de acesso de terceiros aos arquivos de dados pessoais), art. 37.4 CRP (direito de rectificação, resposta e indenização por danos sofridos por meio da imprensa), art. 60.1 CPR (direito dos consumidores à informação, à proteção da saúde e dos seus interesses econômicos e à reparação de danos), art. 42.2 CRP (direitos do autor).
Y, por otra, los art. 70 y ss CCPort (relativos a los derechos de la personalidad) y art. 335 CCPort (ofrece los criterios para resolver los conflictos que pueden darse entre distintos derechos).

El TC portugués, en consonancia con las opiniones vertidas por la doctrina, viene diciendo que el derecho a estar solo (*"direito à solidão"*), el derecho al anonimato (*"direito ao anonimato"*) y el derecho a la autodeterminación informativa (*"direito à autodeterminação informativa"*) – entendido, este último, como el derecho del individuo a controlar el acceso a sus datos personales por parte de terceros- son manifestaciones del derecho a la intimidad (*"direito à reserva da intimidade da vida privada"*) que se encuentran estrechamente relacionadas entre sí[21]. En su Acórdão nº 230/2008, afirma: "O bem jurídico protegido pelo *direito à reserva da intimidade da vida privada* é, em larga medida (e nisso se distinguindo ele do bem protegido pelos demais direitos pessoais consagrados no artigo 26º), algo que diz respeito à *informação em sentido lato*[22], pelo que a prossecução de tal bem se realiza através do direito, que cada um tem, de *evitar ou controlar a tomada de conhecimento, por parte de terceiros, de informações relativas à sua própria «privacidade»*"[23]. En esta resolución, el TC de Portugal examina una manifestación concreta del derecho a la autodeterminación informativa que deriva de la previsión del art. 35.4 CRP: la prohibición del acceso no autorizado a los datos personales; pero no analiza cómo se relacionan entre sí los art. 26 y 35.4 CRP[24][25].

En el ámbito doctrinal, Correia sostiene que "o conceito de *proteção de dados*, assim como o conceito de *autodeterminação informativa*, não são mais do que uma nova aplicação jurídica do direito a privacidade, pois quando se defende o direito à proteção de dados pessoais, e à autodeterminação informativa, defende-se impli-

[21] Acórdãos nºs 230/2008, 306/2003 e 368/2002, disponibles en http://www.tribunalconstitucional.pt; Acórdão nº 355/97, em *Acórdãos do Tribunal Constitucional*, 37º vol., p. 7 y ss.

[22] Pinto, Paulo Mota "O Direito à Reserva sobre a Intimidade da Vida Privada", em *Boletim da Faculdade de Direito*, 69, 1993, p. 525.

[23] Seguidamente reconoce que el ámbito de protección de esa "reserva" no es fácil de determinar dada la indeterminación del concepto de privacidad.

[24] A su juicio: "Não interessa agora indagar como, e em que medida, se relacionam um e outro preceitos constitucionais: saber, por exemplo, se a proibição contida no nº 4 do artigo 35º valerá apenas – como parece indicar a epígrafe do preceito – para os casos de utilização de informática, alargando-se assim o tatbestand do direito que já vinha consagrado no artigo 26º, é questão de resolução por agora inútil. Certo é – e só essa certeza releva para o caso concreto – que aí onde não houver lesão do direito-matriz, que é afinal o direito à autodeterminação informativa, também não haverá lesão dessa sua expressão particularizada que é aquela que decorre do nº 4 do artigo 35º".

[25] También puede verse el Acórdão TC 555/2007, referido a un supuesto muy parecido.

caitamente algo que, no fundo, está incluído no direito à privacidade"[26]. Por su parte, PINHEIRO se refiere a la evolución del derecho a la protección de datos hacia un nuevo y más completo derecho a la identidad digital (*"direito à identidade informacional"*). Dicho derecho "tem integração constitucional por via não só do art. 35, mas especialmente do art. 26 CRP". Estamos, por tanto, ante un derecho que comprende los aspectos propios de la protección de datos personales, aproximándolos a los derechos de identidad personal y libre desarrollo de la personalidad; estamos ante un derecho de la personalidad[27].

Se considere, pues, el derecho a la protección de los datos personales como un derecho autónomo o se entienda como un nuevo ámbito de aplicación del derecho a la intimidad, ambos países lo reconocen en sus textos constitucionales como un derecho fundamental.

2.1.2. El derecho a la protección de datos en la normativa comunitaria

A nivel comunitario, el derecho a la protección de datos se reguló inicialmente en el Convenio Nº 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual determinó la aprobación de la Directiva 1995/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. La trasposición de esta Directiva al Ordenamiento portugués vino de la mano de la lei nº 67/1998, de 26 de outubro, sobre a proteção dos dados pessoais, una vez reformado el art. 35 CRP[28]. En España, se llevó a cabo a través de la LO 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD), ley que fue objeto de desarrollo por el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la referida LO (RDLOPD). Ambas leyes –la española y la portuguesa- prevén su aplicación al tratamiento de datos efectuado tanto por entidades públicas como por entidades privadas privadas; ahora bien, beneficiarios son sólo las personas físicas.

La Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, tradujo los principios

[26] CORREIA, Victor, *Sobre a privacidade, op. cit.*, pág. 72.
[27] PINHEIRO, Alexandre Sousa, *Privacy..., op. cit.*, pág. 777-819.
[28] Dicha Ley fue modificada por la Lei 103/2015, de 24 de agosto.

establecidos en la Directiva 95/46/CE en normas concretas para el sector de las telecomunicaciones. La necesidad de adaptar dicha Directiva de 1997 al desarrollo de los mercados y las tecnologías de los servicios de comunicaciones electrónicas motivó su derogación y su sustitución por la actual Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Esta última Directiva fue traspuesta al Ordenamiento portugués por la Lei nº 41/2004, de 18 de Agosto, sobre protecção do dados pessoais e privacidade nas telecomunicações[29] y al español por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, hoy derogada y sustituida por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

La Directiva 1995/46/CE quedará sin efecto el 25 de mayo de 2018 por obra del RGPD, el cual entró en vigor a los 20 días de su publicación en el *DOUE* pero no será aplicable hasta el 25 de mayo de 2018[30]. A partir de entonces, toda referencia hecha a la referida Directiva deberá entenderse hecha al Reglamento. Dicho Reglamento, sin embargo, no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE

En el ámbito de la UE, el derecho a la protección de datos aparece expresamente reconocido, además, en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE)[31].

En el presente trabajo, nos proponemos estudiar cómo ha ido construyéndose el derecho al olvido o derecho a la supresión de datos, que recoge hoy el RGPD, partiendo de la base de que un amparo excesivo de dicho derecho podría

[29] Dicha Ley fue modificada por la Lei 46/2012, de 29 de agosto.
[30] Reglamento publicado en el *DOUE* L 119, de 4 de mayo de 2016, pág. 1.-88.
[31] Art. 7 Carta de Derechos Fundamentales de la Unión Europea, dedicado al "Respeto de la vida privada y familiar", determina: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".*
Art. 8 Carta de Derechos Fundamentales de la Unión Europea, bajo la rúbrica "Protección de datos de carácter personal", establece:
1. *"Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente".*

permitirnos crear un pasado a nuestra medida e incidiendo en las dificultades que plantea su aplicación[32].

2.2. Planteamiento del problema tomando como referencia el caso Costeja

Imaginemos que, como consecuencia del impago de una deuda, aparecemos en un listado de morosos que es publicado por un medio de comunicación. Años más tarde, comprobamos que, cuando ponemos nuestro nombre en el buscador de Google (es el más utilizado), aparece un enlace que lleva indefectiblemente a la web en que se publicó aquel listado de morosos. Sigamos imaginando, imaginemos que nosotros ya hemos saldado aquella deuda; ya no somos morosos y, en consecuencia, no queremos que esa información siga estando accesible en la web. La pregunta que nos formularíamos sería: ¿Podemos hacer algo frente al titular de la página web en que se publica dicha información? ¿Podemos hacer algo frente a Google?[33]

Esto es lo que le ocurrió a Mario Costeja, quien inició el proceso correspondiente al darse cuenta de que su nombre aparecía en el buscador ligado a una información de «La Vanguardia», publicada 15 años atrás, sobre un anuncio de una subasta de bienes embargados por una deuda con la Seguridad Social. La deuda había sido pagada pero su nombre seguía apareciendo; ¡para Google seguía siendo deudor![34]

[32] AZURMENDI, Ana, "Por un «derecho al olvido» para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia Europeo del caso *Google Spain* y su recepción por la sentencia de la Audiencia Nacional española de 29 de diciembre de 2014", *Revista de Derecho Político*, nº 92, enero-abril, 2015, pág. 294-301, señala que el derecho al olvido se configura como una consecuencia del derecho a la autodeterminación informativa; su perfil se diferencia del de otros derechos de la personalidad reconocidos en el art. 18 CE, pues el derecho al olvido se concentra en las reglas de protección de datos personales.

[33] Una pregunta similar podría formularse la mujer, víctima de malos tratos, que concurre a un procedimiento de concurso-oposición para acceder a la función pública en España y, como consecuencia, ve publicados múltiples datos personales en internet, el político condenado por malversación de caudales públicos que fue indultado pocos años después o el profesor universitario que fue injustamente acusado de plagio hace años, por ejemplo.

[34] El 19 de enero 1998 el matutino español "La Vanguardia" publicó en su pág. 23 un habitual anuncio de subastas del Ministerio de Trabajo con inmuebles embargados por la Secretaría de Seguridad Social; en él, aparecía casi una veintena de propiedades con su correspondiente localización, descripción y dueño; una de ellas era una propiedad indivisa de 90 m2 en San Feliú de Llobregat (Cataluña), perteneciente a Mario Costeja González y esposa.
Diez años más tarde, dicho matutino digitalizó íntegramente su hemeroteca, quedando disponible en internet gratuitamente todo el material, en formato PDF, y permitiendo búsquedas por fechas y palabras. Los robots o arañas de internet hicieron su trabajo: registraron de forma automática e indexaron la información de la web y los contenidos históricos de la Vanguardia empezaron a aparecer en los resultados de Google.

2.3. Canalización del problema a través de los llamados derechos ARCO

El Ordenamiento español no contenía norma alguna que regulara el derecho al olvido, como tal, con carácter general[35]; pero sí ofrecía instrumentos que permitían instar que se borrara o se bloqueara el acceso a los datos en cuestión pues regulaba y regula los denominados derechos ARCO: Derecho de acceso, rectificación, cancelación y oposición[36]. El ejercicio de estos dos últimos (reconocidos en los art. 16 y 17 LO 15/1999, de Protección de datos de carácter personal[37]) podía

Para ese entonces, Mario Costeja González se había divorciado, había pagado su deuda a Seguridad Social y, un buen día, al poner su nombre en Google y picar sobre buscar, se encontró con que el resultado para la cadena "Mario+Costeja+González" arrojaba entre los primeros resultados un enlace a aquella pág. 23 de la Vanguardia de 1998, donde figuraba su nombre y apellido en el anuncio de los embargos judiciales. Ante esta circunstancia, Mario Costeja (abogado y perito calígrafo judicial – en aquel momento, consultor de empresas –) se dirigió a "La Vanguardia Ediciones S.L." y, ejercitando su derecho de oposición al tratamiento de sus datos personales, solicitó su remoción pero La Vanguardia se negó a suprimir la información ya que había sido publicada en forma lícita, proveniente de un organismo del Estado (que a su vez lo hacía para dar cumplimiento a la legislación). No pudiendo actuar contra el diario, Costeja se dirigió a Google. En última instancia, el problema para Costeja no era tanto figurar en la hemeroteca digital de La Vanguardia como aparecer en los resultados del buscador más consultado del mundo – que sus posibles clientes también utilizarían para obtener referencias personales de él-. La respuesta de Google tampoco fue favorable.

[35] A nivel europeo, la referencia al derecho al olvido aparece en la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre un enfoque global de la protección de los datos personales en la Unión Europea, de 4 de noviembre de 2010 [COM (2010) 609 final].

[36] El derecho a la protección de datos se concreta en el derecho a oponerse a que determinados datos sean recabados o utilizados para fines diferentes de aquél que justificó su obtención, así como en el derecho a que se cancelen o se rectifiquen los datos del sujeto en cuestión. Véanse los art. 5d), 6.4, 15 y 16 LOPD, en España y los art. 10, 11 y 12 de la Lei nº 67/98, en Portugal.

[37] Art. 16 LOPD: *Derecho de rectificación y cancelación*
1. *"El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.*
2. *Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.*
3. *La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.*
4. *Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.*
5. *Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".*
Íntimamente relacionado con lo dispuesto en el art. 16.3 y 16.5 LOPD se encuentra el art. 22 RD 1720/2007, el cual establece el deber de destruir o devolver los datos al responsable una vez cumplida la prestación contractual; ahora bien, en el caso de que exista una previsión legal que exija su conservación no procederá la destrucción de los datos sino que deberá procederse a su devolución garantizando el responsable del fichero dicha conservación; y también el informe AEPD 408/2010 que, recogiendo la

amparar la referida pretensión. No en vano, según el art. 31.2 RD 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD, *"El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este Reglamento"*. Y el art. 34 del mismo texto reglamentario define el derecho de oposición como *"el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:*

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.
b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este Reglamento, cualquiera que sea la empresa responsable de su creación.
c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este Reglamento.

Tales derechos no operan en todo caso; no en vano, la propia LOPD fija límites a los mismos en los art. 22, 23, 16.5, 4.1, 6.4, a los que hay que sumar la libertad de información y los ficheros excluidos de la LOPD, fundamentalmente[38]. Junto a los preceptos citados, resulta de interés para el caso el art. 29.4 LOPD, según el cual:

doctrina sentada en el de 1 de agosto de 2005, ofrece algunos criterios orientativos para tratar de determinar el plazo a que se refiere el art. 16.3 ya que no es posible fijar un plazo concreto.
Art. 17. *Procedimiento de oposición, acceso, rectificación o cancelación*
1. *"Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.*
2. *No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación".*
En Portugal, habría que atender al art. 11.1 de la Lei 67/98, según el cual: *"O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos: d) A rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente lei, nomeadamente devido ao carácter incompleto ou inexacto desses dados; e) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea d), salvo se isso for comprovadamente impossível"*. El art. 12, por su parte, reza: *"O titular dos dados tem o direito de: a) Salvo disposição legal em contrário, e pelo menos nos casos referidos nas alíneas d) e e) do artigo 6º, se opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados"*.

[38] En Portugal se establecen límites al derecho de acceso (ámbito en el que se regula el derecho de cancelación de los datos) en el propio art. 11, apartados 2, 3, 4, 5 y 6 Lei 67/98, y con carácter más general, en los art. 5, 6, 7 y 8 de la misma, a los que debemos añadir los tratamientos a los que dicha ley no resulta aplicable.

"Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos" [39].

A la vista de esta normativa, Mario Costeja presentó una reclamación ante la AEPD contra la Vanguardia y contra Google Spain y Google Inc, solicitando que se exigiera a la Vanguardia la eliminación o modificación de la publicación a fin de que no aparecieran sus datos personales o la utilización de las herramientas facilitadas por los motores de búsqueda a fin de proteger dichos datos y, a Google Spain y a Google Inc, la eliminación y ocultación de sus datos a fin de que no se incluyeran en sus resultados de búsqueda[40]. Alegaba precisamente que el embargo había tenido lugar hacía años, era un asunto que estaba resuelto y había perdido su relevancia.

La AEPD, en Resolución de 30 de julio de 2010, desestimó la reclamación en relación a la Vanguardia (no en vano, la publicación que ésta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores) pero estimó la reclamación dirigida contra Google Spain y Google Inc., considerando que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. En consecuencia, le ordenó que retirara los enlaces.

[39] Este precepto, de alguna manera, recoge el derecho al olvido en los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.
En el ámbito sanitario, sin embargo, el art. 17 Ley 41/2002 impone a los centros sanitarios la obligación de conservar la documentación clínica durante el tiempo adecuado al caso y, como mínimo, 5 años contados desde la fecha del alta de cada proceso asistencial. Los datos de la historia clínica relacionados con el nacimiento del paciente que resulten determinantes para la determinación del vínculo de filiación con la madre no se destruirán. También debe conservarse la historia clínica a efectos judiciales y cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud.
[40] Conforme a lo previsto en el art. 18 LOPD: *Tutela de los derechos*
1. *"Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.*
2. *El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.*
3. *El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.*
4. *Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo".*
En Portugal, el art. 33 Lei 67/98, bajo la rúbrica *"Tutela administrativa e jurisdicional"*, establece: *"Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais"*.

2.4. La STJUE de 13 de mayo de 2014

Google Spain y Google Inc impugnaron la referida resolución de la AEPD ante la AN, quien optó por plantear una cuestión prejudicial al TJCE para que aclarase básicamente las siguientes cuestiones:

- ¿Puede entenderse que la actividad desarrollada por los buscadores consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, queda comprendida en el concepto de tratamiento de datos del art. 2 b) de la Directiva 95/46?
- Caso de ser así, ¿la empresa que gestiona (Google Search) es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?
- Si lo es, ¿se podría requerir directamente [a Google Search] para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información? ¿Se le podría exigir la retirada incluso cuando los datos en cuestión se hubieran publicado lícitamente por terceros y se mantenga la página de origen?
- ¿Es posible aplicar territorialmente la Directiva 95/46 a Google aunque su domicilio empresarial se encuentre fuera de la Unión Europea?
- ¿Debe interpretarse la Directiva en el sentido de que los derechos de supresión y bloqueo de los datos y el derecho de oposición comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de información publicada lícitamente por terceros?

La archiconocida STJCE de 13 de mayo de 2014 vino a dar respuesta a todos los interrogantes de la AN[41].

[41] Esta Sentencia causó cierta sorpresa pues es una de las pocas en las que el Tribunal no ha seguido la interpretación dada por el Abogado General en el dictamen preliminar. Así lo reconocen Botana, Gema Alejandra y Ovejero Puente, Ana Mª "Claves de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en la cuestión prejudicial planteada en el caso Google", *Actualidad Civil*, 9 de Junio

La primera de las cuestiones planteada tenía que ver con la aplicación material de la Directiva. Partiendo del concepto que ofrece el art. 2 b) de la Directiva 95/46 del «tratamiento de datos personales» como *"cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción"*, y teniendo en cuenta que, al explorar internet de manera automatizada, constante y sistemática, el gestor de un motor de búsqueda «recoge» una serie de datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas, el TJCE entiende que la actividad desarrollada por el gestor de un motor de búsqueda debe calificarse como tratamiento, aun cuando no diferencie, al realizar estas operaciones, entre datos personales y otros tipos de información y aunque se refieran a información ya publicada tal cual en los medios de comunicación.

En la medida en que es el propio gestor del motor de búsqueda quien determina los fines y los medios de dicha actividad, entiende que debe considerarse responsable del tratamiento al gestor del motor de búsqueda.

Por lo que se refiere a la aplicación territorial de la Directiva, el problema derivaba del hecho de que Google Inc tiene su domicilio social en California y tanto Google Inc como Google Spain alegaban que quien gestionaba Google Search era Google Inc sin intervención alguna de Google Spain, cuya actividad se limitaba a prestar apoyo a la actividad publicitaria del grupo Google, algo distinto de su servicio de motor de búsqueda. El TJCE sostiene, sin embargo, que Google Spain es una filial de Google Inc. en territorio español, constituye una instalación estable en España, está dotada de personalidad jurídica propia por lo que puede considerarse un «*establecimiento*» de los referidos en el art. 4.1 a) de la Directiva 95/46[42].

de 2014, (LA LEY 3951/2014), y más tangencialmente, Rallo Lombarte, Artemi "La garantía del «derecho al olvido» en internet", (BIB 2014\1761).
Entre quienes la han estudiado cabe citar a: García de Pablos, Jesús Félix, "El derecho al olvido en la red", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 36, Septiembre-Diciembre, 2014, pág. 47-66; Hernández Ramos, Mario, "Motores de búsqueda y derechos fundamentales en internet. La STJUE Google C-131/12, de 13 de mayo de 2014", *Revista General de Derecho Europeo*, nº 34, Octubre 2014, y "El derecho al olvido...", *op. cit.*, pág. 115-148.

[42] Para llegar a tal conclusión el Tribunal toma como inequívoca referencia interpretativa el Considerando 19 de la Directiva que requiere dos elementos característicos: 1') el ejercicio efectivo y real de una

Ahora bien, -reconoce el TJCE- para que resulten aplicables las disposiciones nacionales, el tratamiento de datos debe efectuarse «en el marco de las actividades» de dicho «establecimiento»[43]. En su opinión, el tratamiento de datos se efectúa «en el marco de las actividades» del establecimiento "si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor". Sobre esta base, concluye: "...se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro".

Como decíamos, la STJUE no admite matices al atribuir al gestor del buscador de Internet la condición de responsable del tratamiento de datos pues «determina los fines y los medios de esta actividad» en el sentido del art 2 d) de la Directiva 95/46. La STJUE establece las pautas que delimitan la responsabilidad de los webmasters en relación con la de los buscadores[44]:

- el tratamiento de datos efectuado por los buscadores es distinto al de los editores de sitios de Internet[45];
- el impacto de los buscadores sobredimensiona el tratamiento de datos en las webs de origen; los motores de búsqueda desempeñan un papel en la difusión global de dichos datos, pues facilitan su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado; además, la organización de la información publicada en internet por los motores de búsqueda permite a los usuarios obtener mediante una lista de resultados una visión estructurada de la información relativa al interesado que puede hallarse en internet y establecer sobre esa base un perfil más o menos detallado del interesado (este es el principal problema)
- la falta de utilización por los editores de sitios de Internet de protocolos de exclusión como *robot.txt* y de códigos como *noindex* o *noarchive* no libera «al gestor de un motor de búsqueda de su responsabilidad» puesto que el art. 2 d) de la Directiva 95/46 prevé expresamente que la determinación de fines y medios del tratamiento puede realizarse «sólo o conjuntamente con otros». Por lo tanto, independientemente del ejercicio de derechos que efectúen los ciudadanos ante los webmasters, los buscadores de Internet deberán atender idénticas pretensiones cuando se les dirijan directamente y en el marco específico de su actividad.

El TJCE no lleva a cabo una ponderación de los intereses en juego pero sí ofrece unos criterios para que el órgano jurisdiccional que eleva la consulta (la AN) la efectúe posteriormente. En este orden de cosas, teniendo presente que la injerencia en los derechos fundamentales del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo, entiende que, aunque el art. 7 f) de la Directiva 95/46 permite *a priori* el tratamiento de datos realizado por un motor de búsqueda pues resulta necesario para la satisfacción de su interés empresarial y económico legítimo[46], tal interés no puede prevalecer sobre los derechos y libertades funda-

actividad mediante una instalación estable, 2') sin que resulte determinante que la forma jurídica de dicho establecimiento sea una simple sucursal o una empresa filial con personalidad jurídica.

[43] Frente a la afirmación exculpatoria de que el tratamiento de datos lo efectúa exclusivamente Google Inc. como gestor de Google Search, sin que Google Spain tenga intervención alguna -limitándose a promocionar la actividad publicitaria del Google-, el Tribunal consideró que la protección eficaz y completa perseguida por la Directiva 95/46 obliga a *prescindir de una interpretación restrictiva* del «marco de actividades» del establecimiento reducida a que el tratamiento deba realizarse «por» el establecimiento.

[44] Como esta actividad puede afectar significativamente y de forma adicional a la de los editores de los sitios de internet, a los derechos fundamentales de respeto a la vida privada y protección de datos personales, el gestor del motor de búsqueda debe garantizar en el marco de sus responsabilidades, competencias y posibilidades que su actividad satisface las exigencias de la Directiva para que las garantías establecidas en ella tengan pleno efecto.

[45] El editor simplemente incluye información en la página web; el buscador, en cambio, almacena, trata, organiza, muestra y facilita el acceso a los datos.

[46] Recuerda el TJUE que, a tenor de lo dispuesto en el art. 6 de la Directiva y sin perjuicio de lo que los Estados miembros puedan haber establecido expresamente en relación al tratamiento con fines históricos, estadísticos o científicos, "incumbe al responsable del tratamiento garantizar que los datos personales sean «tratados de manera leal y lícita», que sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines», que sean «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente», que sean «exactos y, cuando sea necesario, actualizados», y, por último, que sean «conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente». En este marco, el mencionado responsable debe adoptar todas las medidas razonables para que los datos que no responden a los requisitos de esta disposición sean suprimidos rectificados".
Al hilo de esta cuestión, cabe recordar que la normativa portuguesa (art. 27 Lei 67/1998) impone al responsable del tratamiento de datos un deber de comunicación (notificación) previo a la Comisión Nacional de Protección de Datos y, tratándose de datos especialmente sensibles, su tratamiento está sujeto al correspondiente control administrativo (art. 7 Lei 67/1998). El tratamiento realizado por los motores de búsqueda estará sujeto, por tanto, a este deber. Y, según apunta Calvão, Filipa Urbano. "A proteção de dados pessoais na Internet: desenvolvimentos recentes", *Revista de Direito Intelectual*, nº 2, 2015, pág. 75, "os fundamentos para o efeito são difíceis de se verificar no caso concreto: consentimento expresso,

mentales del interesado consagrados en los arts. 7 y 8 CDFUE y, más concretamente, sobre la protección de sus datos personales[47]. Los buscadores, además, no son medios de comunicación ni actúan al amparo de la excepción periodística que se contempla en el art. 9 de la Directiva ni ejercen el derecho a informar. En consecuencia, el interesado puede solicitar el *derecho al olvido* ante el gestor del motor de búsqueda ejerciendo los derechos de cancelación y oposición previstos en los arts. 12 b) y 14.1 a) de la Directiva 95/46. De acuerdo con los postulados de la STJUE, los motores de búsqueda están obligados a eliminar de la lista de resultados -obtenida mediante el rastreo del nombre de una persona- los vínculos a páginas web publicadas por terceros que contienen información relativa a la misma, aunque no se borren previa o simultáneamente de las referidas webs e, incluso, aunque la publicación sea en sí misma lícita. Llegados a este punto no podemos olvidar que el TJUE, tomando como referencia los principios de calidad y necesidad en el tratamiento de los datos (recogidos en el art. 6 de la Directiva 95/46), entiende que el tratamiento de los datos inicialmente lícito puede devenir incompatible con la Directiva con el paso del tiempo, esto es, cuando ya no sean necesarios en relación a los fines para los que fueron recogidos o tratados o sean inadecuados, no pertinentes o excesivos; en estos casos, podrá ejercitarse el derecho de oposición aunque no exista un perjuicio para el interesado, a menos que se trate de un personaje público.

Siguiendo con los intereses a tener en cuenta, cabe señalar que la STJUE no reconoce *a priori* un interés legítimo suficiente a *los internautas* que pueda anteponerse al de aquellos que justifican su pretensión de cancelación de datos en los resultados de las búsquedas y restringen la relevancia del interés legítimo de los internautas. Para el TJUE, el interés del público internauta sólo será objeto de valoración y ponderación en el caso concreto cuando los datos personales que se pretende borrar de los índices de búsqueda afecten a un personaje público o a una información de interés

informado e específico de cada um dos titulares dos dados pessoais ou reconhecimento pela autoridade de proteção de dados pessoais do interesse público importante indispensável ao desempenho das atribuiçõoes dessa entidade" (opta por una interpretación restrictiva: "entidades públicas" o "entidades que têm a seu cargo a prossecução de interesses públicos").

[47] Calvão, Filipa Urbano. "A proteção...", *op. cit.*, pág. 77 y 78, se plantea la posibilidad de argumentar que existe una transacción comercial entre el prestador del servicio de búsqueda y el usuario pero lo cierto es que tal afirmación es difícilmente sustentable en sociedades como las europeas. Por una parte, porque –como bien dice- un usuario normal de Internet no se percata de que se encuentra ante una relación de este tipo (particularmente si hablamos de menores) y tampoco es consciente de pagar un precio por el servicio; el servicio es aparentemente gratuito; el "precio" sería la publicidad que acompaña la búsqueda. Y, por otra, porque esa mercantilización de los datos personales conduce a una cosificación de la dignidad humana.

público[48]; aunque, en todo caso, deberán evaluarse tanto la naturaleza de la información como su sensibilidad e impacto en la intimidad de la persona afectada[49].

La STJUE no admite, como pretendía Google apelando al principio de proporcionalidad, que las solicitudes de cancelación deban dirigirse exclusiva o, incluso previamente, al editor del sitio de Internet. Dada la facilidad con que la información publicada en un sitio de internet puede copiarse en otros y que sus responsables no siempre están sujetos a las normas de la UE, difícilmente podría llevarse a cabo una protección eficaz y completa de los interesados si éstos tuvieran que obtener con carácter previo o paralelo la eliminación de la información que les afecta de los editores de los sitios web de internet.

2.5. Valoración doctrinal de la STJUE

La STJUE ha sido bastante bien acogida por la doctrina. Sus postulados son plenamente compartidos por Plaza Penadés, por ejemplo, quien resalta que no afecta única y exclusivamente a Google y demás motores o instrumentos de búsqueda; "afecta a cualquier plataforma tecnológica que permite el tratamiento de datos personales, como ocurre con muchas redes sociales y otros dispositivos tecnológicos"[50]. Como célebre la ha calificado Calvão, a pesar de considerar que el término "derecho al olvido" no es el más adecuado en este caso (es un supuesto de derecho de oposición); la autora últimamente citada resalta también, de una forma muy especial, el efecto extraterritorial de esta Sentencia no declarado por

[48] A la vista del razonamiento seguido por el TJUE, cabe afirmar que, en cualquier caso, el derecho de información de los internautas sigue estando asegurado pues la información puede seguir estando disponible en la web de origen; incluso podría buscarse a través del motor de búsqueda pero no a partir del nombre del individuo sino utilizando otros términos para la búsqueda. Incide también en esta cuestión Calvão, Filipa Urbano. "A proteção...", *op. cit.*, pág. 78.

[49] Calvão, Filipa Urbano. "A proteção...", *op. cit.*, pág. 77, alude también al hipotético interés que podría tener el editor de la página web, el cual no se ve afectado pues "não há um direito do editor à apresentação dos conteúdos publicados no correspondente sítio na Internet na lista de resultados de uma pesquisa realizada a partir de um nome de um indivíduo ou de outro dado pessoal. Quando muito poderia ser-lhe reconhecida uma posição subjetiva (interesse) tutleada *a latere*, apenas protegida como efeito reflexo da proteção do direito à liberdade de informação ou da liberdade de impensa".

[50] PLAZA PENADÉS, Javier. "Doctrina del TJUE sobre protección de datos y derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 35, Mayo-Agosto, pág. 19. Para López Portas, Begoña, "La protección...", *op. cit.*, pág. 285, la STJUE constituye una gran avance en la garantía de los derechos del cibernautas aunque –añade- sólo constituye el primer paso. En su opinión, los límites que fija el configuración del derecho al olvido plantean problemas "tanto desde el punto de vista material –la información personal disponible en la *web* debe presentar los elementos señaladas y solo se elimina su indexación- como desde el punto de vista de los sujetos implicados o de su alcance jurídico-territorial".

el TJUE; en el contexto de internet –afirma- la protección de los datos personales y del derecho a la intimidad precisan "uma afirmação sem fronteiras do direito a desassociação do nome de uma pessoa do resultado da pesquisa", pero ni los tribunales de los Estados miembros ni las Agencias de protección de datos personales disponen de poder suficiente para garantizar su efectividad fuera de las fronteras de la UE[51]. Las *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C131/12* –aprobadas el 26 de noviembre de 2014 por parte del Grupo Europeo de Autoridades de Protección de Datos (también conocido como Grupo del artículo 29)- inciden también en la necesidad de que el alcance de los efectos del ejercicio del derecho al olvido no se circunscribieran al ámbito europeo, sino que tuvieran un alcance global[52]. Sin embargo, no faltan autores que consideran que la aplicación territorial global de la sentencia Google Spain podría generar "no pocos problemas" como una afectación "al propio diseño constitucional de los derechos fundamentales en cada país"[53]

[51] Calvão, Filipa Urbano. "A proteção...", *op. cit.*, pág. 72, 82 y 83. A pesar de las limitaciones a la hora de ejecutar la Sentencia, la autora considera que la adopción de decisiones judiciales de este tenor resulta verdaderamente útil pues los responsables de los tratamientos de datos procuran ajustar las condiciones en que los llevan a cabo a los parámetros marcados por las mismas. Preocupación similar cabe apreciar en Marques, João, "Direito ao esquecimento. A aplicação do Acórdão Google pela CNP", *Revista Forum de Protecçao de dados*, nº 3 julho, 2016, pág. 55, https://www.cnpd.pt/bin/revistaforum/forum2016_3/index.html#1/z (consultado el 3/04/2017).

[52] "In order to give full effect to the data subject's rights as defined in the Court's ruling, delisting decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com", de acuerdo con las "Guidelines on the implementation of the Court of Justice of the European Union judgment on «Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González»", Sumario, punto 7, pág. 3, y texto punto 20, págs. 8 y 9. Disponible en http://www.dataprotection.ro/servlet/ViewDocument?id=1080 (consultado el 18/01/2017).

[53] Es el caso, por ejemplo, de Piñar Mañas, José Luis, "Prólogo" en Álvarez Caro, María, *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, Reus, 2015, pág. 10. También Sarrión Esteve, Joaquín "Tras la larga sombra de Google Spain. De nuevo sobre el alcance territorial del derecho al olvido", disponible en https://deje.ua.es/es/derecho-administrativo/documentos/comunicaciones/tras-la-larga-sobra-de-google-spain-de-nuevo-sobre-el-alcance-territorial-del-derecho-al-olvido.pdf (consultado el 18/01/2017).
Especialmente crítico se muestra Gállego Higueras, Gonzalo F. "Dudas sobre el ámbito territorial de aplicación de las disposiciones sobre protección de datos tras la sentencia del Tribunal de Justicia de la Unión Europea en el caso Google vs AEPD & Costeja", *Diario La Ley*, Nº 8401, Sección Tribuna, 17 de Octubre de 2014, (LA LEY 7134/2014). Según este autor, la interpretación realizada por el TJUE supone aplicar en sentido inverso "la «relación de accesoriedad» entre «actividades del establecimiento» (actividad principal) y «tratamiento de datos» (actividad accesoria)" prevista en el art. 4.1 a) de la Directiva.

e informes, como el Informe del Comité de Asesores de Google, de 6 de febrero de 2015, que recomiendan que los efectos del derecho al olvido en relación a la cuestión territorial tengan una eficacia a nivel de la Unión Europea, si bien es verdad que no hay unanimidad entre todos los miembros de dicho Comité (Sabine Leutheusser-Schnarrenberger, concretamente, discrepa)[54]. Davara Rodríguez, por su parte, se congratula por la STJUE, la cual constituye un paso muy importante para ordenar y centrar el derecho al olvido en Internet;

Efectivamente, conforme a lo establecido en dicho precepto, "el tratamiento que se realice en el marco de las actividades de un establecimiento del responsable queda sujeto a la normativa de protección de datos del Estado Miembro donde se ubique el establecimiento: es decir, existen unas actividades que conforman un marco dentro del cual se realiza el tratamiento o, si se quiere, el tratamiento se realiza para las actividades". Ahora bien, el escenario analizado en la sentencia y al que se aplica el mencionado precepto, es justamente el contrario: "existe, por un lado, un servicio de búsqueda que presta Google Inc. que, según el TJUE, implica la realización por ésta (no por Google Spain) de tratamientos de datos personales y, por otro, unas actividades de gestión publicitaria que desempeña Google Spain, S.L. (que no implican tratamientos de datos, según consta acreditado) que, aparentemente, son necesarias para el sustento del buscador (que basa sus ingresos en publicidad, principalmente). En este caso, el tratamiento de datos no se realiza para que se lleven a cabo las actividades del establecimiento (el tratamiento no es accesorio a la actividad). La situación es, precisamente, la inversa: las actividades del establecimiento se llevan a cabo para que el servicio de búsquedas (y su tratamiento de datos) tenga lugar. El buscador y su tratamiento de datos preexisten a Google Spain, S.L., y sus actividades de gestión publicitaria, siendo tal servicio y tratamiento los que «crean el marco» dentro del cual se llevan a cabo tales actividades. En resumen, Google, Inc, presta un servicio de búsquedas que (en su caso) comporta un tratamiento para el que se llevan a cabo las actividades del establecimiento en España". Desde su punto de vista, esta "«novedosa» interpretación del art. 4.1 a) de la Directiva supone una enorme ampliación del ámbito territorial de aplicación de las normas de protección de datos y genera problemas prácticos de difícil (o imposible) solución". Uno de esos problemas (que la STJUE no aclara) reside en determinar quién tiene que cumplir, a nivel material, con las obligaciones de tratamiento de datos que impone el Estado Miembro en que se encuentra ubicado el establecimiento: ¿el que lleva a cabo el tratamiento o el establecimiento? Si nos decantamos por la primera opción, la aplicación de la doctrina del TJUE implica vulnerar el mercado interior y el principio de libre circulación de datos cuando el tratamiento de datos se realiza en otro Estado miembro; y no cabe entender que sólo se aplica cuando el tratamiento se realiza en un Estado extracomunitario pues tal posibilidad no encuentra soporte en la normativa. Si optamos por la segunda posibilidad, nos encontramos con que el establecimiento no está en situación de cumplir, pues no tiene capacidad real de intervenir directa o indirectamente en el tratamiento de los datos.

[54] "The Advisory Council to Google on the Right to be Forgotten", disponible en https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view (consultado el 18/01/2017). En las pág. 18-20, se defiende que Google ha optado por implementar la supresión a nivel de la Unión en base fundamentalmente a los argumentos que siguen: 1) quienes utilizan google.com son, por lo general, redirigidos al dominio local por el servidor de Google, y más del 95% de búsquedas generadas en Europea se hacen a través de dominios locales; dotar a la supresión de un alcance europeo garantiza, por consiguiente, como regla general, la protección de los derechos de los afectados; 2) ciertamente, atribuir un alcance global a la supresión garantizaría una más absoluta protección a los derechos de protección de datos pero existen otros intereses en juego: ej. el derecho de los usuarios fuera de Europa a acceder a esa información conforme a las leyes de su país; el derecho de los usuarios europeos de acceder a versiones de búsqueda fuera de los dominios europeos... La opinión particular de Sabine Leutheusser-Schnarrenberger puede verse en las pág, 26 y 27.

mas advierte que esto no cubre, por ejemplo, "el olvido cuando una persona tenga el acceso directo a la URL sin necesidad de utilizar un buscador" y que pueden darse muchas otras combinaciones pues, aunque Google (en este caso) no permita el enlace, la información sigue estando en la Red; cuestión distinta es que se complique el acceso a la misma y, por ende, su conocimiento[55].

Más críticos con la sentencia se muestran otros autores que afirman que la misma ha venido a "modificar el actual *status quo* en internet: los buscadores de información se ven obligados a dejar de ser instrumentos «neutros» de exploración de la red, al quedar obligados a introducir valoraciones propias aplicando los criterios de relevancia pública y oportunidad de la información que encuentren"[56]. En este sentido, en la doctrina portuguesa, ha sido calificada como "perturbadora" por CASIMIRO, quien afirma que, con esta sentencia, "o Tribunal de Justiça da União Europeia (...) veio perturbar o delicado ecosistema dos prestadores intermediários de serviços em rede, questionando o seu posicionamento perante os conteúdos de terceiros". Tras analizar la actividad desarrollada por los motores de búsqueda, esta autora viene a decir que no es razonable considerarles automáticamente responsables por el tenor de los contenidos de terceros que ellos tratan: "os motores de busca não têm conhecimento desse teor, não têm que ter conhecimento desse teor e, por regra, não querem ter conhecimento desse teor"; y, si bien reconoce que la Directiva no distingue el contexto en que se realiza el tratamiento de datos personales por lo que cabe entender que la actividad desarrollada por los motores de búsqueda supone un tratamiento de datos personales, entiende que dicha solución presenta diversos problemas e invita al legislador a excluir estas situaciones del tratamiento de datos o, por lo menos –a fin de preservar la integridad de dicho concepto- del ámbito de aplicación de la Directiva[57]. Pero

[55] DAVARA RODRÍGUEZ, Miguel Ángel, "El Derecho al Olvido en Internet", *El Consultor de los Ayuntamientos y de los Juzgados*, Nº 13, Sección Nuevas tecnologías, Quincena del 15 al 29 Jul. 2014, (LA LEY 4523/2014). Precisa el autor que "Google avisará de los enlaces retirados por el derecho al olvido a través de una alerta al final de cada página".

[56] BOTANA, Gema Alejandra y OVEJERO PUENTE, Ana Mª "Claves de la sentencia...", *op. cit.*. También BOTANA GARCÍA, Gema Alejandra "Comentario a la Sentencia...", *op. cit.* donde, retomando la opinión de MARTÍNEZ, Ricard, «Olvidar es un fenómeno muy complejo», consultado el 22 de mayo de 2014 en http://lopdyseguridad.es/olvidar-es-un-fenomeno-muy-complejo, afirma "aunque sea a contracorriente, tenemos bastante poco que celebrar y mucho en lo que pensar".

[57] CASIMIRO, Sofia de Vasconcelos, "O direito a ser esquecido pelos motores de busca: o acórdão Costeja", *Revista de Direito Intelectual*, nº 2, 2014, pág. 307, 310, 313, 314, 318. Desde su punto de vista, si no se produce esa exclusión, se producen algunas disfunciones que explica en las pág. 314-318. Para empezar, considera que los motores de búsqueda cumplen una función meramente instrumental: "o manuseamento dos dados pessoais efectuado através dos motores de busca não desvia esses dados para finalidades distintas daquelas para os quais esses dados foram disponibilizados. Os conteúdos forma originariamente colocados em rede para prosseguir determinadas finalidades e os motores de busca limitam-se a permitir a sua melhor

la autora va más allá: el desarrollo de la Sociedad de la Información pasa necesariamente por la creación de las condiciones necesarias para que la información fluya libremente por sus venas, con velocidad y eficiencia. Es esencial que la información correcta llegue al lugar adecuado en el momento oportuno y, para que ello sea así, es preciso estimular la actividad de los intermediarios y desarrollar herramientas que permitan optimizar la información, incluyendo la mejora de su circulación y localización; en este marco, el TJUE debería haber tomado en consideración el régimen de responsabilidad de los prestadores de servicios que facilitan enlaces a contenidos o instrumentos de búsqueda, a fin de garantizar la coherencia del régimen[58]. Para terminar, apela a la desvalorización de la libertad

localização em rede para assim melhor prosseguirem aquelas finalidades". Y, para continuar, señala que la consideración de los motores de búsqueda como responsable comporta una serie de obligaciones ante las autoridades protección de datos y ante los titulares de los datos cuyo cumplimiento, en el caso que nos ocupa, se revela, si no imposible, muy difícil. Recuerda, a estos efectos, que el TJUE entiende que el tratamiento de datos que llevan a cabo los motores de búsqueda queda comprendido en el supuesto del art. 7 f) Directiva (licitud del tratamiento, sin necesidad del consentimiento del interesado, cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento). Ahora bien, esa dispensa del consentimiento del interesado sólo puede operar en relación a los datos personales comunes; la solución ofrecida por el TJUE, por tanto, no sirve cuando los datos incluidos en las páginas de terceros son datos especialmente protegidos ("dados pessoais sensíveis"). Las condiciones en que han de tratarse estos últimos se expresan en el art. 8 Directiva: por regla general, o se prohíbe o se sujeta a una serie de limitaciones. Teniendo presente lo dispuesto en el art. 6.1 e) Directiva, sostiene que los motores de búsqueda también tendrán problemas para determinar el período de tiempo en que pueden efectuar el tratamiento. A la vista de los derechos que la Directiva reconoce a los interesados (información, acceso, rectificación, eliminación y oposición), se pregunta cómo podrá ejercerse en la práctica el derecho al olvido, cómo podrá el operador del motor de búsqueda determinar si la página de origen contiene informaciones incompletas o inexactas, si se cumplen o no las normas sobre el tratamiento de los datos o si existe un interés legítimo del titular de los datos que justifica la eliminación de los mismos.

[58] *Ibídem*, pág. 318. En las pág. 320-322- acude a la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) y a las normas en virtud de las cuales se traspone en España y Portugal. Y ello, porque de dicha normativa se infiere que los motores de búsqueda no son responsables de los contenidos a que dirigen a los destinatarios de sus servicios –contenidos facilitados por terceros-, a menos que tengan conocimiento efectivo de que la información a que remiten es ilícita y no haga nada para eliminar o bloquear los enlaces correspondientes.

El art. 17 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico –relativo a la "Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda"- determina que:

1. *"Los 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 de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:*

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

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

de expresión y del derecho a la información (tantas veces invocado en el ámbito de las redes informáticas) que debería haber sido tenida en cuenta por el TJUE[59].

2.6. Primeras consecuencias de la STJUE

2.6.1. Reacción de Google, la Comisión europea y las autoridades europeas de protección de datos

Apenas dos semanas después del fallo del TJUE, Google ponía a disposición de los ciudadanos, en su web, un formulario para que pudieran solicitar la

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos".

El Decreto-lei 7/2004, de 7 de janeiro, en su art. 17 -relativo a *"Responsabilidade dos prestadores intermediários de serviços de associação de conteúdos"*- remite al art. 16, que, en relación a los servicios de almacenamiento, por su parte, determina:

1 *"O prestador intermediário do serviço de armazenagem em servidor só é responsável, nos termos comuns, pela informação que armazena se tiver conhecimento de actividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação.*

2 *Há responsabilidade civil sempre que, perante as circunstâncias que conhece, o prestador do serviço tenha ou deva ter consciência do carácter ilícito da informação.*

3 *Aplicam-se as regras comuns de responsabilidade sempre que o destinatário do serviço actuar subordinado ao prestador ou for por ele controlado".*

Pues bien, teniendo esto presente, la autora considera inaceptable la STJUE por cuanto supone exigir más a los motores de búsqueda cuando los contenidos son lícitos que cuando son ilícitos: les exige que realicen una ponderación de los intereses en juego, arrogándose el papel de juez y policía, decidan y ejecuten su decisión. A nuestro modo de ver, esa ponderación responde precisamente al hecho de que el tratamiento, en principio, es lícito; si fuera ilícito, no habría que ponderar otros intereses en juego.

[59] Ibídem, pág. 323. Afirmaciones de este cariz, sin embargo, resultan excesivas para CALVÃO, Filipa Urbano. "A proteção...", *op. cit.*, pág. 78 y 79, pues hay que tener presente que el TJUE considera que la obligación del motor de búsqueda es independiente de la que corresponde al editor del sitio de Internet; la información podría seguir estando disponible en el lugar de origen, lo que ocurre es que se dificulta el acceso a la misma de modo que no pueda buscarse directamente a través del nombre de los interesados; la búsqueda podrá realizarse a partir de otros términos. Aunque se entienda que hay una pequeña restricción del derecho de acceso a la información, la misma está justificada por la salvaguarda de otros derechos fundamentales y resulta adecuada, necesaria y no excesiva. Tampoco puede prevalecer el argumento de que Internet se creó como un espacio de libertad, un espacio de libre circulación de información, pues las libertades no son valores absolutos. Como indica la autora, Internet es un espacio de comunicación y de circulación de la información que no implica renunciar a los derechos fundamentales; lo que hay que hacer es encontrar un punto de equilibrio.

retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea[60] y anunciaba la creación de un comité de expertos para valorar su procedencia caso por caso.

Google daba, así, un primer paso muy importante; sin embargo, no se consideraba suficiente. Enseguida se alzaron voces indicando que era preciso "depurar el procedimiento"; en este sentido, el abogado Víctor Salgado afirmaba que la herramienta, aparentemente, no cumplía exactamente con el contenido de la sentencia al eludir referencias legales al derecho de oposición o cancelación al que se refería y eso abría la puerta a la posibilidad de que Google pudiera incumplir el plazo límite de respuesta de diez días que exige al menos la legislación española en protección de datos[61].

Según los datos publicados por Google en octubre de 2014, desde la apertura de las solicitudes el 29 de mayo habían recibido 142.000 peticiones relacionadas con 490.000 páginas web. Las páginas más frecuentes eran Facebook, Badoo, Google Groups, Twitter y Youtube[62].

[60] GOOGLE: "Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea" https://support.google.com/legal/contact/lr_eudpa?product=websearch (último acceso 16/01/2017).

[61] "El formulario de Google para borrar datos «no cumple exactamente» con la sentencia" en: http://www.20minutos.es/noticia/2154650/0/formulario-google/borrar-datos/paso-buen-camino/#xtor=AD-15&xts=467263#xtor=AD-15&xts=467263 (consultado el 12/05/215).

Hoy por hoy, en el formulario web de Google, el usuario debe reflejar su nombre completo (incluso cuando solicite la retirada de los resultados en nombre de otra persona, en cuyo caso deberá indicar también la relación que tiene con la persona a la que representa), una dirección de correo electrónico, el país cuya legislación se aplica a su solicitud, el nombre utilizado para realizar las búsquedas y las URL del enlace o enlaces que figuran tras una búsqueda en Google con su nombre cuya retirada se solicita, indicando los motivos por los que dicha/s página/s se refiere/n a la persona en cuestión y las razones por las que el usuario considera que el contenido de la página enlazada carece de relevancia, no es pertinente —o ya no lo es— o es obsoleto. A fin de verificar la identidad del usuario, Google exige, además, que se adjunte un documento válido de identificación con foto. La referencia al plazo para resolver sigue sin aparecer.

En Portugal, a la vista de lo previsto en el art. 23 Lei 67/98, la fijación del plazo máximo para cumplir con los deberes impuestos a los responsables del tratamiento de datos en los art. 11 a 13 corresponde a la CNPD. La doctrina de nuestro país vecino, por otra parte, hace hincapié en que las restricciones a que se encuentra sujeto el tratamiento de datos sensibles (datos especialmente protegidos) como los relativos a la vida privada (art. 7 lei 67/98 y 35.3 CRP) determinarán la aceptación prácticamente inmediata de las solicitudes de disociación relativas a la vida privada del titular de los datos pues, por término general, no existirá fundamento alguno que justifique el tratamiento de tales datos por parte del motor de búsqueda (art. 7.2 lei 37/98); así lo pone de relieve MARQUES, João, "Direito ao esquecimento...", *op. cit.*, pág. 53 y 54, quien añade que a ello hay que sumar la no necesidad de alegar un perjuicio.

[62] "Derecho al olvido: Google difunde cifras sobre los pedidos" en https://nostroviarrii.wordpress.com/2014/10/15/derecho-al-olvido-google-difunde-las-cifras/ (consultado el 12/05/2015).

Google creó, además, un Consejo Asesor que le auxiliara en la toma de decisiones relacionadas con las peticiones de retirada de resultados recibidas en los que se incluía el nombre del interesado[63].

La Comisión europea, por su parte, divulgó diversos documentos con información relativa al alcance de la STJUE[64] y el Grupo de Trabajo del art. 29 aprobó el 26 de noviembre de 2014 unos criterios interpretativos comunes que presidirían la aplicación de la sentencia por parte de las Autoridades de los Estados europeos[65]. A los pocos meses, el vicepresidente de la Comisión europea -Andrus Ansip-, en una entrevista publicada el 12 abril de 2015, aseguraba que era "fundamental modernizar las normas de protección de datos en Europa y establecer una serie de nuevos derechos para los ciudadanos"; el derecho al olvido quedaría enmarcado en un mercado único en el que los datos serían "sometidos a la racionalización de la cooperación entre reguladores de los Estados"; la reforma que se precisaba –explicaba- no pasaba por reconocer simplemente el derecho al olvido sino que era mucho más profunda[66]. Esa modernización ha venido de la mano del RGPD, al que nos referiremos más adelante.

[63] Las conclusiones del Consejo de 6 de febrero de 2015 pueden verse en "The Advisory Council to Google on the Right to be Forgotten", disponible en https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view (consultado el 18/01/2017).

[64] "Factsheet on the «Right to be forgotten» ruling", disponible en http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (consultado el 18/01/2017) y "Myth-Busting. The Court of Justice of the UE and the «Right to be Forgotten», disponible en http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_en.pdf (consultado el 18/01/2017).

[65] "Guidelines on the implementation of the Court of Justice of the European Union judgment on «Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González»", disponible en http://www.dataprotection.ro/servlet/ViewDocument?id=1080 (consultado el 18/01/2017).

[66] Entrevista al vicepresidente de la comisión europea Andrus Ansip: "Los europeos podrían ahorrar 11.700 millones cada año con el Mercado Único Digital" en http://vozpopuli.com/economia-y-finanzas/60482-andrus-ansip-los-europeos-podrian-ahorrar-11-700-millones-cada-ano-con-el-mercado-unico-digital (consultado el 12/05/2015).
Del otro lado del océano, sin embargo, el derecho al olvido no despierta muchas simpatías; acaso porque, como indicaba Soriano García, José Eugenio, "Derecho al olvido y la creación de derechos", *Galileu -Revista de Economia e Direito-*, vol. BVII, nº1/nº2, 2012, pág. 210, antes de que se pronunciara el TJUE, en EEUU prima más la incorporación de los datos al mercado de búsquedas no solo por "la insobornable libertad de expresión e información", sino también por el "libre mercado". Tras la STJUE, BROWN, Peter "The Right to be forgoten: US Rulings on Free Speech W'ont Let Google Forge", *Computer Law Review International*, Issue 6, 15 Decembre, 2014, pág. 161-166, insiste en la idea de que el derecho al olvido es contrario a las leyes y valores de EEUU.

2.6.2. Aplicación de la doctrina del TJUE por los órganos jurisdiccionales de los Estados miembros. El caso de España, en particular.

Las consecuencias tampoco se hicieron esperar en el ámbito jurisprudencial. En España, la Audiencia Nacional (AN) acogió los razonamientos del TJUE en un sinfín de Sentencias, entre las que vamos a destacar las Sentencias de la sección 1ª de la AN de 29 de diciembre de 2014 dictadas en los recursos 781/2009, (Roj: SAN 5217/2014) y 69/2012 (Roj: SAN 5254/2014), 30 de diciembre de 2014 en el recurso 503/2012 (Roj: SAN 5239/2014) y 12 de Febrero de 2015 en el recurso 24/2013, (Roj: SAN 626/2015)[67].

El problema, sin embargo, no estaba resuelto: ¿Quién debía gestionar ese "derecho al olvido"? Apenas veintidós meses después de que se dictara la STJUE, el TS español (Sala de lo Contencioso-administrativo) dictaba cuatro sentencias [SSTS de 11 de marzo de 2016 (Roj: STS 1055/2016), 14 de marzo de 2016 (Roj: STS 1056/2016), nº 574/2016, de 14 de marzo de 2016 (Roj: STS 964/2016)[68],

[67] La aplicación de la doctrina del TJUE por parte de la AN determinó que Google desistiera en 136 casos en que había recurrido la decisión de la AEPD ante la AN, dejando vivos únicamente aquellos en los que tenía posibilidades. Según las afirmaciones del director de la AEPD de las que se hace eco "La Audiencia Nacional aplica la doctrina del TJUE y fija los criterios del «derecho al olvido»", *Diario La Ley*, Nº 8492, Sección Tribuna, 3 de Marzo de 2015, (LA LEY 1377/2015), se confirmaron las resoluciones de la AEPD en 150 casos y sólo se corrigió su interpretación en 4 casos.

[68] El supuesto que da origen a esta sentencia difiere del correspondiente al litigio que motivó la resolución europea, pues la reclamación inicial del afectado por el tratamiento de sus datos personales, en el presente caso, no tiene por objeto la eliminación de referencias a enlaces en los índices de resultados del buscador a publicaciones realizadas en páginas web de terceros alojadas en servidores de esos terceros, sino que se refiere a la eliminación de los datos personales del reclamante contenidos en un blog de la plataforma Blogger, alojado en el espacio de almacenamiento que Google proporciona de forma gratuita; dicha petición se dirige, además, única y exclusivamente contra Google Spain. Pues bien, a pesar de que de la reclamación presentada ante la AEPD no se infería que el afectado interesaba también la eliminación de las referencias al blog en cuestión en la lista de resultados del buscador facilitada cuando se introducía su nombre en el motor de búsqueda, la AN consideró que dicha medida era la que procedía una vez ponderados los intereses en liza cuando no era posible sancionar al buscador con la eliminación de los datos en cuestión. Aducía la AN que "Google Spain no es responsable de los contenidos del blog, sino que es una plataforma, alojador de contenidos, un intermediario entre el editor del blog y los usuarios"; por ello, se planteaba hasta qué punto se le podía imponer la obligación de eliminar el contenido en el marco de un procedimiento de tutela de derechos, contemplado en la LOPD. Teniendo en cuenta que la AEPD había tramitado el expediente sin oír al titular del blog y no habiendo quedado acreditado que Google fuera el responsable del fichero que integraba el blog en el que constaba la información y los datos a los que se refería el denunciante, entendía que no se le podía exigir que eliminara los datos personales del reclamante del blog sino únicamente la no indexación de los mismos. El TS, por su parte, no se para a analizar si la petición debería haberse dirigido frente al titular del blog y acoge el argumento esgrimido por Google Spain relativo a la falta de responsabilidad de la filial por cuanto es la matriz estadounidense la que determina los fines y medios del tratamiento de datos que se lleva a cabo en la plataforma Bloger. En su opinión, lo que caracteriza la condición de responsable es la determinación de los fines y medios

15 de marzo de 2016 (Roj: STS 1103/201)] en las que declaraba la nulidad de las decisiones de la Agencia Española de Protección de Datos (AEPD) y las resolu-

del tratamiento, no cualquier otro tipo de colaboración como la promoción de servicios publicitarios. Argumenta también que no cabe aplicar la doctrina de los actos propios pues, aunque efectivamente Google Spain ha sido condenada como responsable en otros litigios y cumplido su condena, ello no puede extenderse a procedimientos administrativos y judiciales distintos.
Sobre esta sentencia puede verse: MAYOR GOMEZ, Roberto, "Comentarios a la Sentencia nº 574/2016 de la Sala de lo Contencioso Administrativo del Tribunal Supremo (sección sexta) de 14 de marzo de 2016: falta de legitimación pasiva de Google Spain S.L en procedimiento de tutela de derechos al no ser responsable del tratamiento de datos personales", *GABILEX*, Revista del Gabinete Jurídico de Castilla-La Mancha, Nº 5, marzo 2016, en http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160418/comentarios_a_la_sentencia_no_574-2016_roberto_mayor.pdf (consultado el 18/01/2017); DI PIZZO CHIACCHIO, Adrián, "Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso «Google Spain». La interpretación de la responsabilidad de los gestores de motores de búsqueda en la implementación del derecho al olvido digital", *Revista jurídica de Catalunya*, Vol. 115, 2016, Nº 4, pág. 952-957; MINERO ALEJANDRE, Gemma, "Tratamiento de datos de carácter personal en Internet. Blogs alojados en espacio de almacenamiento de Google. Concepto de responsable. Comentario a la STS de 14 de marzo de 2016 (RJ 2016, 1525)", *CCJC*, nº 102, Septiembre-Diciembre 2016, pág. 345-394. En opinión de esta última autora, si se mantiene esta interpretación por parte del Alto Tribunal "el Estado español se expone a un potencial recurso por incumplimiento del Derecho de la Unión. Recurso que será menos probable en tanto la aplicación de la interpretación del concepto de responsable contenida en el pronunciamiento del Tribunal Supremo se restrinja a supuestos de publicación de informaciones o comentarios en blogs alojados en espacio de almacenamiento de Google y a reclamaciones que busquen su completa eliminación, y no se extienda a todo supuesto originado por reclamaciones de eliminación de las referencias a blogs o páginas web en las listas de resultados del buscador". Consciente de que es preciso diferenciar las funciones que presta Google en sus servicios relacionados con el tratamiento de datos de carácter personal –el buscador y el alojamiento de contenidos de blogs en la plataforma Blogger- sostiene que, aunque el TJUE no se haya pronunciado aún en relación a la responsabilidad de Google con respecto al tratamiento de datos por publicaciones de blogs almacenados en la referida plataforma, "parece acertado extender a estos supuestos la potencial condena a Google para la eliminación de referencias en su lista de resultados". Asimismo estima procedente oír al titular del blog en el que se inserte la publicación litigiosa (con base en lo dispuesto en el art. 117 RD 1720/2007), "pues la condena a Google para la eliminación de esas informaciones en ausencia del trámite de audiencia del titular del blog podría afectar al correcto ejercicio de ponderación entre el derecho a la protección de datos personales del sujeto al que se refiere la publicación y el derecho a la libertad de expresión, así como, en su caso, el derecho a la tutela judicial efectiva del titular del blog". Ahora bien, desde su punto de vista, esa diferenciación de las funciones que desempeña Google no conduce inexorablemente a la conclusión de que Google Spain será responsable del tratamiento de los datos personales cuando la reclamación del interesado se limite a solicitar la eliminación de las referencias en los índices de resultados del buscador pero no cuando se solicite también la eliminación de los datos contenidos en el blog de la plataforma. Dado que esta segunda petición debería rechazarse cuando no se dirigiera contra el titular del blog en cuestión, -continúa argumentando- defender en todo caso que Google Spain carece de toda responsabilidad y que la reclamación en conjunto debe tener como único destinatario Google Inc supone realizar una distinción en relación al primer punto del petitum –esto es, la condena a la modificación de los resultados de búsqueda del buscador-, cuando el TJUE, en relación a este servicio de Google, "exige la aplicación de una interpretación funcional del concepto de responsabilidad del tratamiento, que incluye las filiales nacionales dedicas a la comercialización de espacios publicitarios". Por ello, defiende que "la responsabilidad de Google Spain en caso de condena

ciones de la Audiencia Nacional que acabamos de citar, aduciendo que habían sido dictadas en un procedimiento dirigido contra Google Spain S.L., la cual no era responsable del tratamiento de datos y, por consiguiente, no estaba sujeta al cumplimiento de las obligaciones declaradas en tales resoluciones.

A la vista de estas sentencias, la AEPD publicó una nota informativa (15/03/2016) recordando que la forma en que los ciudadanos pueden ejercer el derecho al olvido frente a Google se mantiene intacta. "Los usuarios –dice textualmente la Agencia- pueden seguir dirigiéndose a Google para ello, por ejemplo, a través del formulario que la compañía mantiene habilitado en español desde el 30 de mayo de 2014. Del mismo modo, si Google deniega la solicitud del interesado o éste no estuviera conforme con la decisión de la compañía, podrá seguir solicitando la tutela de la Agencia en los mismos términos en que podía hacerlo hasta ahora". La AEPD subraya que la sentencia "no supone que los interesados no puedan ejercer sus derechos conforme a lo previsto en la LOPD ni que deje de aplicarse la Ley española. Tampoco modifica los principios y criterios de ponderación que estableció el TJUE en su sentencia, sino que aclara que el destinatario de las solicitudes deberá ser Google Inc.". Termina aconsejando a los ciudadanos afectados directamente que, en primer lugar, comprueben si Google ha indexado los enlaces de nuevo. En caso afirmativo, deben solicitar el derecho al olvido a través del formulario habilitado. "Si la entidad no responde a la petición realizada o el ciudadano considera que la respuesta que recibe no es la adecuada, puede seguir solicitando la tutela de la AEPD frente a Google"[69].

Poco después, el 5 de abril de 2016, la Sala Primera de lo civil del TS dictaba sentencia (Roj: STS 1280/2016) en relación a un supuesto de tutela del derecho al honor, a la intimidad, a la propia imagen y a la protección de datos de carácter personal, que se refería a la responsabilidad de Google Spain S.L. en el tratamiento de tales datos y la incidencia que, para el ejercicio por el interesado del derecho a la tutela judicial efectiva, puede tener la consideración como responsable de

a la eliminación de las referencias al blog en su lista de resultados no puede quedar afectada (en otras palabras, no puede quedar en manos únicamente de Google Inc y defender que las reclamaciones deben tener por único destinatario la empresa estadounidense) cuando la reclamación del interesado pretenda también (o pretenda de manera exclusiva) la eliminación de sus datos personales contenidos en el blog o la inserción en éste de medidas que impidan la indexación por buscadores, e incluso cuando yerre en la identificación del sujeto frente al que ejercitar sus derechos de oposición y cancelación".

[69] "Nota informativa de la Agencia Española de Protección de datos de 15/03/2016" en https://www.agpd.es/portalwebAGPD/noticias-inicio/news/2016_03_15-ides-idphp.php (consultado el 16/01/20017).

Google Inc., con domicilio en otro país[70/71]. Dicha sentencia no incorporaba, en lo sustancial, una motivación diferente a la valorada por la Sala de lo Contencioso al resolver los recursos de casación interpuestos contra las sentencias de la AN en las sentencias anteriormente referidas, pero modifica el criterio haciendo referencia a la falta de efecto perjudicial de las sentencias dictadas por ambas salas y recordando la existencia de "distintos criterios rectores en las distintas jurisdicciones, por la diversidad de las normativas que con carácter principal se aplican en unas y otras"[72]. El responsable es Google Spain[73].

Conociendo la Sentencia dictada por la Sala de lo Civil, la Sala de lo Contencioso-Administrativo del Tribunal Supremo, en Sentencias de 13 de junio de 2016[74], 20 de junio de 2016[75], 27 de junio de 2016[76], 04 de julio de 2016[77] 11 de

[70] El supuesto de hecho puede resumirse así. En 1999, el BOE había publicado el RD por el que se indultaba al demandante la pena privativa de libertad pendiente de cumplimiento, a la que había sido condenado como autor de un delito contra la salud pública, por hechos cometidos en 1981. En enero de 2009, el demandante se dirigió al BOE, para solicitar la retirada de sus datos, por cuanto el mantenimiento de dicha publicación le ocasionaba importantes perjuicios. El BOE adoptó las medidas a su alcance necesarias para evitar al automatización de los datos del demandante, haciendo imposible acceder a la noticia en el buscador de la página web del BOE a partir del nombre del demandante e incluyendo los documentos en que aparecía el nombre del demandante en una lista de exclusión, mediante robots.txt, a fin de evitar su futura indexación por los buscadores genéricos (ej. Google o Yahoo). Se dirigió también a Google, para solicitar la no indexación de la publicación del indulto en el BOE y reclamar el pago de la indemnización de los daños producidos por el mantenimiento durante años de la citada noticia en la primera página de resultados del buscador en búsquedas realizadas a partir del nombre del demandante, mas su pretensión no tuvo éxito. Lo mismo hizo frente a Yahoo, empresa que le pidió (para poder ayudarle adecuadamente) que determinase el link exacto en el que se hallaban los resultados. No consta ninguna otra comunicación al respecto. En abril de 2009 el demandante presenta la correspondiente reclamación en la AEPD que dirige contra BOE, Google Spain y Yahoo.

[71] Afirma textualmente: "Los sujetos protegidos por la normativa sobre protección de datos son las personas físicas (art. 1 y 2.a de la Directiva). El efecto útil de la normativa comunitaria se debilitaría enormemente si los afectados hubieran de averiguar, dentro del grupo empresarial titular de un motor de búsqueda, cuál es la función concreta de cada una de las sociedades que lo componen, lo que, en ocasiones, constituye incluso un secreto empresarial y, en todo caso, no es un dato accesible al público en general. También se debilitaría el efecto útil de la Directiva si se diera trascendencia, en el sentido que pretende la recurrente Google Spain, a la personificación jurídica que el responsable del tratamiento de datos diera a sus establecimientos en los distintos Estados miembros, obligando de este modo a los afectados a litigar contra sociedades situadas en un país extranjero. Incluso en el caso de litigar en España, la inmensa mayoría de las personas tendría enormes dificultades prácticas para interponer la demanda de protección de sus derechos fundamentales contra una sociedad domiciliada en Estados Unidos y obtener la tutela judicial efectiva de sus derechos en un plazo razonable, tanto por el elevado coste que supone la traducción al inglés de la demanda y la documentación que le acompaña, como por la dilación que implicaría la inevitable tardanza en el emplazamiento de dicha sociedad, al tener que acudir a los instrumentos de auxilio judicial internacional, con lo que se prolongaría la situación de vulneración de sus derechos fundamentales. Y, sobre todo, en caso de obtener una sentencia condenatoria, si la demandada no le diera cumplimiento voluntariamente, el ciudadano afectado debería solicitar el reconocimiento y la ejecución de la sentencia en los Estados Unidos de América, con el coste y las dificultades, tanto de orden teórico como práctico, que ello trae consigo. Por otra parte, dadas las características del servicio que prestan estos motores de búsqueda, la sociedad más directamente relacionada con la determinación de los fines y los medios del tratamiento de datos personales podría ser ubicada en otro Estado con el que no existieran relaciones que permitieran el emplazamiento de la sociedad y el posterior reconocimiento y ejecución de la resolución que se dictara" (esto es, un Estado con el que el nivel de cooperación judicial fuera aún menor).

[72] Las sentencias de la Sala de lo Contencioso Administrativo resuelven en relación a resoluciones dictadas en un procedimiento administrativo seguido ante la AEPD, mientras que la sentencia de 5 de abril de 2016 se dicta en un proceso civil que tiene por objeto la protección de los derechos fundamentales del demandante: concretamente, los derechos al honor, a la intimidad y a la protección frente al tratamiento automatizado de sus datos de carácter personal.

[73] Noemí Brito considera que la solución de la Sala de lo Civil "garantiza una tutela eficaz y completa de las libertades y de los derechos fundamentales y, con ello, aplica la jurisprudencia del Tribunal de Justicia de la Unión Europea, como máximo intérprete del Derecho de la Unión". Y es que, desde su punto de vista, "no resulta lógico dificultar al ciudadano el ejercicio de sus derechos fundamentales a través de dilaciones y costes indebidos e innecesarios en orden a la debida protección y atención de aquéllos". De hecho, añade "ello podría ser contrario a la actual normativa europea que exige que se atienda sin dilación indebida cuando así proceda". Se hace eco de la opinión de esta abogada, BIURRUN ABAD, Fernando, "La determinación del responsable del tratamiento a efecto del derecho al Olvido", *Actualidad Jurídica Aranzadi*, nº 919/2016, (BIB 2016\3124). Sobre esta sentencia se pronuncia también Di Pizzo Chiacchio, Adrián "Efectos...", *op. cit.*, pág. 957-964.

[74] SSTS (Sala de lo Contencioso-Administrativo) de 13 de junio de 2016 nº 1381/2016 (Roj: STS 2722/2016), nº 1382/2016 (Roj: STS 2699/2016), nº 1383/2016 (Roj: STS 2724/2016), nº 1384/2016 (Roj: STS 2723/2016), nº 1385/2016 (Roj: STS 2696/2016), nº 1386/2006 (Roj: STS 2707/2016); nº 1387/2016 (Roj: STS 2725/201), nº 1388/2016 (Roj: STS 2702/2016).

[75] SSTS (Sala de lo Contencioso-Administrativo) de 20 de junio de 2016 nº 1454/2016 (Roj: STS 2845/2016), nº 1455/1960 (Roj: STS 2836/2016), nº 1456/2016 (Roj: STS 2876/2016), nº 1457/2016 (Roj: STS 2850/201), nº 1458/2016 (Roj: STS 2837/2016), nº 1459/2016 (Roj: STS 2842/2016), nº 1460/2016 (Roj: STS 2847/2016).

[76] SSTS (Sala de lo Contencioso-Administrativo) de 27 de junio de 2016 nº 1529/2016 (Roj: STS 3006/2016), nº 1531/2016 (Roj: STS 3000/2016), 1532/2016 (Roj: STS 3048/2016), nº 1533/2016 (Roj: STS 2997/2016), 1534/2016 (Roj: STS 2998/201), nº 1535/2016 (Roj: STS 2996/2016), y nº 1536/2016 (Roj: STS 3005/2016).

[77] SSTS (Sala de lo Contencioso-Administrativo) de 4 de julio de 2016 nº 1610/2016 (Roj: STS 3333/2016), nº 1611/2016 (Roj: STS 3313/201) –la cual constituye la culminación del Caso Costeja- nº 1612/2016 (Roj: STS 3315/201), nº 1613/2016 (Roj: STS 3336/2016), nº 1615/2016 (Roj: STS 36/201/E2) y nº 1618/2016 (Roj: STS 3316/2016).
Formalmente, la referida STS (Sala de lo Contencioso-Administrativo) nº 1611/2016, de 4 de julio de 2016, casa la SAN y anula la RAEPD en lo relativo a la atribución a Google Spain de la condición de corresponsable por el tratamiento de datos efectuado por Google Search en el caso Costeja (motivo por el cual se le imponía la obligación de adoptar las medidas necesarias para hacer efectivo el derecho de oposición ejercitado por el interesado en calidad del responsable del tratamiento de datos), la sentencia; ello, sin embargo, no entraña repercusión material alguna para el afectado (Sr. Costeja), pues la parte dispositiva que impone la obligación de proceder a la desindexación de la noticia relativa a un antiguo embargo de una propiedad no se anula respecto de Google Inc. .La diferencia reside en que la AEPD consideró corresponsable del tratamiento a Google Inc. junto con Google Spain y la Sala Tercera del TS atribuye a Google Inc. la responsabilidad única de dicho tratamiento.

julio de 2016[78], 18 de julio de 2016[79] y 21 de julio de 2016[80] –a las que han seguido otras muchas-, ha vuelto a pronunciarse sobre la Sentencia del TJUE, confirmando el criterio expuesto en sus anteriores Sentencias y poniéndolo en relación con el RGPD, el cual –afirma- viene a confirmar el criterio mantenido por la Sala de lo Contencioso-Administrativo[81]. En las referidas sentencias recuerda que, "en el ámbito de esta jurisdicción contencioso administrativa, la tutela de los derechos de oposición, acceso, rectificación y cancelación reconocidos al titular de los datos personales objeto de tratamiento se recaba mediante la impugnación de la correspondiente resolución de la Agencia Española de Protección de Datos, resolución que se produce (...) a través de un procedimiento que comienza con la reclamación o comunicación dirigida al responsable del tratamiento, ejercitando el correspondiente derecho (art. 25 RD 1720/2007), frente a cuya respuesta el interesado puede formular reclamación ante la referida AEPD (art. 117 RD 1720/2007), que deberá dictar resolución en el plazo de seis meses, contra la cual puede interponerse el recurso contencioso administrativo (art. 18 LOPD 15/1999)". En este ámbito jurisdiccional, la identificación de Google Inc. como responsable del tratamiento al que debe dirigirse el titular de los datos personales en ejercicio de su derecho se justifica en virtud de: 1) la clara definición legal de la condición de responsable establecida tanto en el art. 2 d) la Directiva 95/46/CE como en el art. 3 d) LOPD 15/1999; 2) la interpretación realizada por el TJUE en su sentencia de 13 de mayo de 2014; 3) las resoluciones adoptadas por ocho órganos jurisdiccionales europeos demuestran que el planteamiento de la referida STJUE es objetivamente sostenible[82]; 4) la propia naturaleza de la obligación cuyo cumplimiento se exige por el interesado: se trata de una "obligación de hacer o no hacer impuesta por la ley [art. 12.b) de la Directiva 95/46/CE] en virtud de la efectiva participación del responsable en el tratamiento de datos objeto de impugnación, participación que delimita el alcance de su responsabilidad y la exigencia de la correspondiente reparación, adoptando las medidas precisas al efecto"; este caso, el cumplimiento de la obligación exige la utilización de unos medios sobre los que solo tiene capacidad de disposición el responsable, como gestor del motor de búsqueda; y 5) la asunción por Google Inc. de la condición de responsable como propia, al adoptar medidas tendentes a facilitar el ejercicio del denominadõ "derecho al olvido" a raíz de la sentencia del TJUE.

La Sala de lo Contencioso argumenta, además, que en este ámbito jurisdiccional, la identificación de Google Inc. como responsable del tratamiento no supone para el interesado una dificultad o carga añadida significativa para la obtención de una eficaz tutela judicial, en ninguna de las fases del procedimiento previsto al efecto, por el hecho de que tenga su domicilio en otro país. En su primera fase, el procedimiento es sumamente sencillo y gratuito[83]. Y en la segunda ante la Autoridad de control tampoco presenta mayores complicaciones

[78] SSTS (Sala de lo Contencioso-Administrativo) de 11 de julio de 2016 nº 1689/2016 (Roj: STS 3489/2016), nº 1690/2016 (Roj: STS 3347/2016), nº 1693/2016 (Roj: STS 3359/2016), nº 1694/2016 (Roj: STS 3362/201), nº 1695/2016 (Roj: STS 3361/2016), nº 1696/2016 (Roj: STS 3370/2016); y nº 1697/2016 (Roj: STS 3349/2016).

[79] SSTS (Sala de lo Contencioso-Administrativo) de 18 de julio de 2016 nº 1797/2016 (Roj: STS 3687/2016), nº 1799/2016 (Roj: STS 3676/2016), nº 1800/2016 (Roj: STS 3669/2016), nº 1801/2016 (Roj: STS 3668/2016), nº 1802/2016 (Roj: STS 3667/2016), nº 1803/2016 (Roj: STS 3671/2016), nº 1805/2016 (Roj: STS 3675/2016), nº 1806/2016 (Roj: STS 3690/2016), nº 1807/2016 (Roj: STS 3674/2016), nº 1808/2016 (Roj: STS 3693/2016), nº 1809/2016 (Roj: STS 3860/2016); y 1810/2016 (Roj: STS 3694/2016).

[80] SSTS (Sala de lo Contencioso-Administrativo) de 21 de julio de 2016 nº 1910/2016 (Roj: STS 3727/2016), nº 1911/2016 (Roj: STS 3733/2016), nº 1912/2016 (Roj: STS 3722/2016), nº 1913/2016 (Roj: STS 3725/2016), nº 1915/2016 (Roj: STS 3746/2016), nº 1916/2016 (Roj: STS 3717/2016), nº 1917/2016 (Roj: STS 3721/2016), nº 1918/2016 (Roj: STS 3695/2016), nº 1919/2016 (Roj: STS 3706/2016) y nº 1920/2016 (Roj: STS 3713/2016).

[81] Dado que el RGPD será objeto de análisis expreso más adelante, omitiremos las referencias al mismo al hilo de esta sentencia. No obstante, cabe apuntar que autores como Di Pizzo Chiacchio, Adrián "Efectos...", *op. cit.*, pág. 966, se sorprenden de que, pese a reconocer que el Reglamento comunitario no es aún aplicable, uno de los pilares argumentativos en que se asientan estas resoluciones sea la disposición que introduce la regulación de la corresponsabilidad en el tratamiento de datos personales (art. 26).

[82] Las sentencias citadas por la recurrente son: Audiencia Territorial de Berlín de 21 de agosto de 2014; auto de la Sala de lo Civil nº 2 de la Audiencia Territorial de Hamburgo de 18 de agosto de 2014; providencia de la Audiencia Territorial de Hamburgo de 22 de septiembre de 2014; sentencia del Tribunal de Roma de 4 de noviembre de 2014; sentencia del Tribunal de Amsterdam de 18 de septiembre de 2014 y del Tribunal de Apelación de 31 de marzo de 2015; auto del Tribunal de Gran Instancia de París de 8 de diciembre de 2014; sentencia del Tribunal de Primera Instancia de Arenas de 16 de febrero de 2015; y sentencia del Tribunal Regional de Düsseldorf de 7 de mayo de 2015.

[83] De acuerdo con lo dispuesto en el 24 RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal el interesado puede ejercitar sus derechos de acceso, rectificación oposición y cancelación a través de los servicios de cualquier índole para la atención al público o el ejercicio de reclamaciones relacionadas con el servicio prestado de que disponga el responsable del tratamiento; dicho precepto impone al responsable, además, la obligación de atender la solicitud del interesado aun cuando no hubiera utilizado el procedimiento establecido específicamente al efecto por aquel, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud. Por consiguiente, la reclamación puede realizarse electrónicamente de manera sencilla, gratuita y directa por el interesado; sirve cualquier forma siempre que permita justificar el envío y la recepción por el responsable. En el caso de Google Inc., -afirma el TS- es especialmente sencillo pues Google Inc. "ofrece a los interesados información completa sobre el ejercicio de su derecho, facilita los correspondientes formularios y proporciona instrucciones precisas para cumplimentarlos, habiendo establecido un Consejo Asesor, compuesto por cualificados miembros de distintos países, para evaluar las solicitudes y remitiendo al interesado, caso de desacuerdo con la decisión adoptada, a su impugnación ante la autoridad de protección de datos local, en congruencia con lo dispuesto en el art. 35 del citado RD 1720/2007, que establece genéricamente el plazo de diez días para resolver por el responsable, transcurrido el cual sin resolución, el interesado podrá interponer la reclamación prevista en el art. 18 LO 15/1999 ante la Agencia de Protección de Datos.

porque, como dispone el art. 117 del Reglamento aprobado por RD 1720/2007, para iniciar el procedimiento, basta con presentar la reclamación correspondiente ante la AEPD[84/85].

Otra sentencia importante en el marco del llamado "derecho al olvido digital" es la dictada por la Sala de lo civil del TS, en pleno, de 15 de octubre de 2015, pero a ella nos referiremos más adelante.

Con este panorama jurisprudencial, los problemas prácticos que surgen al hilo de la desindexación de información de los motores de búsqueda distan mucho de quedar resueltos. Veremos qué ocurre en el futuro: ¿Terminará imponiéndose la vía tuitiva ofrecida por el procedimiento jurisdiccional civil o seguirá compaginándose con la vía administrativa y jurisdiccional contencioso administrativo, fomentando la falta de seguridad jurídica en la tutela al derecho al olvido?

2.7. El Reglamento (UE) 2016/679

El 25 de mayo de 2016 entró en vigor el Reglamento (UE 2016/679) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (RGPD)[86]. Aunque no comenzará a aplicarse hasta dos años más tarde, conviene ir analizándolo a fin de detectar las dificultades que puede suscitar su aplicación[87/88].

[84] Trae a colación el TS, a estos efectos: a), la implicación de los intervinientes en el desarrollo de la sociedad de la información y la constante evolución normativa hacia la tramitación de los procedimientos a través de medios electrónicos, que queda patente en el art. 71 de la nueva Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común; b) la gran cantidad de procedimientos tramitados ante la Agencia de Protección de Datos con la intervención de Google Inc.; c) el interesado puede instar y abrir la vía jurisdiccional mediante un simple escrito de impugnación de la resolución adoptada por la Agencia de Protección de Datos, a partir del cual el proceso contencioso-administrativo se impulsa de oficio hasta su terminación en cualquiera de las formas establecidas en la propia Ley reguladora de la Jurisdicción Contencioso-Administrativa

[85] Di Pizzo Chiacchio, Adrián "Efectos...", *op. cit.*, pág. 969 y 970, muestra su desacuerdo con la doctrina del TS indicando que "Google Spain -al igual que el resto de filiales geográficas- incide de manera cuando menos indirecta en la fijación de los medios y fines del tratamiento, por cuanto (...) los espacios de publicidad que la filial española promociona son estratégicamente dispuestos por Google Inc. en las consultas realizadas a través de «www.google.es»"; su responsabilidad no puede excluirse porque ello equivale a decir que no influye de manera alguna en la forma en que se configura el conjunto de operaciones que desarrolla Google Search. lo cual solo puede calificarse como «paradoja jurídica» pues "¿qué, si no la rentabilidad económica, determina «cómo» y «para qué» se emplearán los datos personales indexados por el buscador? (...), ¿cómo puede descartarse que Google Spain no incide mediante la rentabilidad económica de su promoción publicitaria en determinar la manera en que debe hallarse la información, indexarla, máxime almacenarla, y ponerla a disposición de los usuarios?". La distinta naturaleza de la actividad que desarrollan una y otra entidad -concluye- "no obsta a que la primera ayude a determinar, de una manera u otra, las actividades que conforman el tratamiento de datos personales". Tampoco le convencen los argumentos del Alto Tribunal basados en las notas características propias del procedimiento administrativo y del ulterior proceso jurisdiccional; a su modo de ver, viene a "deformar" la exégesis realizada con anterioridad.

[86] El RGPD no viene solo; forma parte del llamado «paquete de protección de datos», que incluye a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Dicha Directiva extiende la regulación de la protección de datos a extremos no contemplados en la anterior Directiva de 1995 o el nuevo Reglamento, cuales son los relativos a los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

[87] El RGPD, como de costumbre, finaliza con la frase: *"El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro"*.

En el caso de Portugal, como pone de relieve LOPES, Joaquim de Seabra, "Oartigo 35º da Constituição: dagénese à atualidade e ao futuro previsível", *Revista Forum de Protecçao de dados*, nº janeiro, 2016, pág.42-44, https://www.cnpd.pt/bin/revistaforum/forum2016_2/index.html#15/z (consultado el 13/01/2017), la aplicación directa del RGPD no impide lógicamente que exista el art. 35 CRP, pero sí trae consigo la necesidad de modificar este último para que no choque con la norma comunitaria. El autor se refería en dicho trabajo a la propuesta de Reglamento, pero sus conclusiones son igualmente predicables del Reglamento finalmente aprobado, que es el que a nosotros vamos a aludir. A su modo de ver, la aplicación del Reglamento plantea verdaderos problemas a la vista de la actual redacción del art. 35 CRP:

– La referencia que hace a la ley en 6 de sus 7 apartados debería completarse con el término "comunitaria" o sustituirse por el de "reglamento comunitario"; otra opción sería utilizar la expresión *"nos termos das disposições legais aplicáveis"*.

– El apartado 3º choca con el art. 9.1 del Reglamento, el cual ha sido finalmente redactado como sigue: *"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física"*. Y ello porque los supuestos de no aplicación de lo dispuesto en el referido art. 9.1 son sustancialmente distintos de los que se contemplan en el art. 35.3 CRP y bastante más amplios; no en vano, la CRP menciona únicamente *"consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis"*.

– El art. 35.4 CRP choca con la previsión del art. 17.2 RGPD pues el acceso a los datos personales se formula de una forma completamente diferente y el concepto de tercero manejado por la norma portuguesa resulta bastante confuso. El precepto comunitario obliga al responsable del tratamiento de datos que, habiéndolos hechos públicos, resulte obligado a suprimirlos a adoptar las medidas razonables (incluidas medidas técnicas), teniendo en cuenta la tecnología disponible y el coste de su aplicación, a fin de informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a los mismos, o cualquier copia o réplica de los mismos.

– El Reglamento no contiene disposición alguna que prohíba la atribución de un nº nacional único a los ciudadanos; aunque suscitó ya algunas dudas cuando se revisó la Constitución por cuarta vez, lo cierto es que tal prohibición -inútil a juicio del autor- sigue apareciendo en el art. 35.5 CRP.

– No se puede mantener el art. 35.6 CRP en los términos actuales pues el flujo transfronterizo de datos en el ámbito de la UE no puede estar sujeto a una ley nacional. De acuerdo con lo dispuesto en el art. 1.3 RGPD *"La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales"*. Pero no sólo

De entrada cabe señalar que el Reglamento amplía el ámbito de aplicación territorial en relación al marcado por la Directiva: se aplicará no sólo al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, con independencia de que el tratamiento tenga lugar en la Unión o no), sino también cuando nos encontremos ante el tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuyas actividades estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión (independientemente de si a estos se les requiere su pago), o con el control de su comportamiento (en la medida en que este tenga lugar en la Unión)[89]. Como señala Calvão, se pretende así "garantir a tutela efetiva dos direitos dos cidadãos residentes no território da UE contra ingerências nos seus dados pessoais, independentemente do Estado onde se situa a sede da empresa que trata os dados"[90]. El problema reside en que el precepto no ofrece *ad exemplum* unos criterios que permitan determinar con claridad cuándo podrá entenderse cumplido este requisito: ¿debemos fijarnos en el idioma en que se facilita la información sobre tales bienes y servicios? ¿en la moneda con que se anuncian esos bienes y servicios?[91]

Por lo que se refiere a los derechos reconocidos a los interesados, el RGPD contempla el derecho de acceso (ar. 15), el derecho de rectificación (art. 16), el derecho a la supresión ("Derecho al olvido") (art. 17), el derecho a la limitación del

eso: el Reglamento en sus art. 44-50 regula minuciosamente la transferencia de datos personas a terceros países u organizaciones internacionales se regula con detenimiento.
- El art. 35.7 CRP difiere también de lo previsto en el art. 2.1 Reglamento, según el cual, dicho instrumento se aplica *"al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"*. El precepto de la Constitución portuguesa habla únicamente de *"dados constantes de ficheiros manuais"*.
En las pág. 46-49, nuestro autor hace referencia a algunas de las reformas que habría que acometer en el precepto constitucional a la vista del Reglamento comunitario y aboga por dotar al referido art. 35 CRP de una redacción mucho más simple y atemporal, capaz de resistir los avances tecnológicos que vayan sucediéndose, que garantice el derecho de los ciudadanos a la protección de sus datos personales, correspondiendo al Estado el deber de adoptar las medidas necesarias para asegurar dicho derecho.

[88] Obras de referencia en la doctrina española relativas a este RGPD son: López Calvo, José, *Comentarios al Reglamento Europeo de protección de datos*, Sepin, Las Rozas (Madrid), 2017; Piñar Mañas, José Luis (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016; López Álvarez, Luis Felipe, *Claves Prácticas: Protección de datos personales: adaptaciones necesarias al nuevo Reglamento Europeo*, Transcis Fefebvre, Madrid, 2016.

[89] En términos similares a la Directiva, añade el art. 2.3 RGPD que también se aplicará *"al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público"*.

[90] Calvão, Filipa Urbano. "A proteção...", *op. cit.*, pág. 74.

[91] Otro criterio que se sugerido es el procedimiento o forma de adquisición del bien o servicio. *Ibidem.*

tratamiento (art. 18), el derecho a la portabilidad de los datos (art. 20), el derecho de oposición (art. 21) y el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar (art. 22). Se amplía así el elenco de derechos de los titulares de los datos, hasta ahora conocidos como derechos ARCO[92]. De todos ellos, nos vamos a centrar en el derecho de supresión o "derecho al olvido" y vamos a ver cómo se encaja la doctrina del TJUE, seguida por el TS español- en este nuevo instrumento.

2.7.1. El reconocimiento del derecho de supresión // "derecho al olvido"[93]

La supresión de los datos personales del interesado se configura en el art. 17.1 RGPD como un derecho de éste y como una obligación del responsable del tratamiento de dichos datos que debe satisfacerse sin dilación indebida cuando concurra alguna de las circunstancias que indica el precepto[94]. El RGPD, al igual que la Directiva en relación a la cancelación, no fija un plazo para que se proceda a la supresión del dato (a su cancelación) pero de él se infiere que no puede demorarse sin razón alguna. Aunque el RGPD es directamente aplicable, habrá que atender a la normativa de cada Estado la cual podría establecer un plazo concreto para hacer efectivo este derecho[95]. Las circunstancias en que cabe ejercitar este derecho son las siguientes:

[92] El ejercicio de los derechos ARCO resultaba especialmente difícil cuando los datos se habían volcado en internet. Dada la celeridad con que los datos personales son puestos a disposición en páginas web a diario en la práctica totalidad del mundo, esas dificultades se manifiestan en relación a: 1) saber quién tiene acceso a los datos; 2) saber cuáles son los datos que efectivamente se han volcado; 3) saber durante cuánto tiempo han estado puestos a disposición de los usuarios de la red. Así lo pone de relieve Estancona Pérez, Araya Lucía, "Un derecho al olvido...", *op. cit.*, pág. 473. El derecho al olvido viene a permitir al titular de los datos volcados en internet la retirada automática de los mismos por su expreso deseo, con las excepciones que determine la normativa.

[93] La utilización del término "derecho al olvido" ha sido cuestionado por autores como Estancona Pérez, Araya Lucía, "Un derecho al olvido...", *op. cit.*, pág. 474, pues el olvido es "un ejercicio eminentemente subjetivo e indudablemente voluntario". Aparicio Vaquero, Juan Pablo, "La protección de datos que viene: el nuevo Reglamento General europeo", *Ars Iuris Salmanticensis*, vol. 4, diciembre 2016, pág. 29, considera también un acierto la identificación de este derecho como "derecho de supresión".

[94] Junto a esta significativa obligación y las ya contempladas en los art. 12, 14 y 23 Directiva 95/46, el RGPD precisa otras, que van referidas también al responsable del tratamiento: registro de actividades (art. 30), notificación de violaciones de seguridad a la autoridad de control (art. 33), comunicación de dicha violación al interesado (art. 34), evaluación de impacto (art. 35) o consulta previa (art. 36).

[95] En España, como hemos visto, el plazo actualmente para hacer efectivo el derecho de rectificación y cancelación es de 10 días.

a) los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo. Este supuesto encuentra su razón de ser en el principio de "limitación de la finalidad" que opera en el tratamiento de los datos personales[96].

b) el interesado retira el consentimiento en que se basa el tratamiento conforme a lo previsto en el art. 6.1a), o en el art. 9.2a)[97], y este no se basa en otro fundamento jurídico[98];

c) el interesado se opone al tratamiento con arreglo a lo dispuesto en el art. 21.1, y no prevalecen otros motivos legítimos para el tratamiento, o el interesado se opone al tratamiento con arreglo al art. 21.2[99];

En Portugal, la Comissão Nacional de Protecção de Dados ha publicado el pasado 28 de enero de 2017 "10 Medidas para preparar a aplicação do Regulamento Europeo de Proteção de Dados", disponible en https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf (consultado el 11 de marzo de 2017). En ellas, se indica a las empresas y entidades públicas que deben revisar los procedimientos internos que garantizan los derechos de los ciudadanos a la protección de datos, atendiendo a las exigencias del RGPD, especialmente en lo relativo a los plazos máximos para contestar.

[96] No en vano, de acuerdo con lo dispuesto en el art. 5.1b) RGDP, los datos personales serán *"recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el art. 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)"*.

[97] El art. 9.1 RGPD prohíbe el tratamiento de determinados datos personales: aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. El art. 9.2, sin embargo, excluye su aplicación si media el consentimiento del titular de los datos y el Derecho de la UE o de los Estados miembros no impide al interesado levantar esa prohibición. Sobre el consentimiento puede verse YÁÑEZ, Sofia "Consentimento do interessado – a propósito do novo Regulamento de Proteção de Dados", *Jusfornal*, Nº 2528, 19 de Janeiro de 2017, Editora Wolters Kluwer.

[98] A la vista de los previsto en el art. 6.1 RGPD, el tratamiento de los datos no es lícito solo si el interesado presta su consentimiento, también cuando el tratamiento *"es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales"*; se necesita *"para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"*; se precisa *"para proteger intereses vitales del interesado o de otra persona física"*; es imprescindible *"para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento"*; o *"es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño"*. Habrá que atender, en cualquier caso, a las especificidades que, con relación a algunos de estos fundamentos (los contemplados en las letras c y e del apartado 1), introduzcan los Estados al adaptar sus normas al Reglamento.

[99] Se vincula así el derecho al olvido con el derecho de oposición, regulado en el art. 21 RGPD, según el cual: 1. *"El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el art. 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. 2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. 3. (...) 4. (...) 5. (...) 6. (...)"*.

d) los datos personales han sido tratados ilícitamente. Nos encontramos, pues, ante un supuesto en que se ha incumplido uno de los principios básicos en materia de tratamiento de datos: el principio de licitud[100]. Por lo que se refiere a esta cuestión cabe traer a colación la STJUE de 13 de mayo de 2014, cuyo apartado 93 del caso declara: "incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Este es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido"; y, en la misma línea, la STS de 5 de abril de 2016 (Roj: STS 1280/2016) en la que se indica: "un tratamiento de datos que es lícito inicialmente, por respetar las exigencias de calidad de datos, puede, con el paso del tiempo, dejar de serlo. El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los requisitos que determinan su carácter lícito y, en concreto, con los principios de calidad de datos (adecuación, pertinencia, proporcionalidad y exactitud), no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento. Un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para la finalidad con la que los datos personales fueron recogidos y tratados inicialmente, y el daño que cause en derechos de la personalidad como el honor y la intimidad, desproporcionado en relación al derecho que ampara el tratamiento de datos". Pues bien, a los principios relativos a la calidad de los datos de licitud, lealtad, limitación de la finalidad, pertinencia, adecuación, proporcionalidad, exactitud y limitación del plazo de conservación presentes en la Directiva se suman ahora, en el RGPD, los de transparencia, integridad y confidencialidad y se habla más de minimización de los datos que de proporcionalidad de los datos (es decir, se tratan los datos estrictamente necesarios en relación al fin para el que son tratados).

[100] Según el art. 5.1a) RGPD, los datos han de tratarse *"de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)*. El art. 6 especifica cuándo es lícito el tratamiento de los datos.

e) los datos personales han de suprimirse a fin de cumplir una obligación legal impuesta por la normativa de la UE o de los Estados miembros que se aplique al responsable del tratamiento[101].

f) los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el art. 8.1. Este precepto se refiere expresamente a los requisitos que deben darse para que sea lícito el tratamiento de datos de un niño: es lícito si el menor que presta su consentimiento es mayor de 16 años o si, siendo menor de esa edad, consiente el titular de la patria potestad o el tutor del niño y únicamente en la medida en que presta el consentimiento. El RGPD, no obstante, deja abierta la puerta para que los Estados miembros, si lo desean puedan rebajar la edad a que puede consentir el menor hasta los 13 años.

El art. 17.2 establece un deber adicional para el responsable del tratamiento que hubiere hecho públicos los datos personales y resultara obligado a suprimirlos: el de 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, para lo cual deberá adoptar *"medidas razonables, incluidas medidas técnicas"*[102]. Del tenor del precepto se infiere

[101] Como hemos indicado ya, en España, por ej., el art. 29.4 LOPD limita a 6 años el tiempo por el que se pueden tratar los datos personales relativos a la solvencia económica.

[102] Tras poner de relieve que el Reglamento Europeo recoge el "derecho al olvido pero no desarrolla suficientemente cómo debe ser considerado y tratado en la práctica", Davara Rodríguez, Miguel Ángel, "El Código del Derecho al Olvido", *El Consultor de los Ayuntamientos*, Nº 1, Quincena del 15 al 29 Enero 2015, pág. 99, tomo 1, (LA LEY 9276/2014) destaca este deber al que se aludía en el considerando 54 del proyecto de Reglamento europeo y en el que se insiste en el Considerando 66 del Reglamento finalmente aprobado. Desde su punto de vista, "es en este aspecto en el que podemos encontrar un primer acercamiento a que se haga efectivo el derecho al olvido ya que es el responsable del tratamiento el que puede adoptar medidas organizativas, incluso técnicas, para impedir que los datos puedan salir de su entorno de responsabilidad". El problema es que, en la práctica, va a resultar muy difícil controlar estos datos porque, aunque no puedan ser descargados del sitio web, pueden haberse «subido» a otra página de Internet o a otro lugar de almacenamiento aunque solo sea para facilitar la velocidad de comunicación y acceso o la optimización de la información a recibir. En esos casos, los datos habrían salido del "ámbito de responsabilidad del responsable del tratamiento" y en muchos de ellos, éste ni siquiera sería consciente de ello.

El Considerando 78 RGPD insiste en la necesidad de adoptar *"medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. (...), el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad".*

que la razonabilidad de las medidas deberá valorarse atendiendo a la tecnología disponible y el coste de su aplicación. El art. 19 RGPD le impone, además, el deber de notificar la rectificación, supresión o limitación de datos que se haya efectuado a cada uno de los destinatarios a los que se hubieran comunicado los datos personales, salvo que ello sea imposible o exija un esfuerzo desproporcionado; deberá informar también al interesado acerca de dichos destinatarios en el caso de que así lo solicite.

Ahora bien, al derecho al olvido, como hemos puesto de relieve ya, no es un derecho absoluto. La supresión de los datos no puede equivaler en todos los casos a borrado de los datos. Para empezar, es preciso conciliarlo con la libertad de expresión y el derecho a la información[103]. Consciente de ello, el art. 17.3

Davara Rodríguez asocia estos conceptos con el estudio de la denominada trazabilidad (algo fundamental tanto en el ámbito del análisis de mercados y fidelización de clientes, como en la mejora de la competencia y optimización en la fabricación y distribución). Desde su punto de vista, en el ámbito que nos ocupa, esta trazabilidad puede ser importante en orden a proteger los datos y la privacidad desde el diseño y por defecto, de tal forma que las aplicaciones de los tratamientos de datos se ciñan al cumplimiento de los principios de la protección de datos en garantía del respeto de la normativa. "Si mediante la trazabilidad nos podemos referir a patrones determinados a través de una serie de comparaciones que presenten algunas características previamente señaladas", -afirma- "la aplicación de tratamiento de datos tanto en la fase previa de definir o resolver sobre la arquitectura de sistema, como la de adaptación e interoperabilidad de bases de datos, mensajes y notificaciones, así como los estándares mínimos de planificación, seguridad y otros, se convierte en una necesidad". Y concluye, "Si el sistema gestiona datos de carácter personal, se deben incorporar los mecanismos para establecer la trazabilidad de acceso a dichos datos."

[103] Este derecho se encuentra también reconocido en la Carta de los Derechos Fundamentales de la UE (art. 11).

En la CE, en el art. 20

1. *"Se reconocen y protegen los derechos:*

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

b) A la producción y creación literaria, artística, científica y técnica.

c) A la libertad de cátedra.

d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. *El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.*

3. *La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.*

4. *Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.*

5. *Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial"*

En la CRP, en el art. 37: *"Liberdade de expressão e informação"*

RGPD prevé la no aplicación de lo dispuesto en sus apartados 1 y 2 cuando el tratamiento sea necesario a) *"para ejercer el derecho a la libertad de expresión e información*[104]. Mas no es éste el único supuesto en que debe ceder el derecho de supresión: tampoco resultan aplicables los apartados 1 y 2 del art. 17 cuando el tratamiento se precise: b) *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*[105]; c) *por razones de interés público en el ámbito de la salud pública de conformidad con el art. 9, apartado 2, letras h) e i), y apartado 3;* d) *con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el art. 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento*[106], o[107] e) *para la formulación, el ejercicio o la defensa de reclamaciones"*[108]. No podemos estar de acuerdo con CASIMIRO cuando, refiriéndose aún a la propuesta de Reglamento, afirmaba que su art. 17 parecía sugerir que su objetivo no es otro que eliminar todos los datos personales comprendidos en el tratamiento (eliminarlos en la página de origen) y no sólo dificultar su localización por parte de terceros. El objetivo –añadía- es eliminar la información relativa al titular de los datos. A nuestro modo de ver, el RGPD no se aparta de los planteamientos del TJUE: la finalidad con que tratan

1. *"Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações.*
2. *O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura.*
3. *As infracções cometidas no exercício destes direitos ficam submetidas aos princípios gerais de direito criminal ou do ilícito de mera ordenação social, sendo a sua apreciação respectivamente da competência dos tribunais judiciais ou de entidade administrativa independente, nos termos da lei.*
4. *A todas as pessoas, singulares ou colectivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta e de rectificação, bem como o direito a indemnização pelos danos sofridos".*

[104] El art. 85 RGPD se refiere expresamente también a la necesidad de conciliar el tratamiento de datos con la libertad de expresión y de información al disponer:

1. *"Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.*
2. *Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.*
3. *Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas".*

Esta remisión de la regulación a los Estados miembros puede derivar en un conflicto entre distintas normativas que, según el considerando 153, que resolverá a favor del Derecho del Estado miembro aplicable al responsable del tratamiento. Llama la atención que tal previsión se contenga en el referido considerando y no en el articulado del RGPD.

[105] Piénsese, por ej., en el tratamiento de datos con fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad. En estos casos, apunta López Álvarez, Luis Felipe, *Claves Prácticas: Protección... op. cit.*, pág. 38, debe determinarse si el tratamiento puede ser llevado a cabo por una entidad de Derecho privado como una asociación profesional.

[106] Según el art. 89 RGPD: *"El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines puedan alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo".*

[107] Llama la atención el empleo de la conjunción disyuntiva "o" en vez de la conjunción copulativa "y"; da la sensación de que la enumeración tiene carácter ejemplificativo y queda abierta a otros supuestos equivalentes.

[108] Al hilo de la propuesta de Reglamento, Davara Rodríguez, Miguel Ángel, "El Código del Derecho al Olvido", *op. cit.*, señalaba que, si la supresión equivaliera al borrado de los datos en todo caso, podría darse la situación de que el responsable del tratamiento al que se le hubiera exigido la supresión se encontrara indefenso en un momento posterior ante una eventual reclamación al no poder acudir al dato primitivo aunque solamente fuera para defenderse. En la propuesta de Reglamento, esa situación se contemplaba en art. 17.4, según el cual, en lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando se den determinadas circunstancias, de entre las que destacaba en el apartado b), cuando "el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios". El Reglamento finalmente aprobado dedica un precepto expresamente –el art. 18- a regular el derecho a la limitación del tratamiento de datos, un derecho que parece quedarse a medio camino entre el derecho de rectificación y el derecho de oposición. En virtud de este derecho, el interesado tiene derecho a obtener del responsable del tratamiento de los datos la limitación de dicho tratamiento cuando se cumpla alguna de las condiciones que siguen: a) *"el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;* b) *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;* c) *el responsable 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;* d) *el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado".* La limitación del tratamiento se define en el art. 4.3 RGPD como *"el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro"*; este derecho supone, en definitiva, que el responsable del mismo deberá reservarlos (conservarlos) pero sólo podrán ser utilizados con el consentimiento del interesado para la formulación, el ejercicio o la defensa de reclamaciones, para defender, en materia de protección de datos, los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. El art. 18.3 finalmente contempla el deber del responsable del tratamiento de informar a los interesados que hayan obtenido la limitación del tratamiento de que van a dejar de aplicar la referida limitación. La necesidad de un desarrollo normativo por parte de las autoridades nacionales o del Comité Europeo de Protección de Datos que acote los plazos aplicables en cada supuesto, el procedimiento para ejercitarlo... y un largo etc, es evidente.

los datos los responsables en origen y los motores de búsqueda es diferente; de ahí que, como sucede en el caso Costeja, pueda mantenerse la información en la web del Diario La Vanguardia y, sin embargo, deba eliminarse en los motores de búsqueda. El tratamiento efectuado por el primero se realiza con fines periodísticos; tal justificación no existe, en cambio, en el caso del motor de búsqueda pues dicho motor no informa sino que difunde la información publicada por otros.

El alcance de este derecho y las obligaciones que lleva aparejadas[109], sin embargo, puede verse limitado por la propia normativa de la Unión o de los Estados miembros, siempre que esa limitación *"respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles"*. Así lo prevé expresamente el art. 23 RGPD, cuyo apartado 2, precisa el contenido mínimo que debe incluir la medida en cuestión: a) *"la finalidad del tratamiento o de las categorías de tratamiento;* b) *las categorías de datos personales de que se trate;* c) *el alcance de las limitaciones establecidas; d) las garantías para evitar accesos o transferencias ilícitos o abusivos;* e) *la determinación del responsable o de categorías de responsables;* f) *los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;* g) *los riesgos para los derechos y libertades de los interesados, y* h) *el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta"*.

[109] El art. 23 RGPD se refiere concretamente al *"alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22"* (aquí es donde se incluye el derecho a la supresión de los datos –derecho al olvido-) *"y el artículo 34"* (este precepto regula cómo ha de procederse cuando se produce una violación de la seguridad de los datos personales del interesado), *"así como en el artículo 5"* (este precepto contiene los principios conforme a los cuales ha de realizarse el tratamiento de los datos personales) *"en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22"*.

2.7.2. Cuestiones a tener en cuenta en relación al responsable del tratamiento cuando se ejercita el derecho al olvido frente a los motores de búsqueda a la luz del Reglamento

A la vista del art. 17 RGPD, no cabe duda de que es el responsable del tratamiento el que tiene que facilitar el ejercicio del derecho al olvido. El art. 4 (7) RGPD considera "responsable del tratamiento" a *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"*. Sus términos no difieren de los del art. 2 d) de la Directiva 95/46/CE[110] y de los manejados en el ámbito nacional[111]. Ahora bien, como hemos tenido oportunidad de ver, en la jurisprudencia española, la determinación de quién es efectivamente el responsable no es una cuestión pacífica.

El art. 17 RGPD se ve complementado por el art. 58 del mismo texto, según el cual, entre los poderes de la autoridad de control, se incluye el de ordenar al responsable o encargado del tratamiento que atiendan las solicitudes del ejercicio de los derechos del interesado [art. 58.2 c)] y, en concreto, ordenar la supresión de los datos con arreglo al art. 17 y la notificación de las medidas adoptadas por el responsable en los términos del art. 17.2 [art. 58.2.g)], medidas que, como señala el considerando 66, se imponen al responsable del tratamiento que haya hecho públicos los datos, precisamente para reforzar el derecho al olvido. Es igualmente significativo que la decisión de la autoridad de control, aun notificada al establecimiento principal o único establecimiento del responsable en el territorio de un Estado miembro, se adopta en relación con el responsable del tratamiento, que

[110] Según dicho precepto, se entenderá por *"responsable del tratamiento"*: *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario"*.

[111] En España, el artículo 3.d) LOPD considera responsable del tratamiento a la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*. El artículo 5.1.q) RD 1720/2007, por su parte, define al *"Responsable del fichero o del tratamiento"* como la *"Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados"*.
En Portugal, el art. 3 Lei 67/98 lo define como *"a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios do tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa"*.

es quien a su vez debe adoptar las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión (art. 60.9 y 10).

El RGPD incluye también entre las definiciones de su art. 4 la correspondiente a "establecimiento principal". En lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, señala que es el *"lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones"*. El alcance de este concepto se explica en el considerando 36, según el cual, el establecimiento principal de un responsable en la Unión debe determinarse "en función de criterios objetivos y debe implicar el ejercicio efectivo y real de las actividades de gestión que determinan las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables". Estamos, por tanto, ante un concepto de carácter funcional por cuanto supone el ejercicio y desempeño efectivo de las atribuciones determinantes del tratamiento de datos, fijación de los fines y medios. En el ámbito que nos ocupa –el de los motores de búsqueda- ¿podría entenderse que una entidad como Google Spain, S.L. reúne los requisitos y condiciones que permitan considerarla como establecimiento principal del responsable –esto es, Google Inc.- en el ámbito de la Unión Europea? No parece que así sea[112].

En el ámbito de la responsabilidad, cobra especial interés la regulación, en el art. 26 RGPD, de la corresponsabilidad en el tratamiento de datos. Dicho precepto considera corresponsables a quienes determinen conjuntamente los objetivos y los medios del tratamiento y les exige (a los corresponsables) que determinen de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el Reglamento, en particular en lo relativo al ejercicio de los derechos del interesado[113]. De lo dicho se sigue

[112] Así lo ponen de relieve las SSTS (Sala de lo Contencioso-Administrativo) citadas en las notas nº 74-80.

[113] Bajo el subepígrafe *"Corresponsables del tratamiento"*, el art. RGPD determina:

1. *"Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las 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 podrá designar un punto de contacto para los interesados.*

2. *El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.*

3. *Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables".*

que los elementos básicos que definen la condición de corresponsable son dos: 1) la efectiva participación en la determinación de los objetivos y los medios del tratamiento (elemento principal), y 2) la delimitación de su concreta responsabilidad en el cumplimiento de las obligaciones impuestas por el Reglamento (elemento especialmente trascendente en orden a garantizar el ejercicio de sus derechos por el interesado). Queda, así, al arbitrio de los corresponsables («mutuo acuerdo») la determinación de sus responsabilidades en relación al cumplimiento de las obligaciones derivadas de su condición, «en particular en cuanto al ejercicio de los derechos del interesado». Abunda en ello el considerando 79 cuando señala que, la protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables. Ahora bien, ¿qué ocurrirá en el caso de que los corresponsables no determinen su concreta responsabilidad? ¿Qué pasará si entre los agentes que ejecutan un tratamiento de datos (dos o más) se confía la responsabilidad formal (simulada) sólo a uno de ellos pero entre ellos hay más de un responsable material (real)? Esto es precisamente lo que parece suceder en los casos que venimos analizando entre Google Inc. y Google Spain, por lo que, llegados a este punto, nos asalta la duda: cuando resulte efectivamente aplicable el RGPD, ¿asumirán la matriz y sus sucursales ubicadas a lo largo y ancho de la geografía europea, *motu proprio*, la corresponsabilidad de sus filiales?[114]

Para terminar, no está de más recordar que el responsable del tratamiento puede incurrir en responsabilidad civil (art. 82 RGPD[115]), administrativa (art. 83

[114] Di Pizzo Ciuacchio, Adrián, "Efectos...", *op. cit.*, pág. 970-971, duda de que así sea. En su opinión, teniendo en cuenta el periplo administrativo y jurisdiccional que se ha seguido en el Ordenamiento español -y en el resto de Ordenamientos nacionales europeos- durante los últimos años (negando la participación de las sedes geográficas de Google en la fijación de los medios y fines en el tratamiento de datos personales de su buscador), no tendría mucho sentido que "Google Spain asumiera su carácter de corresponsable junto con Google Inc. o esta última le atribuyera tal condición y recíprocamente delimitaran las operaciones que cada una lleva a cabo al respecto". No obstante, habrá que ver cómo actúan a tales efectos Google Inc. y sus filiales una vez comience a aplicarse el RGPD.

[115] Como se indica en el considerando 146 RGPD, el responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento (por tal se entiende también, el que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento); eso sí, quedarán exentos de responsabilidad en el caso de que demuestren que, en modo alguno, son responsables de los daños y

y 84 RGPD[116]) o incluso, penal[117]. Como veremos más adelante, a nosotros nos interesa especialmente la responsabilidad civil.

perjuicios. El RGPD apuesta por una interpretación amplia del concepto de daños y perjuicios (a la luz de la jurisprudencia del Tribunal de Justicia), a fin de que se respeten plenamente los objetivos del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. En el caso de que los responsables o encargados participen en el mismo tratamiento, cada responsable o encargado deberá ser considerado responsable de la totalidad de los daños y perjuicios; ahora bien, si se acumularan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización podría prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre que se garantizase la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. El responsable o encargado que abone íntegramente la indemnización podrá reclamar después la parte correspondiente a los demás responsables o encargados que hayan participado en el mismo tratamiento. Lo dicho debe entenderse sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros.

Actualmente, tanto la normativa interna española como la portuguesa contemplan la necesidad de indemnizar los daños y perjuicios causados por los responsables del tratamiento de datos.

El art. 19 LOPD regula el *derecho a indemnización* en los términos que siguen:

1. *"Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.*
2. *Cuando se trata de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.*
3. *En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria".*

El art. 34 Lei 67/98, por su parte, se refiere a la *"Responsabilidade civil"* en los siguientes:

1. *"Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto que viole disposições legais em matéria de protecção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido".*
2. *"O responsável pel o tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável".*

[116] Estos preceptos contemplan la imposición de multas administrativas como consecuencia de la infracción de lo preceptuado por el RGPD.

[117] La responsabilidad penal no es objeto de regulación por el RGPD. En este sentido cabe traer a colación el considerando 149, en el que se afirma que *"Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio «ne bis in idem», según la interpretación del Tribunal de Justicia".* Y el considerando 152, en el que se insiste en que, en los casos en que el presente Reglamento no armonice las sanciones administrativas, o en aquellos otros en que se requiera (ej. supuestos de infracciones graves del presente Reglamento), *"los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias".* Será el Derecho de los Estados miembros el que determine la naturaleza de dichas sanciones, ya sea penal o administrativa.

Así pues, parece que será necesario adaptar la normativa interna. En España, en el ámbito penal, el art. 197 CP.

3. Las dificultades para aplicar el derecho al olvido

La realidad, sin embargo, evidencia múltiples dificultades para aplicar satisfactoriamente este derecho de supresión o derecho al olvido, tanto en los términos que marca la STJUE como en los términos que ha definido finalmente el RGPD. La adaptación de la normativa interna de España y Portugal sobre protección de datos, por su parte, tampoco parece estar exenta de problemas. Sin ánimo de ser exhaustivos, nos referiremos a algunos de los problemas que hemos apreciado, tomando como referencia, fundamentalmente la legislación y jurisprudencia españolas.

3.1. Invocación de un motivo legítimo y fundado en los casos en que la publicación ha sido ordenada por la ley

El derecho de supresión o derecho al olvido, aunque se reconozca como un derecho independiente, en el fondo va ligado al ejercicio del derecho de oposición. En tales casos, el interesado tendrá que invocar un motivo legítimo y fundado. En este orden de cosas podría alegar que la información le perjudica injustificadamente o le hace desmerecer. Sin embargo, esa primera valoración puede no resultar tan sencilla si pensamos en supuestos en los que se ha publicado en un Boletín Oficial un indulto, la concesión de una ayuda o subvención pública, los resultados del concurso oposición para acceder a la función pública, por ejemplo, o cuando se trata de noticias. El motivo personal existe, puede ser legítimo pero puede no ser fundado. En algunos casos, podemos encontrarnos con que existe una obligación legal de publicar determinados datos; así sucede, por ej., con los indultos; dicha obligación legal se proyecta sobre el editor pero no necesariamente ha de transferirse al buscador; a nadie se le escapa, además, que la indexación de dicha información puede incidir muy negativamente en la vida futura de la persona. También se publican en Boletines oficiales las ayudas y subvenciones o los datos relativos al concurso-oposición para acceder a la función pública; en estos casos, es patente el interés público; mas, ¿qué ocurriría si la persona que concurre al concurso es una mujer víctima de violencia de género?, por ej. Es evidente – como muy bien pone de relieve MARTÍNEZ MARTÍNEZ – que hay que diferenciar entre la obligación legal del editor y las obligaciones del buscador; este último, a la hora de llevar a cabo el juicio de ponderación, no debe tomar en consideración las obligaciones legales de publicación[118]. En los supuestos en que

[118] MARTÍNEZ MARTÍNEZ, Ricard, "Aplicar el derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 36, pág. 124-126. De lo contrario –añade – "se complicará extraordinariamente el juicio a

no existe deber legal de publicar es preciso realizar una ponderación de los intereses en juego: a tal efecto, hay que determinar si se ha producido, efectivamente, una injerencia en derechos como el derecho al respeto a la vida íntima y familiar o el derecho a la protección de datos (por citar algunos), y verificar después si dicha intromisión se encuentra legalmente prevista y si es legítima y necesaria[119]. Habrá que valorar, por consiguiente, el derecho a la información y la libertad de expresión: ¿Hasta qué punto el interés público de una información justifica su mantenimiento e indexación? ¿Estamos ante un personaje público? ¿Tienen las personas jurídicas un derecho al olvido?[120] Mas las dificultades no terminan aquí.

3.2. Concesión de una indemnización por incumplimiento de los deberes que derivan del ejercicio del derecho al olvido por parte del interesado

A fin de analizar los problemas que surgen a la hora de conceder una indemnización por incumplimiento del derecho que nos ocupa resulta especialmente interesante traer a colación la STS, Sala de lo civil, de 15 de octubre de 2015 (LA LEY 139641/2015) anteriormente mencionada[121]. Para empezar, esta sentencia ha sido dictada en pleno, de modo que asienta la tendencia que va a seguir, de ahora en adelante, nuestro Alto Tribunal en esta materia; y, para continuar, no sólo aplica el llamado derecho al olvido sino que concede una indemnización al particular que ejercita dicho derecho, al entender que se ha producido un quebranto de su derecho al honor y la intimidad. El supuesto de hecho que da origen a la misma puede resumirse como sigue. En los años ochenta, los ahora

realizar por el segundo tanto en lo que se refiere al supuesto concreto como respecto de lo que podríamos definir como el coste de tiempo vinculado al estudio minucioso del Derecho aplicable".

[119] El principio de necesidad no puede interpretarse de forma homogénea para todos los países y en todo momento. Como indica Martínez Martínez, Ricard, "Aplicar el derecho...", *op. cit.*, pág. 128, la interpretación más cercana al art. 8 de la Carta de los Derechos Fundamentales de la UE en la jurisprudencia del TEDH "se identifica con la idea de necesidad entendida en términos de «exigencia social imperiosa» de la injerencia".

[120] Para Botana García, Gema Alejandra "Comentario a la Sentencia...", *op. cit.*, el debate está abierto no sólo en relación a las informaciones sensibles sobre una persona concreta que han sido publicadas en Internet por los medios de comunicación como una manifestación del derecho a la información (ej. relativas a imputaciones de delitos) o las informaciones publicadas en las ediciones digitales de Boletines y Diarios Oficiales por imperativo legal, (ej. notificaciones, resoluciones...); también lo está respecto a las informaciones publicadas por usuarios de la red, de forma anónima, en ejercicio de su libertad de expresión y las informaciones publicadas por el propio usuario en redes sociales, quien quiere que se cancelen cuando solicita la baja en la red de que se trate.

[121] Una reseña de esta importante sentencia puede verse en Rubio Torrano, Enrique "El derecho al olvido digital", *Revista Doctrinal Aranzadi Civil-Mercantil*, nº 1/2016, (BIB 2015\18280).

demandantes –quienes tenían un alto grado de drogodependencia- fueron detenidos por tráfico de drogas, y, una vez en prisión, recibieron la correspondiente atención por sufrir síndrome de abstinencia. Un periódico de ámbito nacional se hizo eco inmediatamente de la noticia y la publicó con los hechos descritos, identificando a las personas afectadas con sus nombres, apellidos e, incluso, profesión. Los demandantes resultaron condenados por los hechos indicados pero, pasado el tiempo, superaron su adicción a las drogas y desarrollaron una vida familiar y profesional con absoluta normalidad. En noviembre de 2007, la empresa propietaria del diario permitió el acceso público general y gratuito a la hemeroteca digital pero la página web en que se encontraba recogida la noticia no sólo no contenía código o instrucción alguna que impidiera la indexación de los datos personales sino que los datos personales aparecían como palabras clave en la cabecera de dicho código fuente, resaltando su relevancia; además, la web del diario fomentaba el acceso a la página pues incluía instrucciones informáticas («index» y «follow») que potenciaban la indexación del contenido de la noticia y su inclusión en las bases de datos de los motores de búsqueda más populares en internet, de modo que, cuando se introducía el nombre y los apellidos de alguno de los demandantes, el enlace a la web de la hemeroteca digital del diario que contenía la noticia aparecía como primer resultado en Google y Yahoo. En 2009, estas personas solicitaron al diario que cesara en el tratamiento de sus datos personales en la página web o que los sustituyera por las iniciales de sus nombres y apellidos, y adoptara las medidas tecnológicas necesarias para que la página web de la noticia no fuese indexada por los motores de búsqueda de Internet pero el diario, apelando a la libertad de información, rechazó la petición. Así las cosas, interpusieron la correspondiente demanda –única y exclusivamente contra el diario[122]- solicitando básicamente que: 1º) se declarara que la difusión realizada por ediciones X, a través del sitio web de la editora, de la noticia publicada por el periódico diario, suponía una vulneración del derecho a la intimidad y al honor de las personas demandantes, y se condenara a la editora al cese inmediato en la difusión a través de internet de dicha noticia; 2º) se declarara que la utilización por la editora del diario de los nombres y apellidos de las personas demandantes en

[122] Esta es una de las peculiaridades que presenta el caso: la demanda no se dirige frente al editor y el motor de búsqueda; se dirige únicamente frente al editor.
Y es que, como señalara Touriño, Alejandro, *El derecho al olvido y a la intimidad en Internet*, Los libros de la Catarata, Madrid, 2014, pág. 44, muchas veces no sabe siquiera a quién dirigirse para plantear la solicitud de retirada de contenidos: ¿al titular del sitio web o al buscador de Internet? Si acude al titular del sitio web donde el buscador de Internet ha encontrado la información, se defenderá aludiendo a la existencia de un conflicto de derechos, el derecho a la libertad de expresión e información y los derechos individuales de la persona.

el código fuente de la página web vulneraba el derecho a la intimidad y al honor de los actores y, en consecuencia, se condenara a dicha editora al cese inmediato en el uso de sus datos personales; 3º) se declarara que el modo en que la editora del periódico había programado la página web que contenía la información, permitiendo que los proveedores de servicios de intermediación de búsqueda indexaran su contenido por el nombre y apellidos de las personas demandantes, suponía una vulneración de su derecho a la intimidad y al honor; 4º) se declarara que el tratamiento de los datos personales de los actores que la editora del diario realizaba en la página web y en el código de la misma constituía una vulneración del derecho a la protección de datos personales de los demandantes y, en consecuencia, se condenara a la citada editora al cese inmediato en el uso de los datos personales contenidos en la mencionada página web y en el código fuente de la misma o, subsidiariamente, a sustituir sus nombres y apellidos por las iniciales de los mismos; y 5º) se fijara una indemnización.

El Juzgado de Primera Instancia estimó la demanda, declaró que la difusión de la noticia realizada por la editora del periódico constituía una vulneración del derecho al honor, intimidad y protección de datos de los demandantes y condenó a la demandada al cese inmediato de la difusión de la noticia y a la implantación de las medidas tecnológicas adecuadas para impedir dicha difusión y evitar que dicha noticia apareciera cuando se insertaban los nombres y apellidos de los actores en Google, así como a una indemnización de 7.000 €. Recurrida la sentencia en apelación, la Audiencia Provincial desestimó el recurso y estimó la impugnación realizada, a su vez, por los demandantes, quienes consideraban que la sentencia de instancia había incurrido en incongruencia omisiva pues no se había pronunciado sobre la solicitud del cese en el tratamiento de sus datos personales o, subsidiariamente, la sustitución de los nombres y apellidos por las iniciales en la noticia y en el código fuente de la página web que la contiene. Al estimar la impugnación, la AP de Barcelona añade una nueva condena a la editora del periódico: ha de cesar en el uso de los datos personales en el código fuente de la página web que contenía la noticia. Ante esta situación, el diario demandado interpone recurso de casación que se basa fundamentalmente en dos motivos:

1. Caducidad de la acción ejercitada: infracción del art. 9.5 LO 1/82, de 5 de mayo, del protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en relación con la vulneración del art. 20.1.d) CE, pues han transcurrido más de cuatro años desde que se difundió la información.
2. Infracción del art. 7 LO 1/82, de 5 de mayo, en relación con el art. 2.1 del mismo Cuerpo normativo y en conexión con la vulneración del art. 20.1.d CE. Se aduce a estos efectos por la recurrente que: a) las reiteradas referencias a la finalidad económica de la digitalización de la hemeroteca no pueden sostenerse pues el carácter privado del medio de comunicación y la utilización de la publicidad como fuente de ingresos no impide que su actuación quede amparada por las libertades de expresión y de información, contempladas en el art. 20 CE; b) los hechos publicitados, declarados delictivos, fueron veraces y tenían interés público; el transcurso del tiempo no los convierte en inveraces y carentes de interés público; y c) la actuación de la demandada constituye un tratamiento de datos personales con fines periodísticos, por lo que está amparada por la libertad de información.

Por lo que se refiere al primero de ellos (caducidad de la acción), el TS indica que lo relevante no es el momento en que se publicó la noticia en el periódico en papel – como pone de manifiesto la STS de 29 de enero de 2014 (Roj: STS 434/2014) –, "sino si persiste el tratamiento de los datos personales que no cumple los requisitos de la normativa sobre protección de datos personales y causa un daño a los afectados al vulnerar su honor y su intimidad". En el caso en cuestión, al tiempo de iniciarse el proceso, persistía el tratamiento de los datos personales que los demandantes entendían ilícito, vulnerador de sus derechos fundamentales y causante del daño, pues sus datos continuaban estando incluidos en la web en un modo que permitía la indexación por parte de los buscadores de internet.

Por lo que se refiere al segundo, el TS precisa que lo que se enjuicia, en este caso, no es la publicación en papel hace más veinte años sino el tratamiento derivado de la digitalización de la hemeroteca del diario en que se publicó la información. Sobre esta base, siguiendo los postulados del TJUE -quien considera que el *«editor de una página web en la que se incluyen datos personales realiza un tratamiento de datos personales y como tal es responsable de que dicho tratamiento de datos respete las exigencias de la normativa que lo regula, en concreto las derivadas del principio de calidad de los datos»*- entiende que la editora del diario es efectivamente responsable del tratamiento de los datos personales de los demandantes contenidos en la página web mencionada.

La calidad de los datos, de acuerdo con el art. 6 de la Directiva 1995/46/CE, de 24 de octubre, se asienta en los principios de adecuación, pertinencia, proporcionalidad y exactitud. En el supuesto en cuestión, el problema no reside en que el tratamiento de los datos personales sea inveraz (la editora no ha vulnerado la exigencia de veracidad de los datos), sino en si puede considerarse o no adecuado a la finalidad con la que los datos personales fueron recogidos y tratados inicialmente. En este punto -afirma el Alto Tribunal –, el factor tiempo resulta fundamental, pues el tratamiento de los datos personales debe cumplir con los principios de calidad no solo en el momento en que son recogidos e inicial-

mente tratados, sino durante todo el tiempo en que se produce ese tratamiento. El problema, por tanto, radica en concretar el momento a partir del cual ha de considerarse que los datos han perdido la legítima finalidad con que fueron recogidos inicialmente y deben desaparecer de la base de datos correspondiente, o, como dice el art. 4.1 LOPD el momento en que han *"dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados"*; sólo a partir de ese momento podremos entender que se está produciendo un daño resarcible civilmente. Llegados a este punto, el TS recuerda, a modo de ejemplo, que los sujetos responsables de los ficheros sobre solvencia patrimonial, de acuerdo con lo previsto en el art. 29.4 LOPD, no pueden conservar datos adversos de personas por un período superior a seis años. Ahora bien, como pone de relieve SELIGRAT GONZÁLEZ, este es un caso peculiar en el que la LOPD impone expresamente una obligación especial de control en el tratamiento de datos y del tiempo en que pueden estar almacenados. En el supuesto de los datos que consten en bases de datos de Internet, habrá que dilucidar "si sobre el responsable del tratamiento de tales datos pesa el deber de estar pendiente del momento en que dichos datos han perdido la finalidad con la que fueron recogidos inicialmente, de manera que se vea obligado a su cancelación. O, si por el contrario, debe ser el perjudicado quien, una vez aprecie que ya no se cumple con el requisito de calidad de los datos, esté obligado a comunicar a la persona encargada del tratamiento su derecho de cancelación y sólo a partir de este momento se entienda que el anterior sujeto está obligado al borrado de los datos". En opinión de este autor, la primera de las opciones supone imponer un gravamen excesivo a los sujetos encargados de las bases de datos, pues su diligencia debe manifestarse cuando tengan conocimiento del ejercicio del «derecho al olvido» por parte del interesado; no en vano, según el art. 12 b) de la Directiva 95/46 (antecedente a nivel europeo de la LOPD), el interesado tendrá derecho a obtener del responsable del tratamiento la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la citada Directiva; estamos ante un derecho que el interesado puede ejercer o no; en consecuencia, "no cabe interpretar una imposición de un deber de análisis por parte del sujeto encargado del tratamiento de los datos sobre en qué momento han perdido la finalidad con la que inicialmente fueron recogidos"[123]. El TS, sin embargo, en esta Sentencia de 15 de octubre de 2015 no

[123] SELIGRAT GONZÁLEZ, Víctor Manuel, "El «derecho al olvido digital». Problemas de configuración jurídica y derivados de su incumplimiento a la vista de la STS de 15 de octubre de 2015", *Actualidad Civil*, nº 12, Diciembre 2015, (LA LEY 8063/2015). El autor considera, no obstante, que "el legislador podría imponer un especial deber de vigilancia sobre los datos obrantes en bases de datos de diarios digitales". Siguiendo a VILASAU, M. "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *Revista de Internet, Derecho y Política*, nº 18, junio 2014, pág. 32, apuntaba que, de cristalizar, el art. 17.8 bis de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos podría sustentar esta interpretación, pues prevé que "el responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de los datos personales, así como para el examen periódico de la necesidad de conservar los datos". Dicha previsión se infiere hoy de lo previsto en el art. 5 e) RGPD, según el cual: los datos han de mantenerse *"de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales"*, pudiendo conservarse durante períodos más largos cuando se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, *"sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado"* («limitación del plazo de conservación»); y, más concretamente, del 24.1 RGPD *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario"*. Nótese a estos efectos, además que el art. 23 contempla la posibilidad de que el Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento limite, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los art. 5, 12 a 22 y 34, *"cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles"*. Conforme a lo previsto el art. 23.2, cualquiera de estas medidas a que se refiere el art. 23.1 deberán indicar: *a) "la finalidad del tratamiento o de las categorías de tratamiento; b) las categorías de datos personales de que se trate; c) el alcance de las limitaciones establecidas; d) las garantías para evitar accesos o transferencias ilícitos o abusivos; e) la determinación del responsable o de categorías de responsables; f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento; g) los riesgos para los derechos y libertades de los interesados, y h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta"*. (El subrayado es nuestro).
SELIGRAT GONZÁLEZ recuerda también, a estos efectos, las propuestas doctrinales de autores como ZITTRAIN, Jonathan L., *The future of the Internet and how to stop it*, Yale University Press, New Haven, 2008, pág. 229 y ss, https://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future%20of%20the%20Internet.pdf?sequence=1 (consultado el 1/03/2017) o MAYER-SCHÖNBERGER, Viktor, *Delete: the virtue of forgetting in the digital age*, Princeton University Press, Princeton, 2009, pág. 163 y ss.. ZITTRAIN desarrolla una teoría según la cual la gente podría declarar una quiebra de reputación cada diez años aproximadamente, dejando su reputación en blanco (eliminando ciertas categorías de calificaciones u otra información sensible) y empezar de nuevo. MAYER-SCHÖNBERGER, por su parte, sostiene que la tecnología digital y las redes globales están erosionando la capacidad natural para olvidar de las personas y propone establecer fechas de caducidad en la información. También RULLI JÚNIOR, Antonio y RULLI NETO, Antonio, "Direito ao esquecimento e o superinformacionismo: apontamentos no direito brasileiro

establece con claridad en qué momento la información sobre la participación delictiva de los interesados perdió su legitimidad en su tratamiento; se limita a decir (como veremos después) que, al haber transcurrido más de veinte años, los interesados estaban ya legitimados para solicitar la cancelación de estos datos. A falta de mayor desarrollo legislativo, serán, por tanto, los tribunales quienes lo determinarán a la vista del caso concreto, pues no toda información tiene idéntico contenido ni puede despertar idénticas sensibilidades.

A efectos de determinar la licitud o no del tratamiento, el TS lleva a cabo, lógicamente, una ponderación de los distintos derechos y bienes jurídicos en juego. Por una parte, el ejercicio de la libertad de información[124] (ámbito en el que el Tribunal reconoce que, tratándose de la edición y puesta a disposición del público de hemerotecas digitales en internet, el ejercicio de la libertad de información otorga un ámbito de protección menos intenso que cuando se trata de la publicación de noticias de actualidad)[125]; y por otra, el respeto a los dere-

dentro do contexto de sociedade da informação", disponible en http://www.cidp.pt/publicacoes/revistas/ridb/2012/01/2012_01_0419_0434.pdf (consultado el 25/01/2017), consideran que "falta o estabelecimento de critérios temporais para a permanência de informações.".

[124] La necesidad de conciliar el "derecho al olvido" con la libertad de expresión y el derecho a la información está también presente en el art. 85 RGPD, cuyo apartado 1, establece: "Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria". A tal fin, indica el apartado 2, los Estados miembros establecerán exenciones o excepciones entre otras en el marco de los derechos del interesado en que se incardina precisamente ese derecho de supresión o "derecho al olvido".

[125] Trae a colación las STEDH de 10 de marzo de 2009 (caso Times Newpapers Ltd –nº 1 y 2- contra Reino Unido, párrafo 45) y de 16 de julio de 2003 (caso Wegrzynowski y Smolczewski contra Polonia, párrafo 59), en las que se afirma "que los archivos de Internet suponen una importante contribución para conservar y mantener noticias e información disponibles, pues constituyen una fuente importante para la educación y la investigación histórica, sobre todo porque son fácilmente accesibles al público y son generalmente gratuitos".

Ahora bien, -añade el TS- "la función que cumple la prensa en una sociedad democrática cuando informa sobre sucesos actuales y cuando ofrece al público sus hemerotecas es distinta y debe tratarse de modo diferente. Así lo ha hecho el TEDH, que ha considerado que mientras que la actividad de los medios de comunicación cuando transmiten noticias de actualidad es la función principal de la prensa en una democracia (actuar como un "perro guardián", en palabras de ese tribunal), el mantenimiento y puesta a disposición del público de las hemerotecas digitales, con archivos que contienen noticias que ya se han publicado, ha de considerarse como una función secundaria, en la que el margen de apreciación de que disponen los Estados para lograr el equilibrio entre derechos es mayor puesto que el ejercicio de la libertad de información puede considerarse menos intenso.

Internet es una herramienta de información y de comunicación que se distingue particularmente de la prensa escrita, principalmente en cuanto a su capacidad para almacenar y difundir información. Esta red electrónica, que comunica a millones de usuarios por todo el mundo, no está y posiblemente nunca estará sometida a las mismas reglas ni al mismo control que la prensa escrita, pues hace posible que la información sea accesible a millones de usuarios durante un tiempo indefinido. El riesgo de provocar daños

chos de la personalidad (fundamentalmente el derecho a la intimidad personal y familiar pero también el derecho al honor) cuando la información que aparece en el medio digital puede afectar negativamente a la reputación de la persona. Para llevar a cabo esa ponderación, el TS valora el potencial ofensivo que para los derechos de la personalidad tiene la información publicada y el interés público que puede suponer que esa información aparezca vinculada a los datos personales del afectado.

Siguiendo a la mejor doctrina, el Alto Tribunal precisa que el interés público viene a ser "el interés en formarse una opinión fundada sobre asuntos con trascendencia para el funcionamiento de una sociedad democrática" e indica que también podría entenderse justificado el tratamiento de los datos personales cuando los hechos concernidos y su vinculación con esas concretas personas presente un interés histórico. Tales circunstancias, sin embargo, no se dan en el supuesto enjuiciado: los demandantes no son personas de relevancia pública, y los hechos objeto de la información carecen de interés histórico en tanto que vinculados a esas personas[126]. Prosigue su argumentación, indicando que la publicidad general y permanente de la implicación de los demandantes en los hechos delictivos (algo que no sólo posibilitaba la editora del diario en su hemeroteca digital sino que lo potenciaba al utilizar los datos personales en la cabecera del código fuente y al emplear las instrucciones index y follow) "supuso un daño desproporcionado

en el ejercicio y goce de los derechos humanos y las libertades, particularmente el derecho al respeto de la vida privada, que representa el contenido y las comunicaciones en Internet, es sin duda mayor que el que supone la prensa escrita. Así lo ha entendido el TEDH en sus sentencias de 16 de julio de 2003, caso Wegrzynowski y Smolczewski contra Polonia, párrafo 58 , y 5 de mayo de 2011, caso Equipo Editorial de Pravoye Delo y Shtekel contra Ucrania , párrafo 63".

[126] El Tribunal reconoce que "los sucesos delictivos son noticiables por su propia naturaleza, con independencia de la condición de sujeto privado de la persona o personas afectadas por la noticia" (SSTC 178/1993, de 31 de mayo, FJ 4; 320/1994, de 28 de noviembre, FJ 5; 154/1999, de 14 de septiembre, FJ 4). "En general, reviste interés público la información tanto sobre los resultados de las investigaciones policiales, el desarrollo del proceso y el contenido de la sentencia, como sobre todos aquellos datos, aun no directamente vinculados con el ejercicio del "ius puniendi" [facultad sancionadora] del Estado, «*que permiten una mejor comprensión de su perfil humano o, más sencillamente, de su contexto vital*» de la persona que participa en el hecho delictivo" (STC 154/1999) y recuerda que él mismo (TS) en sus sentencias núm. 946/2008, de 24 de octubre (LA LEY 164137/2008), y 547/2011, de 20 de julio (LA LEY 186203/2011), ha entendido justificada la publicación de datos de identidad de los implicados en hechos delictivos. Ahora bien, -añade- "una vez publicada la noticia en los medios de prensa por el interés que supone su carácter actual, el tratamiento automatizado de los datos personales de los implicados en ella, vinculado a la información de manera que una consulta a través de los motores de búsqueda de Internet en la que se utilice como palabras clave esos datos personales (particularmente el nombre y apellidos) arroje como resultados destacados los vínculos a las páginas de la hemeroteca digital en las que aparezca tal información, va perdiendo su justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esas personas, carecen de interés histórico".

para el honor de las personas demandantes, al vincular sus datos personales con unos hechos que afectaban seriamente a su reputación, y para su intimidad, al hacer pública su drogodependencia en aquellas fechas, con tan solo introducir su nombre y apellidos en los motores de búsqueda de internet utilizados con más frecuencia". Y llega a la conclusión de que, aunque los hechos eran veraces y el tratamiento de los datos personales pudo cumplir los requisitos de calidad de los datos en fechas próximas al momento en que se produjeron y conocieron los hechos, "el paso del tiempo ha supuesto que el tratamiento de estos datos vinculados a hechos pretéritos sea inadecuado, no pertinente y excesivo para la finalidad del tratamiento".

De acuerdo con el planteamiento del TS, por tanto, el derecho al olvido cede ante las exigencias del derecho a la libertad de información cuando los hechos que se revelen presenten un interés específico para su divulgación. Ahora bien, el factor tiempo puede ser decisivo a la hora de inclinar la balanza del lado del derecho a la libertad de información y/o expresión o del lado del derecho al olvido: es posible que, en un primer momento, prime el derecho a la libertad de información, pero, transcurrido un determinado periodo de tiempo, deba prevalecer el derecho al olvido en la medida en que la información haya perdido la cualidad de noticiosa. "Con el transcurso del tiempo, cuando ya no se trata de una cuestión de actualidad o noticiable, y siempre y cuando ya no exista una razón que justifique una nueva divulgación de la información como noticia" -como explica TERWANGNE "el derecho al olvido anula el derecho a la información"[127]. Y eso es lo que sucede en el caso resuelto por la STS de 15 de octubre de 2015: el derecho al olvido de los demandantes prevalece sobre el derecho a la información del diario digital, puesto que habían transcurrido más de veinte años desde la primera publicación de la noticia en papel y los interesados carecían de relevancia pública. De no haber sido así, el TS tendría que haber resuelto a favor de la prevalencia del derecho a la información declarando improcedente derecho al olvido. Sólo habría dos supuestos en los que, pese al transcurso del tiempo, prevalecería el derecho a la información sobre el derecho al olvido: 1) aquel en que la noticia tuviera un interés histórico; 2) aquel en que los hechos se encontraran vinculados al ejercicio de la actividad pública por parte de una figura pública. Llegados a este punto, mostramos nuestro acuerdo con SELIGRAT GONZÁLEZ, quien considera que, transcurrido ese periodo de tiempo en virtud del cual la recogida de datos deja de cumplir con la finalidad informativa inicial, se puede seguir ejercitando el derecho a la información; ahora bien, ese ejercicio quedará limitado a dar divulgación del

[127] TERWANGNE, Cécile de, "Privacidad en internet y el derecho a ser olvidado/derecho al olvido", *Revista de Internet, Derecho y Política*, nº 13, febrero 2012, pág. 56.

hecho noticioso, no pudiendo aludir ya a los sujetos objeto de noticia. Para que esto ocurra, será necesario que las personas implicadas ejerciten su derecho de cancelación, pues, a su modo de ver, no corresponde al responsable de la recogida de datos analizar en qué momento pierde la noticia la finalidad legítima con que los recogió inicialmente[128].

Como hemos indicado anteriormente, la SAP de Barcelona recurrida en casación había estimado plenamente la demanda y había acordado, entre otros pronunciamientos, exigir a la editora del periódico la adopción de medidas tecnológicas para que la página web de su hemeroteca digital no pudiera ser indexada por los proveedores de servicios de internet. Pues bien, el TS considera correcta esa medida, pero no otras de las establecidas en la misma sentencia como, por ejemplo, la relativa a la eliminación de los datos personales del código fuente de la página web que contenía la noticia, suprimiendo los nombres y apellidos de los actores, no permitiendo siquiera que constasen sus iniciales. A juicio del Alto Tribunal, tal medida supone un sacrificio desproporcionado, por excesivo, del derecho a la libertad de información: "El llamado «derecho al olvido digital»" -afirma- "no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día". Considera también desproporcionado el sacrificio de la libertad de información que supone la adopción de medidas técnicas que impidan la indexación de los datos personales a efectos de su consulta por el motor de búsqueda interna de la web, pues esos motores de búsqueda internos de las hemerotecas digitales solo sirven para localizar la información contenida en el propio sitio web una vez que el usuario ha accedido al mismo y no son asimilables a los motores de búsqueda de Internet (Google, Yahoo...), los cuales permiten obtener el perfil completo con solo introducir el nombre de una persona. Con relación al pronunciamiento de la sentencia del Juzgado de Primera Instancia, asumido por la Audiencia Provincial, en el que se declara la ilicitud de la "difusión" de la noticia y condena al diario a cesar en su "difusión", puntualiza que se refiere única y exclusivamente al tratamiento de los datos personales incluidos en la noticia tal y como se está haciendo en la hemero-

[128] SELIGRAT GONZÁLEZ, Víctor Manuel, "El «derecho al olvido digital»...", *op. cit.*. Añade el autor que, aceptar que el responsable de los datos es quien debe examinar en qué momento se perdió la finalidad legítima con que se recogieron y trataron inicialmente los datos supondría un coste económico excesivo, pues, como manifiesta TERWANGNE, Cécile de, "Privacidad...", *op. cit.*, pág. 60, actualmente «se ha vuelto menos costoso almacenar los datos que eliminarlos o hacerlos anónimos». Pero, aun aceptando ese especial deber de vigilancia por parte del responsable de tratamiento de datos, seguiría existiendo un problema de concreción sobre el momento en que la noticia perdió su finalidad informativa y, por ende, el momento en que los interesados pueden solicitar la cancelación de su registro, lo que conduce nuevamente al análisis judicial de cada caso.

teca digital, esto es, permitiendo su indexación por los motores de búsqueda de Internet. El resto de los pronunciamientos se mantienen (la obligación del diario de instalar códigos o instrucciones en la página web que impidan la indexación y archivo de los datos personales de las personas demandantes en las bases de datos de los motores de búsqueda de Internet; la indemnización por los daños causados como consecuencia de la intromisión ilegítima en el honor y la intimidad por el tratamiento de los datos personales sin respetar las exigencias derivadas del principio de calidad de los datos, en lo relativo a su pertinencia, adecuación y proporción en relación a los fines para los que se hizo la recogida y el tratamiento de tales datos; y la prohibición de que en la publicación de cualquier noticia que se refiera a este proceso se incluyan datos que puedan identificar a las personas demandantes, como sus nombres, apellidos o iniciales)[129].

Expuesta la STS, conviene profundizar en el tema de la procedencia o no de la indemnización, pues una cosa es que se reconozca que el tratamiento de datos ha devenido ilegítimo por no cumplir con el requisito de la calidad de los datos y otra diferente pensar que, siempre que tal circunstancia se produzca, el interesado tendrá derecho a reclamar una indemnización que repare su honor o su intimidad[130]. Como pone de relieve la SAP de Barcelona de 17 de julio de 2014 (AC\2014\1661), "El incumplimiento de la normativa de protección de datos no implica automáticamente un daño o lesión indemnizable del afectado[131]"; para

[129] Coincidimos con MINERO ALEJANDRE, Gemma, "Tratamiento...", *op. cit.*, pág. 386 y 387, en que, si la reclamación se hubiera dirigido también contra el buscador, sólo habría tenido éxito la pretensión relativa a la eliminación de las referencias al diario en cuestión (El País) en las listas de resultados creados por los buscadores a partir del empleo de los nombres de los reclamantes como criterios de búsqueda. No se habría estimado, en cambio, la petición de borrado de los datos personales en la página web del tercero, pues "el posible tratamiento realizado por los buscadores se limita a producir el efecto de la citada híper-accesibilidad, sin que exista un control de los contenidos de las webs referidas en sus índices de resultados, más allá de la indexación automática de éstas cuando no cuenten con medidas que la impidan".

[130] Refiriéndose a algunos casos que se han dado en Brasil, concretamente al Chacina da Candelária (REsp 1334097/RJ), MARQUES WOHJAN, Bruna y WISNIEWSKI, Alice "Direito ao esquecimento...", *op. cit.*, señalan que "O STJ entendeu que o réu condenado ou absolvido pela prática de um crime tem o direito de ser esquecido, pois se a legislação garante aos condenados que já cumpriram a pena o direito ao sigilo da folha de antecedentes e a exclusão dos registros da condenação no instituto de identificação (art. 748 do CPP), logo, com maior razão, aqueles que foram absolvidos não podem permanecer com esse estigma, devendo ser assegurado a eles o direito de serem esquecidos". El interesado en cuestión, en este caso, era un hombre que había sido denunciado pero había quedado absuelto y años más tarde vio como un programa de TV mostraba su nombre como el de una de las personas implicadas en los crímenes. El Tribunal entendió que efectivamente tenía derecho al olvido y que el programa podía retransmitirse sin mostrar el nombre y la fotografía del hombre que quedó absuelto. Dado que el programa se había retransmitido, concedió al interesado la indemnización correspondiente.

[131] En este caso, el interesado había sido condenado por un delito contra la salud pública cometido en 1981 y había sido posteriormente indultado. El indulto de la pena privativa de libertad pendiente de

poder recibir una indemnización, el demandante tendrá que demostrar, por tanto, – una vez ejercitado el derecho al olvido directamente ante el responsable del tratamiento o indirectamente ante la AEPD – que se ha producido un daño efectivo, bien en su honor, bien en su intimidad o bien en ambos. Esta resolución es muy ilustrativa pues diferencia perfectamente entre el plano administrativo y el civil-indemnizatorio: la reclamación que eventualmente pueda realizarse ante la AEPD es distinta de la reclamación en concepto de daños y perjuicios; para que proceda esta última es necesario que se produzca un incumplimiento del responsable o encargado del tratamiento de datos personales y que dicho incumplimiento haya causado un daño indemnizable[132].

En el caso resuelto por la STS 15 de octubre de 2015, observamos que el Alto Tribunal entiende que "la publicidad general y permanente de la implicación

cumplimiento, a la que había sido condenado en STS, Sala 2ª, de18 de enero de 1990, se publicó en el BOE de 18 de septiembre de 1999. Se había dirigido al BOE (en Enero de 2009) solicitando la retirada de sus datos pues, cuando realizaba una búsqueda en Google con su nombre y apellidos aparecía la página del BOE informando del indulto.(afirmaba que habían hundido su vida y que quería rehacerla). El BOE había contestado indicando, entre otras cosas: 1) que la página electrónica del BOE reproduce fielmente la edición en papel, por lo que cualquier modificación sobre la página significaría una manipulación sustancial del contenido que alteraría de forma grave una "fuente de acceso público"; 2) que había adoptado las medidas a su alcance necesarias para evitar la automatización de sus datos personales (había eliminado su nombre del buscador del BOE, de modo que ya no era posible acceder a la disposición citada a través del nombre en ninguno de los buscadores de la web del BOE) y los documentos en que aparecía el nombre del actor habían sido incluidos en una lista de exclusión (robots.txt), para notificar a las empresas con buscadores en Internet que no debían utilizar esos datos, los cuales, en unos días, debían desaparecer de los buscadores de Internet. En marzo de 2009, se dirige frente a Yahoo y frente a Google indicando que, desde hacía años, en su buscador, cuando se insertaba el nombre del actor y el motor realizaba la búsqueda, aparecían varias páginas ilegales -no hacía referencia ya a la página del BOE- en las cuales se informaba de su vida pasada (1981, 1999), incumpliendo muchos artículos de la Ley de protección de datos, lo que perjudicaba al demandante en lo personal, familiar, laboral, económico y social, de manera desmesurada y en prácticamente todos los países del mundo, saliendo siempre en la primera página del buscador; solicitaba que retiraran las páginas del buscador y reclamaba una compensación -que no cuantificaba- por los daños sufridos. Google contestó con una respuesta estándar automatizada remitiéndole a los Help Center y Yahoo, por su parte, contestó solicitando determinada información que no consta fuera remitida por el actor. Con posterioridad, se había dirigido a la AEPD, Google Madrid y a Telefónica; esta última contestó diciendo que los datos personales (nombre y apellidos) del Sr. En cuestión no aparecían cuando se realizaba una búsqueda en la página de Terra y adjuntaba una copia de pantalla. Posteriormente reclamó ante la AEPD contra Lycos España y Telefónica España. La AEPD estimó en distintas resoluciones la reclamación contra Google, Yahoo y Telefónica; no así la realizada contra Lycos.

[132] La AEPD, además, no es competente para conocer de la indemnización. De acuerdo con lo dispuesto en el art. 19 LOPD, relativo al *"Derecho a indemnización"*:

1. *"Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.*
2. *Cuando se trata de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.*
3. *En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria".*

del interesado en aquellos hechos (...) supuso un daño desproporcionado para el honor de las personas demandantes, al vincular sus datos personales con unos hechos que afectaban seriamente a su reputación, y para su intimidad, al hacer pública su drogodependencia en aquellas fechas, con tan solo introducir su nombre y apellidos en los motores de búsqueda de Internet utilizados con más frecuencia". Sin embargo, hemos de llamar la atención sobre varias cuestiones:

1) Tras señalar que la acción no ha caducado, el TS en esta Sentencia afirma que nos encontramos ante un supuesto de daños continuados. Trae a colación, a estos efectos, sus sentencias nº 899/2011, de 30 de noviembre, 28/2014, de 29 de enero, y 307/2014, de 4 de junio, en las indica que los daños producidos por el tratamiento de los datos personales que no cumpla los requisitos previstos por el Ordenamiento jurídico, tienen naturaleza de daños continuados "y que el plazo para el ejercicio de la acción de protección de los derechos del afectado por el tratamiento ilícito de datos personales no se inicia en tanto el afectado no tenga conocimiento del cese de dicho tratamiento". Pues bien, ¿significa esto que, en todos aquellos casos en que se deniegue la cancelación de los datos, no empezará a correr la acción para reclamar daños y perjuicios?; dicho con otras palabras, dado que el daño sigue produciéndose, ¿la acción no caducará nunca? Para autores como SELIGRAT GONZÁLEZ, semejante postura resulta excesiva; a su modo de ver, el plazo de caducidad de 4 años para reclamar la indemnización por daños al honor o la intimidad debe empezar a computarse desde el momento en que el perjudicado ejercita su derecho de cancelación y oposición a los datos con base en la LOPD y recibe una respuesta negativa por parte del sujeto encargado del tratamiento de los datos personales; y, en caso de no obtener respuesta, el plazo debe computarse una vez transcurridos los diez días con que cuenta el responsable del tratamiento, según el art. 16.1 LOPD, para cumplir con el derecho de rectificación o cancelación del interesado[133].
2) La segunda cuestión viene ligada a la anterior: ¿cuándo se produce efectivamente el daño a efectos del cálculo indemnizatorio? Si como venimos diciendo, ante la inexistencia de previsión legal específica, hoy por hoy, no puede imponerse un deber de vigilancia de los diarios digitales sobre el momento en que la información recogida en su página web pierde la legitimidad con que contaba en su origen, el daño no puede entenderse producido en el momento en que el interesado puede ejercitar su derecho

[133] SELIGRAT GONZÁLEZ, Víctor Manuel, "El «derecho al olvido digital»...", *op. cit.*.

al olvido por dicho motivo (pérdida de la finalidad legítima de la información); debe entenderse producido en el instante mismo en que el interesado ejercita efectivamente su solicitud de cancelación de los datos y la ve denegada[134]. La cuestión no es baladí: la determinación del momento en que se produce el daño es clave para calcular la cuantía de la indemnización a que, en su caso, pueda haber lugar. A partir de este momento deberá tomarse en consideración, por ejemplo, el grado de divulgación de los datos[135]. Ahora bien, como decíamos, el interesado tendrá que acreditar que efectivamente ha sufrido un perjuicio. Así se infiere de SAP Barcelona de 17 de julio de 2014 (AC\2014\1661) cuando afirma que "No existe en materia de protección de datos la presunción de existencia de perjuicio por la intromisión ilegítima, del art. 9.3 LO 1/1982"; no basta, por tanto, con que el interesado solicite la cancelación de los datos y el responsable de su tratamiento se niegue a retirarlos; el daño no se entiende producido de manera automática. Ahora bien, tratándose de los datos especialmente protegidos a que se refiere el art. 7 LOPD (por ej. los relativos a las infracciones penales), convenimos con SELIGRAT GONZÁLEZ en que, aunque no pueda aplicarse la presunción del art. 9.3 LO 1/1982, debería presumirse que el daño se genera con la denegación por parte del responsable de la solicitud de cancelación[136]. Lo que no plantea ninguna duda es la aplicación de los criterios contemplados en el art. 9.3 LO 1/1982 a la hora de cuantificar el daño moral; esos criterios – que se presentan como orientativos – son: las circunstancias del caso, la gravedad de la lesión efectiva-

[134] Mostramos nuestro acuerdo en este punto con SELIGRAT GONZÁLEZ, Víctor Manuel, "El «derecho al olvido digital»...", *op. cit.*. Nótese que el derecho al olvido podría ejercitarse directamente ante el responsable del tratamiento de los datos o indirectamente, a través de la AEPD, en cuyo caso la fecha que deberíamos tomar como referencia sería aquella en que el referido órgano trasladara la petición al responsable del tratamiento de los datos. En el supuesto resuelto por la SAP de Barcelona de 17 de julio de 2014, la AEPD no sólo había dado traslado de la solicitud de cancelación de los datos al responsable de su tratamiento sino que había entendido que efectivamente procedía la cancelación y había instado al responsable en cuestión a adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos; por eso, entiende que es la notificación de la resolución de la AEPD al responsable la que "marca el momento en que el mantenimiento del resultado controvertido en el índice del buscador deviene incumplimiento culpable de las normas legales de protección de datos. Con la lectura de la resolución motivada de la AEPD", el responsable "debía conocer la antijuricidad de su actuación".

[135] Véase, a estos efectos, el art. 9.3 LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, según el cual: *"La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral, que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido".*

[136] Así lo defiende SELIGRAT GONZÁLEZ, Víctor Manuel, "El «derecho al olvido digital»...", *op. cit.*.

mente producida, y especialmente, tanto la difusión o audiencia del medio a través del que se haya producido como el beneficio que haya obtenido el causante de la lesión como consecuencia de la misma[137].

3) La STS confirma la condena de instancias inferiores en lo relativo a la obligación del diario digital encargado del tratamiento de los datos de instalar códigos o instrucciones en su página web destinados a impedir la indexación y archivo de los datos personales en otras bases de datos de los motores de búsqueda más conocidos en internet, revoca la condena impuesta al diario en cuestión relativa a la eliminación de tales datos también en la propia base de datos de la página web del diario digital y concede a los demandantes una indemnización por daños a su derecho al honor e intimidad. Para SELIGRAT GONZÁLEZ, resulta incongruente que se estime la existencia de una vulneración del honor e intimidad de los sujetos que ejercitan su derecho al olvido, cuando el «olvido» de los datos se limita únicamente a que no aparezcan en lo sucesivo en el motor de búsqueda de los principales buscadores de internet, permitiendo que continúen apareciendo en el buscador interno de la página web del periódico que tiene registrados tales datos. A su juicio, la vulneración del derecho al honor e intimidad de los demandantes persiste; la única diferencia es que, ahora,

[137] La STS de 22 de enero de 2014 (Roj: STS 355/2014), conociendo de un caso en que se habían incluido los datos de una persona en un registro de morosos sin cumplirse los requisitos establecidos por la LOPD, considera indemnizable, como daño moral: 1) "la afectación a la dignidad en su aspecto interno o subjetivo, y en el externo u objetivo relativo a la consideración de las demás personas. Para calibrar este segundo aspecto ha de verse la divulgación que ha tenido tal dato, pues no es lo mismo que sólo hayan tenido conocimiento los empleados de la empresa acreedora y los de las empresas responsables de los registros de morosos que manejan los correspondientes ficheros, a que el dato haya sido comunicado a un número mayor o menor de asociados al sistema que hayan consultado los registros de morosos"; 2) "el quebranto y la angustia producida por el proceso más o menos complicado que haya tenido que seguir el afectado para la rectificación o cancelación de los datos incorrectamente tratados".
La STS de 24 de abril de 2009 (Roj: STS 2227/2009), en un supuesto similar, declaró que la inclusión de una persona, ciudadano particular o profesionalmente comerciante, en este tipo de registros "afecta directamente a su dignidad, interna o subjetivamente, e igualmente le alcanza, externa u objetivamente, en la consideración de los demás, ya que se trata de un imputación de un hecho consistente en ser incumplidor de su obligación pecuniaria que, como se ha dicho, lesiona su dignidad y atenta a su propia estimación, como aspecto interno, y menoscaba su fama, como aspecto externo". Según el Alto Tribunal resulta intrascendente que el registro haya sido consultado por terceras personas o no, ya que "basta la posibilidad de conocimiento por un público, sea o no restringido, y que esta falsa morosidad haya salido de la esfera interna del conocimiento de los supuestos acreedor y deudor, para pasar a ser de una proyección pública. Si, además, es conocido por terceros y ello provoca unas consecuencias económicas (como la negación de un préstamo hipotecario) o un grave perjuicio a un comerciante (como el rechazo de la línea de crédito) sería indemnizable, además del daño moral que supone la intromisión en el derecho al honor" y que impone el art. 9.3 LPDH.

la divulgación y accesibilidad a la noticia presuntamente atentatoria contra tales derechos es mucho menor. A su modo de ver, si se considera que una noticia veraz y exacta vulnera los derechos al honor y a la intimidad por el mero transcurso del tiempo[138] aunque ninguna disposición indique que dicho lapso temporal genera por sí mismo un perjuicio a las personas noticiosas[139], debe igualmente entenderse que dichos derechos se quebrantan tanto cuando se accede a la información a través de los buscadores populares de internet como cuando se accede desde el buscador interno de la página web concreta que divulgó la noticia inicialmente. "Si se estima la cancelación", – concluye – "debe hacerse a todos los niveles"[140]. Desde nuestro punto de vista, olvida el autor que es preciso cohonestar el derecho a la información con el derecho al honor y la intimidad. Está claro que el diario, cuando – acomodándose a los nuevos tiempos y haciendo uso de las nuevas tecnologías- digitaliza la noticia y facilita el acceso a la misma a través de la hemeroteca digital, está satisfaciendo un interés público: el derecho de todos los ciudadanos a acceder a la información. Las hemerotecas, también las digitales – como pone de relieve el TS en la sentencia que estamos comentando –, están protegidas por la libertad de información[141]; pues bien, si nadie discute la posibilidad de consultar una noticia que se publicó hace veinte años en una hemeroteca que conserva los periódicos en papel, ¿por qué vamos ahora a eliminar la posibilidad de realizar esa misma consulta on line en la hemeroteca digital del diario de que se trate? ¿Consideramos que aquella publicación en papel vulnera el derecho al honor y, en consecuencia, destruimos el ejemplar físico en que se plasmaba? Si la respuesta es negativa, ¿por qué habría de vulnerarlo el mantenimiento de

[138] Recordemos que él no comparte esa posición que defiende la STS; en su opinión, el daño se produce desde la reclamación sin éxito de la cancelación de datos por el interesado.
[139] En el caso de las personas morosas, como hemos indicado ya, el art. 29 LOPD fija un plazo de máximo 6 años para el tratamiento de datos relacionados con la solvencia económica; transcurrido ese plazo, sí podría entenderse que se ha producido un daño.
[140] SELIGRAT GONZÁLEZ, Víctor Manuel, "El «derecho al olvido digital»...", *op. cit.*.
[141] Conviene recordar en este punto –y así lo hace nuestro TS en la sentencia que comentamos- que, según el TEDH, la protección de las hemerotecas digitales por el art. 10 del Convenio para la Protección de Derechos y Libertades Fundamentales de 1999 implica que las noticias pasadas contenidas en ellas no pueden ser eliminadas aunque su contenido pueda afectar a los derechos de las personas. La libertad de expresión protege el interés legítimo del público en acceder a los archivos digitales de la prensa, de modo que «no corresponde a las autoridades judiciales participar en reescribir la historia». Véase la STEDH de 16 de julio de 2013, caso Wergrzynowski y Smolczewski c. Polonia (JUR 2013/252862), párrafo 65, en la que se cita también la STEDH de 10 de marzo de 2009, caso Times Newpapers Ltd -núms. 1 y 2- contra Reino Unido (JUR 2009\100304).

dicha noticia en la hemeroteca digital tal y como fue publicada en su día? La reflexión aquí nos lleva a la mayor o menor dificultad que el ciudadano puede encontrar para localizar la noticia en cuestión. Para acceder a la información deseada en una hemeroteca clásica, tendríamos que desplazarnos hasta allí y probablemente tendríamos que buscar en distintos ejemplares a partir de una fecha aproximada, pero encontraríamos la información tal y como se publicó; en una hemeroteca digital, la búsqueda puede realizarse desde cualquier ordenador con conexión a la red y, sin lugar a dudas, de una forma mucho más rápida y eficaz, pues cuenta con un motor de búsqueda que permite acceder a la información deseada de una forma muy sencilla, información que – a nuestro modo de ver- debe aparecer tal y como se publicó en su momento. La cuestión, por tanto, reside en definir los términos en que puede llevarse a cabo esa búsqueda en la hemeroteca digital, a fin de que el nuevo tratamiento de datos que supone la digitalización de la noticia muchos años después de sucedidos los hechos en ella narrados no entrañe una intromisión en el derecho al honor de la persona. Lo que vulnera el derecho al honor, a nuestro modo de ver, no es la noticia en sí (veraz y exacta) sino la forma en que se tratan posteriormente los datos personales. Es en este punto en el que diferimos del planteamiento de la Sentencia, por cuanto entendemos que sí debería haberse mantenido la condena relativa a la adopción de medidas técnicas que impidieran la indexación de los datos personales a efectos de su consulta por el motor de búsqueda interna de la web. Ciertamente, la repercusión que tiene el tratamiento de los datos personales por parte del motor de búsqueda interno de la web del diario es mucho menor que la que lleva consigo el tratamiento por parte de los motores de búsqueda de Internet pues, a diferencia de estos, aquel no permite la obtención de un perfil completo del interesado[142]; no obstante, si lo que viene a afirmar el TS es que el tratamiento de los datos personales no cumple con los principios de calidad debido al transcurso de ese largo lapso de tiempo, no resulta admisible que establezca una diferenciación de trato en función del tipo de motor de búsqueda; no en vano, la desindexación de los datos personales en el motor de búsqueda interno no conlleva la desaparición de

[142] Como indicaba el TJUE en su Sentencia de 13 de mayo de 2014 el contenido publicado por el editor puede seguir siendo legal con el paso del tiempo; es su difusión universal a través del buscador, unido a la información adicional que facilita sobre el mismo individuo cuando se busca por su nombre, lo que tiene un impacto desproporcionado sobre su privacidad.

la información; eso sí, supondrá que la búsqueda debe realizarse a través de parámetros distintos[143].

Con todo, la cuestión no es fácil de determinar especialmente cuando hablamos de noticias relativas a la comisión de delitos graves: ¿cuándo deviene ilícito el tratamiento de los datos? El problema, en el fondo, es nuevamente el mismo: ¿cuál es la función que desempeñan los buscadores de internet y cuál es la función que desempeña el buscador interno de la hemeroteca digital? ¿Cuáles son las dimensiones que adquiere la noticia con las nuevas tecnologías? ¿Hemos de privar al diario de la utilización de las nuevas tecnologías en la Sociedad de la Información? Evidentemente, la respuesta es no: simplemente hay que adaptar el ejercicio de los derechos a las necesidades que marcan los nuevos tiempos.

3.3. ¿Podría ejercitar el derecho al olvido el heredero/apoderado digital?

En los últimos meses, se ha presentado un proyecto de ley sobre herencia digital en Cataluña[144]. Hoy por hoy, cuando una persona fallece suele dejar tras de sí un legado digital (cuentas en redes sociales, colecciones de libros digitales..., por ejemplo), lo que hace imprescindible afrontar un nuevo problema: ¿cómo morir digitalmente? Dado que Cataluña no tiene competencias en materia de telecomunicaciones y protección de datos, la referida Comunidad Autónoma pretende modificar el CCCat en orden a regular la figura del heredero/apoderado digital[145]; se pretende, así, amparar a todos aquellos familiares que reclamen el

[143] En esta línea discurre también el pensamiento de Di Pizzo Cittacchio, Adrián "Efectos...", *op. cit.*, pág. 951-952, quien afirma que, cuando el Pleno asume que existe una diferencia sustancial entre la búsqueda de información mediante motores de búsqueda internos y externos y equipara la realizada por los primeros a la antes realizada en las hemerotecas físicas, está obviando que la consulta en estos casos se lleva a cabo a través de los datos personales de la persona física, lo cual no era posible en las hemerotecas físicas. Prosigue su argumentación alegando que la desindexación en el motor de búsqueda interno no supone la desaparición de la información, la cual continuaría estando accesible si bien su localización se restringiría a parámetros de búsqueda distintos de los datos personales de los interesados, y que la desvinculación de los hechos a los datos personales sólo tendría lugar a efectos de la búsqueda. El carácter ilícito de los datos –concluye- no puede hacerse depender de la naturaleza del motor de búsqueda en que se efectúe la misma.

[144] "Projecte de llei sobre les voluntats digitals i de modificació dels llibres segon i quart del Codi civil de Catalunya", disponible en http://www.parlament.cat/document/antecedents/201433.pdf (consultado el 1-03/2017).

[145] Sobre este proyecto puede verse LLOPIS, José Carmelo "Proyecto sobre herencia digital el Catalunya" en http://www.notariallopis.es/blog/i/1386/73/proyecto-sobre-herencia-digital-el-catalunya (consultado el 21/02/2017).

control de las cuentas sociales (y cualquier contenido que esté tras las credenciales de un servicio online) de un pariente fallecido. Además, se contempla la creación de un "Registro de Voluntades Digitales"; ahí es donde los catalanes podrán designar a un heredero de sus perfiles, propiedades digitales y cuentas sociales, dejando la posibilidad de hacerlo por notario como algo opcional. Llegados a este punto, podemos formularnos una pregunta a la que el proyecto en cuestión no da respuesta: ¿estará legitimado el heredero digital para ejercitar el derecho al olvido del causante cuando los datos publicados vulneren en alguna medida su derecho al honor? Desde nuestro punto de vista, a la vista de lo previsto en el art. 4 LO 1/1982, de protección jurídica de los derechos al honor, la intimidad y la propia imagen, la respuesta bien podría ser afirmativa. No en vano dicho precepto legitima para ejercitar las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida a quien ésta haya designado a tal efecto en su testamento (puede ser una persona jurídica), y, en caso de que no haya designado a nadie o la persona designada haya fallecido también, al cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento[146].

4. Conclusiones

Es imprescindible formar o alfabetizar al usuario de internet, pues sólo así se podrá valorar si presta o no su consentimiento previamente y si conoce o no sus derechos en orden a poder ejercerlos en el Universo 3.0[147].

Aunque cada solicitud debe ser analizada de forma individual, conviene contar con unos criterios comunes que permitan evaluar cuándo procede estimar o denegar los derechos de cancelación u oposición, en general, y el derecho al olvido, en particular. A nuestro modo de ver, no está claro, por ej., cuándo deviene ilícito el tratamiento de los datos por el transcurso del tiempo. Asimismo, convendría que la jurisprudencia española unificara el criterio para determinar quién es el responsable del tratamiento.

Los buscadores sólo pueden advertir a los usuarios de que la información que muestran puede no estar completa si dicha advertencia no pone de relieve el ejercicio del derecho al olvido por parte de la persona en cuestión.

[146] Continúa diciendo este precepto:
Tres. "A falta de todos ellos, el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal, que podrá actuar de oficio a instancia de persona interesada, siempre que no hubieren transcurrido más de ochenta años desde el fallecimiento del afectado. El mismo plazo se observará cuando el ejercicio de las acciones mencionadas corresponda a una persona jurídica designada en testamento.
Cuatro. En los supuestos de intromisión ilegítima en los derechos de las víctimas de un delito a que se refiere el apartado ocho del artículo séptimo, estará legitimado para ejercer las acciones de protección el ofendido o perjudicado por el delito cometido, haya o no ejercido la acción penal o civil en el proceso penal precedente. También estará legitimado en todo caso el Ministerio Fiscal. En los supuestos de fallecimiento, se estará a lo dispuesto en los apartados anteriores".

[147] En este sentido se manifiesta también López Portas, Begoña, "La protección...", *op. cit.*, pág. 296.