MÁSTER UNIVERSITARIO EN ACCESO A LA PROFESIÓN DE ABOGADO POR LA UNIVERSIDAD DE CANTABRIA

(EN COLABORACIÓN CON EL ILUSTRE COLEGIO DE ABOGADOS DE CANTABRIA)

TRABAJO FIN DE MÁSTER

CURSO ACADÉMICO 2020-2021

TÍTULO

LA CONFIGURACIÓN JURÍDICA DEL DERECHO AL OLVIDO DIGITAL

WORK TITLE

THE LEGAL CONFIGURATION OF THE RIGHT TO BE DIGITALLY FORGOTTEN

AUTORA

LAURA BARROS GONZÁLEZ

DIRECTOR/A:

JOSE IGNACIO SOLAR CAYÓN

ÍNDICE

INTRODUCCIÓN

El vigente Reglamento General de Protección de Datos (RGPD), normativa europea directamente aplicable y con plenos efectos desde el 25 de mayo de 2018, ha supuesto un importante reconocimiento y avance en aras de reforzar la protección de datos personales en el ámbito de la Unión Europea. En este sentido, se establece un marco regulatorio común y uniforme, directamente aplicable y que a su vez podrá ser completado por cada Estado miembro. No obstante, cumple admitir que se trata de una temática compleja, y sobre todo en atención a los importantes retos jurídicos que aún plantean los entornos tecnológicos y medios digitales de comunicación a través de la Red. En este contexto temático e instrumental, una de las cuestiones que adquieren mayor interés, es la relativa a la delimitación funcional y operativa del "derecho a olvido". Es por ello que en el presente TFM se analiza su actual configuración doctrinal, con base en el análisis de destacados pronunciamientos en la materia, especialmente del Tribunal de Justicia de la Unión Europea, y asimismo su incorporación positiva en el RGPD y en la posterior aprobación de la LOPDGDD. Para lo que resulta del todo necesario hacer una previa consideración del derecho de protección de datos, dentro del cual se enmarca el derecho al olvido, y esa necesidad radica precisamente en que el derecho al olvido, como ha señalado el TC en la Sentencia 58/2018, de 4 de junio, es una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4. CE), y es también un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo.

I. MARCO LEGAL DEL DERECHO A LA PROTECCIÓN DE DATOS

Con carácter previo a abordar el derecho al olvido resulta necesario hacer unas consideraciones sobre el derecho a la protección de datos, y esa necesidad radica precisamente en que el derecho al olvido, como ha señalado el TC en la Sentencia 58/2018, de 4 de junio[1], es una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4. CE), y es también un mecanismo de garantía

[1] Sentencia TC 58/2018, de 4 de junio. Disponible en: https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25683

para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo. Es por ello que se va a analizar el marco legal de la protección de datos, dentro del cual se enmarca el derecho al olvido, resultando para ello necesario analizar parte del acervo jurisprudencial que existe al respecto y que ha asentado el concepto de derecho fundamental a la protección de datos, así como su delimitación del mencionado derecho a la intimidad.

El derecho a la protección de datos se encuentra regulado en nuestro ordenamiento jurídico en la Constitución Española, en el Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

1. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN ESPAÑOLA

El punto de partida tiene que ser la Constitución Española, concretamente el artículo 18.4, que dispone lo siguiente:

"*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*."

El Tribunal Constitucional ha sido el encargado de sentar una línea jurisprudencial respecto a este precepto para terminar por definir lo que se entiende por derecho a la protección de datos de carácter personal y darle un estatus de derecho fundamental. Lo que ha sucedido de una forma gradual y nivelada, partiendo de un primer concepto, la libertad informática, entendida como un derecho perteneciente al círculo de la intimidad, para terminar por reconocer el derecho a la protección de datos como un derecho, cuya tutela, como afirma PEREZ LUÑO, en tanto derecho constitucional únicamente es posible garantizar de forma efectiva afirmando su consolidación como un derecho autónomo respecto de la intimidad[2].

[2] PÉREZ LUÑO, A.E. "Nuevos derechos fundamentales de la era tecnológica: la libertad Informática". *Anuario de Derecho Público y Estudios Políticos,* nº 2, 1989, p.187.

La primera de las sentencias que se encarga de hacer una aproximación al derecho a la protección de datos personales es la *Sentencia número 254/1993*[3]:

Dispone el art. 18.4 C.E. que "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 este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un ***uso ilegítimo del tratamiento mecanizado de datos****, lo que la Constitución llama "la informática".*

Es la primera resolución del TC que entra a analizar como cuestión de fondo la interpretación del apartado 4 del artículo 18 CE, por ello su importancia es capital. Como señala SÁNCHEZ-ESCRIBANO, el TC, en la misma, de una forma absolutamente pionera, apunta hacia una doble dimensión en la interpretación de dicho apartado: afirma que contiene, por una parte, un instituto de garantía de otros derechos y, por otra, un derecho o libertad fundamental que denomina libertad informática. Sin llegar todavía a reconocer la libertad informática como un derecho autónomo, configurándola como una manifestación del derecho a la intimidad[4].

Respecto a la primera dimensión, afirma que la libertad informática constituye la cláusula de salvaguarda principalmente del derecho a la intimidad y al honor, que surge como respuesta a una nueva forma de amenaza a la dignidad y a los derechos de la persona, en idéntica forma a como fueron originándose e incorporándose históricamente los distintos derechos.

En cuanto a la segunda dimensión, sienta las bases del contenido mínimo provisional, que concreta en dos aspectos: uno negativo, según el cual el uso de la informática encuentra

[3] Sentencia número 254/1993 de 20 de julio de 1993 del Tribunal Constitucional.
[4] SÁNCHEZ-ESCRIBANO, M.M. "Libertad informática y protección de datos: desarrollo en la jurisprudencia del tribunal constitucional y tutela penal en el delito de descubrimiento y revelación de secretos". *Anuario Iberoamericano de Justicia Constitucional,* nº19, 2015, p.338.

un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos, y otro positivo, que se expresa en la forma de derecho de control sobre los datos relativos a la propia persona y que denomina *habeas data*[5].

Tal y como apunta SÁNCHEZ-ESCRIBANO, la relevancia de esta sentencia es extrema, puesto que no solo contiene la primera referencia en la jurisprudencia constitucional a la libertad informática, sino que reconoce la existencia de un nuevo derecho fundamental. Aunque ello supone un paso indudablemente sustancial —un nuevo derecho tiene ahora nombre propio: libertad informática—, el Tribunal no observa raíces suficientes para afirmar la autonomía de este derecho y asienta su contenido sobre el derecho a la intimidad[6].

Por su parte, el análisis pormenorizado de la *Sentencia número 292/2000* resulta especialmente relevante. En primer lugar, porque dicha sentencia supuso el nacimiento jurisprudencial del derecho a la protección de datos. En segundo lugar, por ser la primera Sentencia en este ámbito que se pronuncia acerca de muchos de los términos relacionados con el derecho a la protección de datos (su alcance, contenido y características entre otros). Y, por último, y en mi opinión más importante, porque es la Sentencia que se encarga de reconocer el estatus de derecho fundamental del derecho a la protección de datos.

En la mencionada Sentencia el TC, haciéndose eco de lo establecido al respecto por el Tribunal Constitucional de la República Federal de Alemania[7], cataloga al derecho de protección de datos como el derecho fundamental de *autodeterminación informativa*, definiéndose esta por el mencionado Tribunal Alemán como el derecho fundamental a decidir el grado de participación de los demás en los actos y pensamientos propios así como para determinar la divulgación y utilización de sus datos personales, que se encuentra regulado, como ya se ha indicado, en el artículo 18.4 de la Constitución Española[8].

---

[5] El TC en la citada sentencia 254/1993, Fundamento Jurídico 7, determina que la llamada "libertad informática" también se concreta en el derecho a controlar el uso de los mismos datos insertos en un programa informático, lo que denomina "habeas data".

[6] SÁNCHEZ-ESCRIBANO, M. M., "Libertad informática y protección de datos: desarrollo en la jurisprudencia del tribunal constitucional y tutela penal en el delito de descubrimiento y revelación de secretos", cit., p. 339.

[7] Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo sobre el derecho a la autodeterminación informativa.

[8] Antecedente Segundo STC 292/2000, de 30 de noviembre de 2000.

Respecto al contenido del derecho fundamental a la protección de datos, el Tribunal Constitucional se pronuncia en los siguientes términos:

> *"El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos."*

El Tribunal Constitucional determina en el Fundamento Jurídico Séptimo cuáles son los derechos con los que cuenta *el afectado* respecto de sus datos personales, lo que supone la delimitación del alcance del mismo:

- Derecho a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.
- Derecho a ser informado de quién posee sus datos personales y con qué fin.
- Derecho a oponerse a esa posesión y uso, requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.

Se reconoce por parte del Tribunal Constitucional el derecho a la protección de datos como un derecho independiente al delimitarse del derecho a la intimidad:

> *"Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz*

protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran."

Establece que la garantía de la vida privada de la persona y de su reputación poseen una dimensión que excede al ámbito propio del derecho fundamental a la intimidad, reconocido en el art. 18.1 CE, y que se traduce en el derecho de control sobre los datos relativos a la propia persona. La libertad del individuo se traduce en el derecho a controlar el uso de los datos personales, y comprende entre otros aspectos, como ya se ha señalado, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

El derecho a la intimidad, como derecho fundamental, protege frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, para impedir su tráfico ilícito y lesivo para su dignidad y derecho como afectado.

En definitiva, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno y el derecho a la protección de datos garantiza a los individuos el poder de disposición sobre sus datos.

Como señala RALLO LOMBARTE, el TC, al establecer el carácter independiente y autónomo del derecho, garantiza no solo un ámbito de protección específico del derecho a la protección de datos de carácter personal, sino también un ámbito más idóneo —que el que podían ofrecer, por sí mismos, los derechos fundamentales al honor, a la intimidad

y a la propia imagen reconocidos en el artículo 18 CE— ante la eclosión de nuevos peligros que las nuevas tecnologías pueden suponer[9].

2. DERECHO A LA PROTECCIÓN DE DATOS EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

En este ámbito de la Unión Europea el derecho a la Protección de Datos se encuentra garantizado en la Carta de Derechos fundamentales de la Unión Europea que lo reconoce en su artículo 8:

> *"Protección de datos de carácter personal.*
>
> *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *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 le conciernan y a obtener su rectificación.*
>
> *El respeto de estas normas estará sujeto al control de una autoridad independiente."*

El RGPD es el marco común de la Unión Europea en lo que respecta a la protección de los datos personales. Contiene normas relativas a la protección de datos de carácter personal, tanto desde el punto de vista de los derechos que tienen en este ámbito las personas físicas como de las obligaciones que tienen las personas y las entidades que tratan datos de carácter personal.

Atendiendo a lo que establece su artículo 1, el objeto del Reglamento es establecer *"normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos".*

[9]RALLO LOMBARTE, A. "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)". UNED, *Revista de derecho político,* nº100, 2017, p. 652.

Para determinar el ámbito de aplicación del RGPD deben tenerse en cuenta los artículos 2 y 3 del mismo, que establecen los ámbitos de aplicación material y territorial, respectivamente.

En relación con el **ámbito de aplicación material**, el mismo se tiene que abordar desde dos vertientes: una positiva y una negativa.

Desde una vertiente positiva, el artículo 2 establece que el Reglamento será de aplicación 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. Ha sido la jurisprudencia la que se ha encargado de perfilar cuándo los tratamientos de datos no automatizados quedan comprendidos dentro del ámbito de aplicación del RGPD.

La Audiencia Nacional ha señalado en reiteradas ocasiones -se cita al efecto la Sentencia de la Audiencia Nacional, Sección Primera, de 9 de julio de 2007- que "*para que una actuación manual sobre datos personales tenga la consideración de tratamiento de datos sujeto al sistema de protección de la LOPD es necesario que dichos datos estén contenidos o destinados a ser contenidos en un fichero. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación del RGPD (...)".*

La Audiencia Nacional define en la citada sentencia de forma muy concisa lo que entiende por fichero: "*conjunto estructurado u organizado de datos con arreglo a criterios determinados".* Por lo que para ampliar el concepto de fichero debemos acudir al artículo 4.6) del RGPD, que lo define como "*todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*."

Del análisis de lo hasta ahora expuesto, en mi opinión, se puede deducir que quedan protegidos por el RGPD los datos personales automatizados y los datos personales que se almacenan en formato papel (datos no automatizados) siempre que los mismos estén contenidos en un fichero, atendiendo a un criterio de ordenación que pudiera permitir la búsqueda e identificación de los datos de una persona.

Desde una vertiente negativa, el artículo 2.2 establece cuatro supuestos en los que no resulta de aplicación el RGPD:

- En primer lugar, cuando se trata del tratamiento de datos personales en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión.
- En segundo lugar, cuando se trate de un tratamiento de datos personales por parte de los Estados miembros en el ejercicio de actividades comprendidas en el ámbito de la política exterior y la seguridad común.
- En tercer lugar, cuando el tratamiento de datos personales se efectúe por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Surge en relación con este punto el debate de si quedan incluidos en el ámbito de aplicación del RGPD los datos de los profesionales individuales. Se pronuncia afirmativamente en este sentido la Audiencia Nacional en una Sentencia de 12 de mayo de 2011, Recurso 31/2010, señalando que "*efectivamente, en el derecho a la protección de datos de carácter personal quedan incluidos los datos de los profesionales individuales, como se deriva del artículo de 2 del Real Decreto 1720/2007, de 21 de diciembre*"[10].
- Y, por último, cuando se trate de un tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención. En esta materia resulta de aplicación lo dispuesto por la Directiva UE 2016/680 del Parlamento Europeo y del Consejo.

Respecto al **ámbito de aplicación territorial** del RGPD, regulado en el artículo 3[11], en mi opinión la cuestión que más debate podía plantear y que ha sido resuelta por el RGPD

[10] Artículo 2. Ámbito de aplicación. "*2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. 3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal."*

[11] Artículo 3. Ámbito territorial.
"1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

es qué ocurre si el responsable del tratamiento de datos se encuentra establecido en un país tercero.

Primeramente, debemos hacer referencia a qué se entiende por "establecimiento" en el ámbito del RGPD, referenciándose en el Considerando 22 que un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables, siendo irrelevante la forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica.

En caso de que el responsable del tratamiento de datos personales no se encuentre establecido en la Unión Europea, para determinar si resulta de aplicación el RGPD se debe determinar si ofrece o no servicios o bienes a interesados, independientemente de si a estos se les requiere su pago. Si la respuesta es afirmativa, el artículo 3 del RGPD considera que en estos supuestos se aplica lo dispuesto en el mismo.

Aunque el RGPD no regula específicamente en ninguno de sus artículos cuál es su **ámbito de aplicación personal**, el mismo se deduce de la lectura del Considerando 14: la protección de datos otorgada por el Reglamento se aplica a las personas físicas, con independencia de su nacionalidad o de su lugar de residencia, excluyendo de manera directa el tratamiento de datos personales relativos a personas jurídicas. De igual manera, se deduce del Considerando 170, que recoge el objetivo del RGPD: "*Garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea*." Refiriéndose única y exclusivamente a la protección de las personas físicas en relación con sus datos personales.

2.1 MARCO CONCEPTUAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.
3. El presente Reglamento se aplica 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."

Antes de seguir analizando el RGPD, tan relevante en esta materia, considero necesario dedicar unas líneas a los conceptos que en el mismo se incluyen y que se van a ir mencionando a lo largo del presente trabajo, para su mejor comprensión.

En primer lugar, considero primordial especificar lo que se entiende por dato personal. La definición de dato personal la encontramos en el artículo 4.1 del RGPD: "*toda información sobre una persona física identificada o identificable*". Cabe señalar que el titular del dato es calificado por el RGPD como "*el interesado*".

A continuación, pasa a determinar cuándo se entiende que una persona es identificable, estableciendo que la identificación de una persona a los efectos de protección de datos se realiza cuando puede determinarse la identidad directa o indirectamente a través de elementos propios de la identidad física, fisiológica, psíquica, económica y cultural o social, a los cuales añade el elemento genético; o por identificadores como por ejemplo el nombre, un número de identificación, datos de localización o un identificador en línea.

Es decir, a modo de aclaración, un dato personal puede ser un identificador, un dato de localización o un nombre, siempre y cuando a través de estos se pueda identificar a la persona.

En relación con ello, el Considerando 26 del RGPD establece la forma en que se puede determinar si una persona es identificable: "*Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos*." El mismo Considerando se encarga de excluir del ámbito de aplicación del Reglamento los datos anónimos, disponiendo para ello que los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Por otro lado, el RGPD establece que por tratamiento se entiende cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Se trata de una definición muy amplia, de manera que a la vista de las ejemplificaciones casi cualquier operación que se haga con datos personales será considerada como tratamiento. En mi opinión, el hecho de que sea un concepto amplio responde a la intención del legislador de establecer un alcance lo más amplio posible para proteger a la persona física cuyos datos personales son objeto de tratamiento, y de esa manera evitar que queden vacíos legales. Por tanto, siempre que, por una parte, estemos ante datos personales y, por otra parte, estos sean objeto de tratamiento, será aplicable la normativa en materia de protección de datos personales.

Se exige por el RGPD que el tratamiento de datos personales tiene que ser lícito, por lo que es necesario aclarar qué implica la licitud del tratamiento. El artículo 6 RGPD dispone que para que el tratamiento sea lícito los datos personales deben ser tratados con el consentimiento del interesado o en alguna de las siguientes condiciones:

• Si el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos se entiende que dicho consentimiento es interpretado como un tratamiento lícito.

• Si para la ejecución de un contrato en el que el interesado es parte es necesario el tratamiento o también para medidas de naturaleza precontractual, dotaría de licitud al tratamiento.

• Si el tratamiento viene justificado a consecuencia de lo establecido en una norma con rango de ley no resultará preciso el consentimiento, sin que se vea afectada la licitud del tratamiento, al venir impuesto por la propia norma.

• En caso de que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

• Cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

• Si el tratamiento 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. Recordemos que el interés legítimo es un concepto jurídico indeterminado que será determinado en función de las circunstancias concurrentes tanto del responsable del tratamiento como de los interesados de los titulares de los datos. Quedando excluido directamente por la norma el tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Por último, resulta pertinente aclarar qué se entiende por "interesado". Haciendo una interpretación de lo que establece al efecto el apartado 1 del artículo 4 RGPD, se puede definir al interesado como la persona a la que los datos identifican.

Acudiendo al Considerando 7 del RGPD, el interesado, refiriéndolo en este caso como "la persona física", debe tener el control de sus propios datos personales, así como la capacidad de decidir a qué tratamientos se someten esos datos, por lo que es el destinatario de la protección y de las garantías que el RGPD establece.

Por tanto, las notas características del "interesado" son, por un lado, que es necesariamente una persona física, y por otro, que es el titular de los datos personales que son objeto de tratamiento.

2.2 LOS PRINCIPIOS QUE DEFINEN EL DERECHO A LA PROTECCIÓN DE DATOS EN EL RGPD

Tales principios los encontramos en el artículo 5 del RGPD[12] y se pueden concretar de la siguiente manera: licitud, lealtad y transparencia; limitación de la finalidad; minimización

[12] Artículo 5 del RGPD. Principios relativos al tratamiento.
"1. Los datos personales serán:
a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad y responsabilidad proactiva. Principios que también se encuentran recogidos en el Título II de la *Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos y garantía de los derechos digitales*.

Considero necesario hacer en este punto unas aproximaciones a cada uno de los mencionados principios.

a) Licitud, lealtad y transparencia: el RGPD impone que todos los tratamientos de datos personales deben ser leales, es decir, el encargado del tratamiento debe preservar que el mismo sea lícito. Así como debe tratarse de un tratamiento basado en la transparencia, informando al interesado de manera abierta al respecto.
b) Limitación de la finalidad: enunciándolo de una manera negativa, está prohibido el tratamiento de datos personales fuera del fin legítimo para el cual los datos personales fueron recogidos.
c) Minimización de datos: la recogida de datos personales para su tratamiento no puede ir más allá del fin legitimo para el que se recaban. Es decir, el análisis de datos se debe limitar a un conjunto de datos anonimizados, o a un conjunto de datos para los cuales se ha obtenido el consentimiento o existe un fin claro de tratamiento legítimo.
d) Exactitud: los datos personales de los interesados deben ser siempre precisos y estar correctamente actualizados. De esta manera se impone un deber a los

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 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»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
e) mantenidos 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; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, 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»);
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).”

responsables del tratamiento de datos personales: deben garantizar que se mantengan los datos precisos; y se reconoce una garantía en favor de los interesados: solicitar la actualización de tales datos cuando lo estimen conveniente.

e) Limitación del plazo de conservación: los datos personales deben ser eliminados una vez que se haya cumplido el fin legitimo para el cual fueron recogidos. Estableciendo el RGPD una excepción, y es que los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1.
f) Integridad y confidencialidad: se debe garantizar una seguridad apropiada de los datos personales que se tratan, que debe incluir una protección contra el tratamiento no autorizado o ilegal de los mismos.
g) Responsabilidad proactiva: la responsabilidad proactiva supone un marco de trabajo de autodisciplina de los encargos del tratamiento de datos, que deben velar por que el tratamiento de datos personales cumpla con lo establecido en la ley, respondiendo en caso de que el mismo no sea legal.

Como señala PIÑAR MAÑAS tales principios, para ser efectivos, requieren el reconocimiento, garantía y tutela de los derechos de las personas regulados en el propio RGPD: transparencia o deber de información a los interesados (arts. 12, 13 y 14 RGDP), derecho de acceso (art. 15 RGPD), rectificación (art. 16 RGPD), supresión (art. 17 RGPD), limitación del tratamiento (art. 18 RGPD), derecho a la portabilidad de los datos (art. 20 RGDP), derecho de oposición (art. 21 RGDP) y derecho a no ser objeto de decisiones individualizadas basadas exclusivamente en el tratamiento automatizado de datos (art. 22 RGPD)[13].

Los derechos de los interesados, entre los que se encuentra el derecho al olvido, suponen el centro del RGPD y se otorgan en aras de asegurar la protección y la privacidad en el tratamiento de los datos personales de los interesados.

[13] Cfr. PIÑAR MAÑAS, J. L., "Protección de datos. Las claves de un derecho fundamental imprescindible", *El Cronista del Estado Social y Democrático de Derecho*, nº 88, 2020, p. 11.

- Derecho de información, mediante el que se reconoce al interesado la capacidad de solicitar al encargado del tratamiento información acerca de qué datos personales están siendo tratados y una justificación de este tratamiento.
- Derecho de acceso: se reconoce al interesado el derecho de acceso a sus datos personales en caso de que se estén tratando los mismos, así como a obtener información respecto a ellos (a modo de ejemplo, el articulo 15 reconoce al interesado poder acceder a los fines del tratamiento o a la información relativa al plazo previsto de conservación de los datos personales).
- Derecho de rectificación, que proporciona al interesado el instrumento necesario para solicitar modificaciones de sus datos personales en caso de que considere que no están actualizados o no son precisos.
- Derecho de supresión o derecho al olvido. Dado que es el tema que nos ocupa en la segunda parte del presente trabajo me remito a la misma para su mejor comprensión.
- Derecho a la limitación del tratamiento de los datos personales, siempre y cuando concurra alguna de las siguientes condiciones:
    1. El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
    2. 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.
    3. El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado sí los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
    4. El interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable deben prevalecer sobre los del interesado.
- Derecho a la portabilidad de los datos: se reconoce la potestad del individuo para recibir los datos personales que haya facilitado a un responsable del tratamiento y trasmitirlos a otro responsable sin que el anterior lo pueda impedir. Los datos se le tienen que facilitar en un formato estructurado, de uso común y lectura mecánica.
- El derecho de oposición proporciona al interesado la capacidad de oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento en los casos establecidos en el artículo 21 del RGPD. Esos casos son:

- Si los datos se tratan lícitamente porque es necesario para el cumplimiento de una misión realizada:
  - en interés público o
  - en el desarrollo de poderes públicos atribuidos al responsable del tratamiento
  - por razones de intereses legítimos del responsable o de un tercero.

En estos casos el responsable tendrá que dejar de tratar esos datos, salvo que exista alguna de las siguientes excepciones: bien que el responsable acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o bien que acredite que el tratamiento de los mismos sea para el enunciado, la presentación o la defensa de reclamaciones. Tal y como establece el apartado 1 del mencionado artículo 21 del RGPD.

- Si los datos personales son tratados con fines de mercadotecnia[14] directa, incluyendo la elaboración de perfiles.

En este segundo caso el RGPD no contempla excepción alguna, en principio. Así pues, el responsable tendrá que dejar de tratar los datos personales del interesado con fines de mercadotecnia directa, incluida la elaboración de perfiles cuando la misma esté relacionada con dicha finalidad. Se dice en principio porque dicho tratamiento de datos con fines de mercadotecnia directa puede fundamentarse en un interés legítimo del responsable o de un tercero. Entonces habrá que ver si prevalece o no el interés legítimo sobre el derecho de oposición.

Cabe señalar que este derecho es diferente a la posibilidad que tiene el interesado de retirar su consentimiento al tratamiento de datos personales. En este sentido, el RGPD indica que el interesado tiene derecho a retirar su consentimiento en cualquier momento, y esa retirada del consentimiento no afectará a la licitud del tratamiento que estaba fundamentado en el consentimiento previo.

- Derecho de oposición al tratamiento automático. Se reconoce al interesado la facultad de solicitar al encargado del tratamiento una decisión manual.

[14] La RAE define la mercadotecnia como "*el conjunto de estrategias empleadas para la comercialización de un producto y para estimular su demanda*".

Recapitulando, considero que tanto los principios como los derechos mencionados son una herramienta efectiva para que el interesado pueda en cualquier momento comprobar que sus datos personales están siendo utilizados de una manera licita para el fin legitimo para el que en su momento fueron proporcionados.

3. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

A modo de recapitulación de lo ya expuesto, y como muy acertadamente señala AMÉRIGO ALONSO, la vertiente de derecho fundamental de la protección de datos personales se justifica por el reconocimiento constitucional[15], y es precisamente lo que justifica que la protección de datos se desarrolle mediante Ley Orgánica. Como consecuencia de esa naturaleza de derecho fundamental son predicables de la protección de datos personales las garantías que la Constitución Española otorga a los derechos fundamentales, en particular, la exigencia de que su ejercicio esté regulado mediante ley, en este caso orgánica (artículo 81 CE), que en todo caso deberá respetar su contenido esencial (artículo 53.1 CE), así como la tutela ante los tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional (artículo 53.2 CE).

Como señala POLO ROCA, la LOPDGDD trae una nueva regulación en materia de protección de datos que pretende dar respuesta a los constantes avances tecnológicos y las nuevas formas de éstos de transgredir la protección de datos[16]. La LOPDGDD deroga la antigua Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, recogiendo la normativa europea y adaptándola a nuestro ordenamiento. Además, en su título X incluye diecisiete nuevos derechos digitales para los ciudadanos españoles en materia de protección de datos.

[15] AMÉRIGO ALONSO, J. "El marco normativo de la protección de datos en España", *El Cronista del estado social y democrático de derecho*, nº 66-69, p. 20.
[16] POLO ROCA, A. "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *Revista de derecho político*, nº 108, 2020, p. 167.

Ahondado ya en su contenido, resulta necesario, en primer lugar, determinar cuál es su objeto, de lo que se encarga el artículo 1, que no es otro que "*adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones*", así como "*garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución*".

En el Título II, bajo la rúbrica "Principios de protección de datos", se establece que a efectos del RGPD no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario, cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador, o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad y se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como "consentimiento tácito". Se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas[17].

Como ya se ha indicado, la Ley Orgánica adapta la normativa interna al Derecho de la Unión Europea, pero introduciendo algunas novedades respecto a la misma, razón por la cual se van a analizar las que suscitan más interés en este punto:

- Hay que resaltar las nuevas especificaciones en el derecho de acceso contenidas en el artículo 13.2 LOPDGDD, reconociéndose la posibilidad de que se pueda crear un módulo en el que el titular de los datos pueda acceder a su información de forma remota, directa, simple y segura. Asimismo, el artículo 13.3 LOPDGDD advierte que en caso de que el interesado repita este ejercicio del derecho de acceso en menos de seis meses, a menos que exista una causa legítima para ello,

[17] Título II Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

se podrá considerar repetitivo, siendo la consecuencia jurídica que podría aplicarle un canon razonable, o incluso negarse a atender la solicitud, de conformidad con la remisión que se contiene al artículo 12.5 del RGPD.

- Reviste mucho interés el cambio en el régimen jurídico de la Agencia Española de Protección de Datos (artículo 44). La Agencia Española de Protección de Datos se configura ahora como una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones, dando así cumplimiento al mandato del artículo 54.1 a) RGPD, que exige que las autoridades de protección de datos se han de establecer y configurar por ley nacional.
- Sin duda, una de las principales novedades de la norma es el reconocimiento y la garantía de diecisiete nuevos derechos digitales en el Título X, que se reconocen conforme al mandato establecido en la Constitución Española[18]. Respecto al tema que nos ocupa, el derecho a la protección de datos y el derecho al olvido digital, resulta de especial interés el análisis de los siguientes derechos:

- El primero de los derechos digitales que se garantiza en este nueva LOPDGDD es el de acceso y neutralidad de Internet (artículos 80 y 81 LOPDGDD). El derecho a Internet es un derecho humano desde 2011 para la ONU y ahora esta nueva ley reconoce que debe ser "universal, asequible, de calidad y no discriminatorio". Se reconoce también el derecho a la seguridad digital (artículo 82 LOPDGDD) en las comunicaciones que los usuarios transmitan y reciban a través de Internet. Se trata de trasladar el artículo 18 de la Constitución en el que se recoge el derecho de privacidad de las comunicaciones al mundo digital.
- Se recoge el derecho de rectificación en Internet (artículo 85 LOPDGDD) y dentro de este apartado se recoge también la libertad de expresión en Internet, prohibiendo que se niegue el servicio o se bloquee la participación de los usuarios por sus opiniones. Además, se reconoce el derecho a la rectificación de información publicada en redes sociales u otros servicios equivalentes, disponiendo a tal efecto que los responsables de redes sociales y servicios

[18] Preámbulo V Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación. Añadiendo que cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

- Un punto muy interesante en mi opinión es el reconocimiento del derecho a la actualización de información en los medios de comunicación digitales (artículo 86 LOPDGDD), que supone el derecho de una persona a que una noticia u opinión publicada en un medio de comunicación sea corregida y modificada si su información no se corresponde con la situación actual y ello le causa un perjuicio. Además, se contemplan como nuevos derechos los siguientes:
    - Derecho a la educación digital (artículo 83)
    - Protección de los menores en Internet (artículo 84)
    - Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (artículo 87)
    - Derecho a la desconexión digital en el ámbito laboral (artículo 88)
    - Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (artículo 89)
    - Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (artículo 90)
    - Derechos digitales en la negociación colectiva (artículo 91)
    - Protección de datos de los menores en Internet (artículo 92)
    - Derecho al olvido en búsquedas de Internet (artículo 93)
    - Derecho al olvido en servicios de redes sociales y servicios equivalentes (artículo 94)
    - Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (artículo 95)
    - Derecho al testamento digital (artículo 96)

A modo de conclusión y en líneas generales, se puede afirmar que la aprobación de la LOPDGDD se trata de una reforma necesaria y positiva para fortalecer, definir, adaptar y aclarar algunos conceptos del RGPD, y asimismo regular de forma más específica determinadas cuestiones en el ámbito de la protección de datos en nuestro ordenamiento jurídico.

Como muy acertadamente señala MUÑOZ DE PEDRO, en el ámbito estrictamente de la protección de datos personales se trata de una normativa innovadora en muchos aspectos (testamento digital, tratamiento específico en materia de salud…), que implementa en las Administraciones Públicas notables garantías para la protección de los datos de carácter personal (anonimización de las publicaciones y notificaciones, esquema nacional de seguridad…). No obstante, plantea algunas dudas que afectan al principio de seguridad jurídica, como el hecho de contemplar que los responsables enumerados en el artículo 77.1 LOPDGDD (órganos jurisdiccionales, AAPP, organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas…) puedan comunicar los datos personales que les sean solicitados por sujetos de derecho privado no solamente cuando cuenten con el consentimiento de los afectados sino también cuando aprecien que concurre en los solicitantes un "interés legítimo" que prevalezca sobre los derechos e intereses de los afectados (conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679), sin que en la norma que se acaba de aprobar se defina de forma precisa los contornos de aquel concepto[19].

Desde un punto de vista sistemático ha sido objeto de crítica por parte de varios autores, entre ellos TEJERINA, el hecho de que se haya incluido dentro de la norma jurídica que regula la protección de datos personales los derechos digitales, ya que estos últimos, sin perjuicio de su relación con la protección de datos, por su importancia y entidad, debieran haberse contemplado en una norma autónoma y propia. Así, se ha convertido a la LOPDGDD en una norma trasversal que afecta a distintas materias que no son strictu sensu "protección de datos personales" (libertad de expresión en Internet, neutralidad de la red, el derecho del trabajador a un horario digno…)[20]. Sin que ello obste a reconocer el

[19] MUÑOZ DE PEDRO, A. "Principales novedades de la ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Revista del gabinete jurídico de Castilla- La Mancha*, nº 16, 2018, p. 53.

[20] TEJERINA, O., "Por qué la nueva LOPD (LOPDGDD) nos Inquieta, nos atormenta y nos perturba", 2018. Disponible en: https://www.internautas.org/html/10141.html (acceso 15-04-2021).

importante hito que supone la inclusión de unos derechos digitales, adaptando así nuestro ordenamiento jurídico la realidad tecnológica de nuestro entorno.

II. RÉGIMEN JURÍDICO DEL DERECHO AL OLVIDO DIGITAL

1. MARCO LEGAL DEL DERECHO AL OLVIDO DIGITAL

El derecho al olvido digital tiene una naturaleza de carácter jurisprudencial, siendo trascendental la Sentencia del Tribunal de Justicia de la Unión Europea (en adelante TJUE) de 13 de mayo de 2014, sobre el caso *Google*[21], que estableció las bases normativas para la regulación posterior de este derecho, tanto a nivel europeo, como a nivel nacional. Surge como respuesta a las reiteradas vulneraciones de la privacidad que los ciudadanos venían sufriendo en el entorno de internet, manifestadas a consecuencia de la invasión que las novedades tecnológicas y el Big Data han provocado en los derechos fundamentales.

Consecuencia del citado pronunciamiento del TJUE, el Reglamento General de Protección de Datos[22] (en adelante, RGPD) reconoce expresamente, y por primera vez, el derecho de supresión de toda persona sobre sus datos personales como una suerte de derivación del derecho a la intimidad y propia imagen y como extensión del derecho al honor[23].

En el artículo 17 del RGDP se regula el derecho al olvido en un ámbito general, bajo la rúbrica "Derecho de supresión", como "*el derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales*." Siempre y cuando concurran ciertas circunstancias:

[21] Tribunal de Justicia de la Unión Europea. Sentencia de 13 de mayo de 2014. Caso Google Spain versus Agencia Española de Protección de Datos. Disponible en: https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

[22] Entró en vigor el 25 de mayo de 2018 reemplazando a todas las leyes nacionales de los Estados miembros de la Unión Europea en esta materia. Y, concretamente, en España sustituyó a la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

[23] Cfr. SANCHO LÓPEZ, M. "Estrategias legales para garantizar los derechos fundamentales frente a los desafíos del Big Data", *Revista General de Derecho Administrativo*, nº 50, 2019, p.10

a) *Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;*
b) *El interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;*
c) *El interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;*
d) *Los datos personales hayan sido tratados ilícitamente;*
e) *Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;*
f) *Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.*

El Considerando 65[24] del mencionado Reglamento dispone lo siguiente: *"Los interesados deben tener derecho a que se rectifiquen los datos personales que les conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el*

[24] Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones".

El Considerando 66[25] se refiere al tratamiento del derecho al olvido de los datos en línea (en la red) disponiendo lo siguiente: *"A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales. "*

El derecho al olvido no se configura en el RGDP como un derecho autónomo o diferenciado de los derechos ARCO[26], sino como una consecuencia de los mismos. Son muchos los autores que defienden esta postura. SANCHO LOPEZ defiende que el derecho al olvido digital supone una modernización de los derechos tradicionales para adecuarlos a la nueva realidad social, incorporándose así a las potestades existentes de solicitar y obtener de los responsables de los ficheros que determinados datos sean suprimidos cuando concurra alguna de las circunstancias del artículo 17 RGDP, todo ello en el entorno digital[27]. CHÉLIZ INGLÉS entiende el derecho al olvido digital como una extensión del derecho a la protección de datos, surgiendo a partir de los nuevos escenarios en internet[28].

Por el contrario, hay quienes sostienen que el derecho al olvido es un derecho autónomo. Entre ellos MARTÍNEZ LÓPEZ-SÁEZ, que sostiene que lo que hace al derecho al olvido ser diferente y autónomo de los conocidos derechos ARCO (acceso, rectificación,

[25] Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807
[26] Los derechos ARCO se regulan en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD) y en el RGDP. Originariamente eran cuatro: Derecho de Acceso, Derecho de Rectificación, Derecho de Cancelación y Derecho de Oposición; el Reglamento General de Protección de Datos añadió con su entrada en vigor en 2016 dos más: el Derecho de Limitación y el Derecho de Portabilidad, con lo que los derechos ARCO pasaron a ser un total de seis.
[27] SANCHO LÓPEZ, M. "Estrategias legales para garantizar los derechos fundamentales frente a los desafíos del Big Data", cit., p.11.
[28] CHÉLIZ INGLÉS, M.C., "El derecho al olvido digital. Una exigencia de las nuevas tecnologías recogida en el futuro Reglamento General de Protección de Datos", *Revista Jurídica Iberoamericana*, núm. 5, 2016, p.258.

cancelación y oposición) es precisamente la obligación jurídica impuesta sobre los responsables del tratamiento de hacer olvidar datos de carácter personal mediante la adopción de medidas razonables, incluidas medidas técnicas, con miras a *informar a los responsables que estén tratando los datos personales* de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. Lo que considera controvertido, pues convierte al responsable del tratamiento también en responsable de la información que publiquen terceros mediante enlaces vinculados a esta, pero que es lo que convierte al derecho en autónomo[29].

El TC ha sido el encargado de pronunciarse acerca de esta cuestión, reconociendo en la Sentencia 58/2018, de 4 de junio, el derecho al olvido como un derecho autónomo.

"El derecho al olvido, que es el derecho a la supresión de los datos personales (...), está estrechamente vinculado con la salvaguardia del derecho fundamental a la protección de datos personales frente al uso de la informática (art. 18.4. CE), y con la protección del artículo 8 de la Carta de los derechos fundamentales de la Unión Europea y del Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal." Así considerado, indica el Tribunal, "el derecho al olvido es una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4. CE), y es también un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo".

Por su parte el Legislador español ha entendido que el derecho al olvido es merecedor de una protección reforzada en el ámbito de Internet, por lo que en el artículo 15 LOPDGDD regula expresamente el derecho al olvido, que se corresponde con el derecho al olvido que se establece en el ya mencionado artículo 17 RGPD, regulando, además, en el Título X "Garantía de los derechos digitales" dos derechos al olvido específicos: el

[29] Cfr. MARTÍNEZ LÓPEZ-SÁEZ, M. "Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: La difícil conciliación entre las libertades económicas y la protección de datos personales", *Estudios de Deusto,* Vol.65/2, 2017, pág. 163.

derecho al olvido en búsquedas de internet[30] (artículo 93) y el derecho al olvido en servicios de redes sociales y servicios equivalentes[31] (artículo 94).

2. MARCO CONCEPTUAL DEL DERECHO AL OLVIDO DIGITAL

Como ya se ha señalado, el derecho al olvido digital se encuentra regulado en el RGDP, definiéndose en el artículo 17 como "*el derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales*" cuando concurran ciertas circunstancias.

Por lo que respecta a la normativa nacional, la Agencia Española de Protección de Datos define el "derecho al olvido" como el derecho que cualquier persona tiene para solicitar

[30] Artículo 93. *Derecho al olvido en búsquedas de Internet.*
1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.
Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.
2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

[31] Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*
1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes. 2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.
Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.
3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

la supresión de sus datos personales en los buscadores de internet. El mismo no es ilimitado, de tal forma que puede ser factible no proceder a la supresión cuando el tratamiento sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, por razones de interés público, en el ámbito de la salud pública, con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

Son numerosos los autores que se han pronunciado acerca del concepto del derecho al olvido digital. ARENAS RAMIRO considera que el derecho al olvido tiene su origen en las reiteradas intromisiones en la vida privada de los ciudadanos surgidas con la aparición de las nuevas tecnologías en convivencia con el Big data e internet[32]. JIMÉNEZ-CASTELLANOS BALLESTEROS lo define como la facultad que tiene una persona de controlar y limitar la difusión actual de hechos verídicos de su pasado, acompañados de sus datos identificativos, que carecen de interés público vigente y afectan a su vida privada[33]. PERE SIMÓN lo entiende como "*aquel derecho a eliminar, ocultar y cancelar aquellas informaciones o hechos pasados relativos a la vida de las personas físicas y que pueden afectar a las mismas en su desarrollo personal para el futuro"*[34]. MALDONADO RAMOS lo configura como el derecho reconocido al ciudadano de obtener la supresión de la difusión de datos y noticias concernientes al mismo a través de los medios activos en Internet[35]. MURGA FERNÁNDEZ lo concibe como el derecho a solicitar que en determinados casos se cancelen datos personales que circulan por Internet ante el riesgo que ello supone en la vulneración de los derechos de la personalidad (particularmente, los derechos al honor e intimidad)[36].

[32] Cfr. ARENAS RAMIRO, M. "Reforzando el ejercicio del derecho a la protección de datos", en *Hacia un nuevo Derecho europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015, p. 335.
[33] Cfr. JIMÉNEZ-CASTELLANOS BALLESTEROS, I. "El conflicto entre el derecho al olvido digital del pasado penal y las libertades informativas: las hemerotecas digitales", *UNED Revista de Derecho Político*, nº 106, 2019, p. 141.
[34] SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012, pp. 21-22.
[35] Cfr. MALDONADO RAMOS, I. "De nuevo sobre el derecho al olvido", *El notario del siglo XXI*, nº 93, 2020, p. 80.
[36] MURGA FERNÁNDEZ, J.P.: "Protección de datos y los motores de búsqueda en internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido", *Revista de Derecho Civil*, núm. 4, 2017, p. 4.

De todas las definiciones que se han hecho al respecto, quizá la más ajustada a la realidad, al menos en mi opinión, es la de SANCHO LÓPEZ, para la que el derecho al olvido digital es la respuesta que se ha ofrecido desde el derecho a los usuarios de la Red para que puedan obtener el borrado digital de cualquier información personal por la cual se vea afectada su privacidad, ya sea debido a causas justificadas[37] o porque con el paso del tiempo sus datos personales han perdido su virtualidad[38].

3. ANÁLISIS DE LA SENTENCIA TJUE CASO GOOGLE

La sentencia del Tribunal de Justicia de la Unión Europea (en adelante TJUE) en el asunto C-131/12 Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, supuso la consagración del derecho al olvido digital**,** por lo que es imprescindible en el presente trabajo hacer un análisis de ésta.

El litigio surge como consecuencia de una reclamación presentada ante la Agencia Española de Protección de Datos (en adelante, AEPD) por un ciudadano español, el Sr. Costeja, contra La Vanguardia Ediciones, S. L. y contra Google Spain y Google Inc.
En dicha reclamación el Sr. Costeja ejercía el derecho de oposición frente a La Vanguardia y frente a Google, basándolo en que cuando un internauta introducía su nombre en el motor de búsqueda, obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González.

Antecedentes

Mediante la reclamación el Sr. Costeja solicitaba lo siguiente:
I) Por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Reclamación que fue desestimada por la

[37] Las causas justificadas son las que recoge el artículo 17 RGDP.
[38] Cfr. SANCHO LÓPEZ, M. "Límites del derecho al olvido. Veracidad y tiempo como factores de ponderación", *Revista General de Derecho Constitucional*, nº 32, 2020, p. 2.

AEDP mediante resolución de 30 de julio de 2010, al considerar que la publicación 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.

II) Por otro lado, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. Reclamación que fue estimada por la AEPD, que consideró 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. La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros.

Google Spain y Google Inc. recurrieron dicha reclamación de la AEPD ante la Audiencia Nacional, que acumuló ambos recursos, exponiendo en el auto de remisión que en el asunto se trataba de dilucidar cuáles son las obligaciones que tienen los gestores de motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contiene sus datos personales y permite relacionarles con la misma, sea localizada, indexada y sea puesta a disposición de los internautas de forma indefinida. Resultando para ello necesario interpretar algunos artículos de la Directiva 95/46 CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, lo que dio lugar a que la Audiencia Nacional decidiese suspender el procedimiento y plantear al TJUE tres cuestiones prejudiciales.

Derecho aplicable relevante

Antes de abordar la cuestión, considero necesario señalar lo que establece el Artículo 2 de la Directiva en relación con los dos conceptos básicos que se dilucidaban aquí: el tratamiento de datos personales y la responsabilidad.

- El artículo 2.b) dispone que por tratamiento de datos personales se entiende cualquier operación o conjunto de operaciones mediante procedimientos automatizados, y aplicadas a datos personales por cualquier forma que facilite el acceso a los mismos (por ejemplo, la comunicación por trasmisión), su cotejo o interconexión, así como su bloqueo, supresión o destrucción.

- Por su parte, el artículo 2.d) de la Directiva considera como 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.

Cuestiones prejudiciales

La Audiencia Nacional planteó al Tribunal de Justicia de la Unión Europea las cuestiones prejudiciales siguientes:

1) la aplicación territorial de la Directiva 95/46 y, consiguientemente, de la normativa española de protección de datos.
2) la actividad de los buscadores como proveedores de contenidos en relación con la Directiva 95/46.
3) el alcance del derecho de cancelación y/oposición en relación con el derecho al olvido.

Opinión del abogado general

El Abogado General Jääskinen consideraba que los proveedores de servicios de motor de búsqueda en Internet no son responsables, sobre la base de la Directiva sobre Protección de Datos, de los datos personales incluidos en las páginas web que tratan.

El Abogado General consideraba que la cuestión ahora referida debía examinarse teniendo en cuenta el modelo de negocio de los proveedores de servicios de motores de búsqueda en Internet. Éste se basa normalmente en la publicidad a partir de palabras clave, que es la fuente de ingresos y la razón de ser económica para proveer una herramienta de localización de información gratuita. La entidad responsable de la publicidad a partir de palabras clave está vinculada al motor de búsqueda en Internet. Esta entidad necesita tener presencia en los mercados nacionales del sector de la publicidad, y por este motivo Google ha creado filiales en muchos Estados miembros.

Por tanto, a su juicio, debe considerarse que un establecimiento trata datos personales si está vinculado a un servicio que participa en la venta de publicidad orientada a los habitantes de este Estado miembro, aunque las operaciones de tratamiento técnico de los datos estén situadas en otro Estado miembro o en países terceros. Por consiguiente, el Sr. Jääskinen propone al Tribunal de Justicia que declare que se lleva a cabo tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable del tratamiento y que, por tanto, la normativa nacional en materia de protección de datos es de aplicación a un proveedor de un motor de búsqueda cuando éste establece en un Estado miembro, a fines de promover y vender espacios publicitarios en su motor de búsqueda, una oficina que orienta su actividad hacia los habitantes de dicho Estado.

En segundo lugar, en lo que atañe a la situación jurídica de Google como proveedor de servicios de motor de búsqueda en Internet, el Sr. Jääskinen recuerda que, cuando se adoptó la Directiva en 1995, Internet y los motores de búsqueda eran fenómenos novedosos y el legislador comunitario no previó su evolución actual. Opina que no se ha de considerar que Google es, con carácter general, «responsable del tratamiento» de los datos contenidos en las páginas web que procesa, siendo así que el responsable del tratamiento, según la Directiva, es responsable del respeto de las normas de protección de datos. En efecto, la puesta a disposición de una herramienta de localización de información no implica control alguno sobre el contenido incluido en páginas web de terceros. Tampoco permite al proveedor de servicios de motor de búsqueda en Internet

realizar distinciones entre datos personales en el sentido de la Directiva, es decir, relacionados con una persona física viva identificable, y otro tipo de datos. A su juicio, el proveedor de servicios de motor de búsqueda en Internet no puede ni jurídicamente ni de hecho cumplir las obligaciones del responsable del tratamiento en relación con los datos personales contenidos en páginas web fuente alojadas en servidores de terceros.

En consecuencia, una autoridad nacional de protección de datos no puede requerir a un proveedor de servicios de motor de búsqueda en Internet que retire información de su índice, salvo en los supuestos en que el proveedor de servicios no ha respetado los códigos de exclusión o en los que no se ha dado cumplimiento a una solicitud emanada de la página web relativa a la actualización de la memoria oculta. Este supuesto no parece pertinente en relación con el presente asunto. La existencia de un procedimiento de «detección y retirada» que afecte a enlaces de las páginas web fuente con contenidos ilícitos o inapropiados es una cuestión regulada por el Derecho nacional, la responsabilidad civil basada en motivos distintos de la protección de datos personales. El editor de páginas web fuente puede utilizar «códigos de exclusión», que recomiendan a los motores de búsqueda que no indexen o almacenen una página web fuente, o que no la muestren en los resultados de la búsqueda. Su uso indica que el editor no desea que determinada información de la página web fuente pueda ser recuperada para su difusión a través de motores de búsqueda.

En tercer lugar, la Directiva no establece ningún «derecho al olvido» generalizado. Por tanto, no puede invocarse tal derecho frente a proveedores de servicios de motor de búsqueda sobre la base de la Directiva, aun cuando ésta se interpreta con arreglo a la Carta de los DF UE. Los derechos de rectificación, supresión y bloqueo de datos establecidos en la Directiva se refieren a datos cuyo tratamiento no cumple lo dispuesto en la Directiva, en particular debido al carácter incompleto o inexacto de los datos. Éste no parece ser el caso en el presente asunto.

La Directiva también reconoce a toda persona el derecho a oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. No obstante, el Abogado General considera que una preferencia subjetiva por sí sola no equivale a una razón legítima y que, por tanto, la Directiva no faculta a una

persona para restringir o poner fin a la difusión de datos personales que considere lesivos o contrarios a sus intereses.

Es posible que la responsabilidad secundaria de los proveedores del servicio de motor de búsqueda con arreglo al Derecho nacional implique la existencia de deberes que exijan bloquear el acceso a páginas web de terceros con contenidos ilegales, como las páginas web que vulneran derechos de propiedad intelectual o que muestran información injuriosa o delictiva. En cambio, solicitar a los proveedores de servicios de motor de búsqueda que eliminen información legítima y legal que se ha hecho pública traería consigo una injerencia en la libertad de expresión del editor de la página web. En su opinión, equivaldría a una censura del contenido publicado realizada por un particular.

Respuestas del TJUE

Y el TJUE respondió a las cuestiones prejudiciales así:

En lo que se refiere al ámbito de aplicación territorial de la Directiva, el TJUE observa que Google Spain es una filial de Google Inc. en territorio español y, por lo tanto, un «establecimiento» en el sentido de la Directiva. El Tribunal rechaza el argumento de que Google Search no realiza un tratamiento de datos de carácter personal en el marco de sus actividades desarrolladas en España y considera a este respecto que, cuando el tratamiento de estos datos se lleva a cabo para permitir el funcionamiento de un motor de búsqueda gestionado por una empresa que, a pesar de estar situada en un Estado tercero, dispone de un establecimiento en un Estado miembro, ese tratamiento se efectúa «en el marco de las actividades» de dicho establecimiento, en el sentido de la Directiva, siempre que la misión de ese establecimiento sea la promoción y la venta, en ese Estado miembro, de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio ofrecido por este último.

El TJUE señala a continuación que al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos, en el sentido de la Directiva. El Tribunal estima, además, que dicho gestor «extrae», «registra» y «organiza» esos datos en el marco de sus programas de indexación, antes de «conservarlos» en sus servidores y, en su caso, los

«comunica» a sus usuarios y les «facilita el acceso» a los mismos en forma de listas de resultados. Estas operaciones, mencionadas en la Directiva de forma explícita e incondicional, deben calificarse de «tratamiento», con independencia de que el gestor del motor de búsqueda las aplique de modo indiferenciado a informaciones que no son datos personales.

Por lo demás, el Tribunal recuerda que las operaciones a las que se refiere la Directiva también deben calificarse de «tratamiento» aun cuando sólo se refieran a información ya publicada, tal cual, en los medios de comunicación. Si en este último caso se estableciera una excepción general a la aplicación de la Directiva, esta última quedaría en gran medida vacía de contenido.

En lo que respecta al alcance de la responsabilidad del gestor de un motor de búsqueda, el TJUE considera que, en determinadas condiciones, éste está obligado a eliminar de la lista de resultados, obtenida tras una búsqueda efectuada a partir del nombre de una persona, los enlaces a páginas web publicadas por terceros que contengan información relativa a esta persona. El Tribunal precisa que esa obligación puede existir también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de esas páginas web y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.

El TJUE pone de relieve, en este contexto, que un tratamiento de datos de carácter personal efectuado por el gestor de un motor de búsqueda permite que cualquier internauta que realice una búsqueda a partir del nombre de una persona física obtenga, a través de la lista de resultados, una visión estructurada de la información relativa a esa persona que circula en Internet. El Tribunal señala también que esa información afecta potencialmente a una multitud de aspectos de la vida privada y que sin dicho motor de búsqueda tales aspectos no se habrían interconectado, o sólo habrían podido interconectarse con grandes dificultades.

Los internautas pueden establecer así un perfil más o menos detallado de las personas buscadas. Por otra parte, el efecto de esta injerencia en los derechos de la persona se multiplica a causa del importante papel que desempeñan en la sociedad moderna Internet y los motores de búsqueda, los cuales confieren ubicuidad a la información contenida en las listas de resultados. Dada su gravedad potencial, el Tribunal considera que esta

injerencia no puede justificarse por el mero interés económico del gestor del motor de búsqueda en el tratamiento de los datos.

Sin embargo, como, según la información de que se trate, la supresión de enlaces de la lista de resultados podría tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión, el Tribunal afirma que es preciso buscar un justo equilibrio entre este interés y los derechos fundamentales de la persona afectada, en particular el derecho al respeto de su vida privada y el derecho a la protección de los datos de carácter personal.

El TJUE señala al respecto que, si bien es cierto que los derechos de la persona afectada prevalecen igualmente, por regla general, sobre el mencionado interés de los internautas, este equilibrio puede depender en casos particulares de la naturaleza de la información de que se trate, de lo delicada que ésta sea para la vida privada de la persona de que se trate y del interés del público en disponer de esa información, que puede variar, en particular, en función del papel que esa persona desempeñe en la vida pública.

Por último, en respuesta a la pregunta de si la Directiva permite que la persona afectada solicite que se supriman de esa lista de resultados unos enlaces a páginas web porque desea que la información sobre ella que figura en esas páginas se «olvide» después de un cierto tiempo, el Tribunal de Justicia indica que si, a raíz de la solicitud de la persona afectada, se comprueba que la inclusión de esos enlaces en la lista es incompatible actualmente con la Directiva, la información y los enlaces que figuran en la lista deben eliminarse.

El TJUE observa a este respecto que, con el tiempo, incluso un tratamiento inicialmente lícito de datos exactos puede llegar a ser incompatible con la Directiva cuando, habida cuenta de todas las circunstancias que caractericen cada caso, esos datos se revelen inadecuados, no pertinentes o ya no pertinentes o excesivos desde el punto de vista de los fines para los que fueron tratados y del tiempo transcurrido.

El TJUE añade que, al apreciar la solicitud presentada en este sentido por la persona afectada contra el tratamiento de sus datos efectuado por el gestor de un motor de búsqueda, se tendrá que examinar, en particular, si dicha persona tiene derecho a que la información en cuestión sobre ella deje de estar vinculada en la actualidad a su nombre a través de la lista de resultados que se obtiene tras efectuar una búsqueda a partir de su

nombre. Si éste es el caso, los enlaces a páginas web que contienen esa información deben suprimirse de esa lista de resultados, a menos que existan razones particulares –como el papel desempeñado por esa persona en la vida pública– que justifiquen que prevalezca el interés del público en tener acceso a esa información al efectuar la búsqueda.

Resolución de la sala de lo Contencioso-Admisnistrativo de la Audiencia Nacional de 29 de diciembre de 2014, en aplicación de la doctrina del TJUE sobre el derecho al olvido.

La Sala de lo Contencioso-Administrativo de la Audiencia Nacional con fecha 29 de diciembre de 2014 dictó Sentencia[39], mediante la que se resuelve el recurso número 725/2010, en aplicación de la doctrina del TJUE sobre el derecho al olvido expuesta en el apartado anterior del presente trabajo.

La Sala se encarga de fijar los criterios, en base a lo establecido por el TJUE, que deben cumplir los particulares, los responsables del tratamiento y la Agencia de Protección de Datos cuando se ejerza por los primeros el derecho al olvido, para llevar a cabo el juicio de ponderación esgrimido por el TJUE y que se resumen en lo siguiente: "*quien ejercite el derecho de oposición ha de indicar ante el responsable del tratamiento o ante la Agencia Española de Protección de Datos que la búsqueda se ha realizado a partir de su nombre, como persona física; indicar los resultados o enlaces obtenidos a través del buscador, así como el contenido de esa información que le afecta y que constituye un tratamiento de sus datos personales a la que se accede a través de dichos enlaces*".

El juicio de ponderación, considera el tribunal, deberá llevarse a cabo en relación con los derechos en conflicto en cada caso, para establecer si el derecho a la protección de datos debe prevalecer sobre otros derechos e intereses legítimos, en atención a "*la concreta situación personal y particular de su titular*". Considerando que la cancelación de esos datos estará justificada cuando las circunstancias de cada caso concreto así lo determinen, "*ya sea por la naturaleza de la información, su carácter sensible para la vida privada del afectado, por la no necesidad de los datos en relación con los fines para los que se recogieron o por el tiempo transcurrido, entre otras razones*".

[39] Disponible en: https://www.poderjudicial.es/search/AN/openCDocument/d6c3141dd81d8758a0bb78e44820713e83b1b8ed4f7b05ec

Respecto al caso concreto que motivó el pronunciamiento del TJUE, la Sala haciéndose eco del mismo resolvió en los siguientes términos.

La Sala en la citada sentencia reconoció el derecho del actor, Mario Costeja González, a retirar los enlaces a unos anuncios aparecidos en la web del periódico la Vanguardia, sobre unos embargos por deudas a la seguridad Social ejecutados hace 16 años. En aplicación de la Doctrina del TJUE da la razón al actor alegando que no tenía relevancia en la vida pública que justificara la prevalencia del interés del público general frente a los derechos de la protección de datos de carácter personal. Pues se trataba de un tratamiento de datos inicialmente lícito, de datos exactos por parte de Google pero que dado el tiempo transcurrido no son necesarios en relación con los fines para los que se recogieron o trataron. Además, el tribunal entiende que en este caso la libertad de información se encuentra satisfecha porque la información subsiste en la fuente, el sitio web donde se publicó por el editor, pudiéndose llegar a estos datos aun eliminando los vínculos a las páginas web objeto de reclamación.

En consecuencia, el Sr. Costeja tiene derecho a que la información sobre una subasta de inmuebles relacionada con un embargo derivado de deudas a la seguridad social "*ya no esté vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de sus datos personales*".

4. ¿CÓMO SE EJERCE EL DERECHO AL OLVIDO DIGITAL?

La Agencia Española de Protección de Datos nos ofrece la respuesta a esta cuestión, estableciendo como se debe actuar en caso de querer ejercer el derecho al olvido[40].

La normativa de protección de datos (RGDP) establece que para ejercer el derecho al olvido es imprescindible que el ciudadano se dirija en primer lugar a la entidad que está tratando sus datos, en este caso al buscador. Los buscadores mayoritarios, a saber, Google, Bing y Yahoo, cuentan con sus propios formularios para recibir las peticiones de ejercicio de este derecho en este ámbito. Una vez presentada la solicitud, nos podemos encontrar con cuatro supuestos: que la entidad no responda a la petición realizada, que

[40] Disponible en: https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido (Acceso 4-03-2021)

obtenida respuesta por parte de la entidad el solicitante no esté conforme con la misma, que se decline la solicitud, y, por último, que la solicitud sea atendida y se proceda por parte de la entidad a la desindexación de los datos.

En los tres primeros supuestos planteados, el interesado podrá acudir ante la Autoridad de Control para que tutele el derecho, acompañando la documentación que evidencie la solicitud de supresión ejercida ante la entidad de que se trate y, cuya resolución agotará la vía administrativa, pudiendo el interesado interponer, en el supuesto de disconformidad con la misma, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos, en el plazo de un mes a contar desde el día siguiente a la notificación de la resolución, o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en el plazo de dos meses desde el día siguiente a la notificación.

5. JURISPRUDENCIA NACIONAL

5.1 SENTENCIA DE LA SALA DE LO CIVIL DEL TRIBUNAL SUPREMO DE 15 DE OCTUBRE DE 2015

El punto de partida se encuentra en la Sentencia de la Audiencia Provincial de Barcelona de 11 de octubre de 2013. Con carácter previo a ahondar en ella y en la jurisprudencia asentada con posterioridad, resulta necesario hacer unas aproximaciones a los antecedentes del caso.

En el año 1985, el diario El País publicó una noticia relativa al desmantelamiento de una red de tráfico de estupefacientes en la que se hallaba implicado el familiar de un destacado cargo público y otros miembros de la clase alta de una determinada localidad. Dicha noticia identificaba a los protagonistas de los hechos por su nombre, apellido y profesión, a la vez que describía su condición de toxicómanos, afirmando que los condenados sufrieron el síndrome de abstinencia durante su estancia en prisión.

En el año 2007, el diario El País estableció el acceso gratuito a su hemeroteca digital y, con ello, se permitió a cualquier persona que introdujese los nombres y apellidos de las personas mencionadas en el cuerpo de la noticia en el motor de búsqueda online Google acceder de nuevo a la noticia comentada anteriormente, ahora digitalizada, apareciendo

ésta como primer resultado ofrecido por dicho proveedor de servicios de intermediación de búsqueda en Internet. Dos de los protagonistas de dichos sucesos, al tener conocimiento de estas circunstancias, solicitaron a El País que cesara en el tratamiento de sus datos personales o, subsidiariamente, que sustituyese en la noticia digital sus nombres y apellidos por sus iniciales y, en todo caso, que adoptase las medidas tecnológicas necesarias para que la página web dónde se había publicado la noticia no fuera indexada por los buscadores web al introducir sus nombres y apellidos. El diario El País no accedió a sus pretensiones en base a su derecho fundamental a la libertad de información y, además, esgrimió la imposibilidad técnica de llevar a cabo la desindexación solicitada. Ante dicha negativa los actores interpusieron demanda de juicio ordinario por vulneración del derecho al honor, a la intimidad y a la protección de datos de carácter personal que dio origen al proceso en septiembre de 2011.

Sentencia del Juzgado de Primera Instancia n°21 de Barcelona de 4 de octubre de 2012

El Juzgado de Primera Instancia número 21 de Barcelona dictó sentencia de fecha 4 de octubre de 2012 desestimando la declinatoria por falta de jurisdicción opuesta por El País y estimó la demanda.

La resolución consideró probado que El País no había adoptado mecanismos de control para evitar la indiscriminada difusión de la noticia, sino que por el contrario, y a fin de aumentar el beneficio económico derivado de la publicidad que se efectuaba en la página web, había introducido en aquélla las instrucciones precisas para incentivar que los robots de búsqueda la localizasen a través de datos identificativos como los nombres propios y la situasen en los primeros puestos de cualquier indagación efectuada a través de Google. La resolución consideró que los hechos que se publicaban en la noticia digital relativos a las personas demandantes -drogadicción y antecedentes penales- afectaban a su derecho a la protección de sus datos personales, y también a su intimidad y honor, al entrañar el menoscabo de su reputación, por lo que la Sentencia concluyó que la vulneración de los citados derechos fundamentales no quedaba justificada por la libertad de información del editor. En consecuencia, declaró que la difusión realizada por el diario de los datos de los demandantes suponía "*una vulneración del derecho al honor, intimidad y protección de*

datos" de los demandantes. Además, condenó a El País a implementar medidas dirigidas a impedir la aparición de la noticia en buscadores al incluir los nombres y apellidos de los demandantes, así como a abonar una indemnización de 7.000 euros a cada uno de ellos por los daños y perjuicios causados.

Sentencia de la Sección 14 de la Audiencia Provincial de Barcelona de 11 de octubre de 2013

Contra la Sentencia de 4 de octubre de 2012 del Juzgado de Primera Instancia número 21 de Barcelona Ediciones El País interpuso recurso de apelación. El País alegó en el recurso motivos casi idénticos a los que ya esgrimió en la contestación a la demanda de instancia y, adicionalmente, improcedencia de la cuantía de la indemnización acordada.

Los demandantes se opusieron al recurso de apelación y, simultáneamente, impugnaron la Sentencia de primera instancia, al considerar que la misma había incurrido en incongruencia omisiva respecto de las pretensiones de la demanda relativas al cese en el tratamiento de sus datos personales por la editorial o, subsidiariamente, la sustitución en la noticia y en el código fuente de la página web de sus nombres y apellidos por las iniciales de éstos, como respecto de la pretensión de que cualquier noticia que el diario El País publicase sobre el proceso omitiese los datos identificativos de las personas demandantes.

La Sentencia de la Sección Catorce de la Audiencia Provincial de Barcelona, de 11 de octubre de 2013, desestimó el recurso interpuesto por parte de El País y estimó la impugnación de los demandantes. La Sala en su pronunciamiento destacaba que el pernicioso efecto del antecedente penal sobre la reputación y la reinserción en la sociedad del ciudadano, había llevado a consagrar en el Código Penal el derecho a su cancelación una vez transcurrido el lapso de tiempo determinado en la norma, a fin de extinguir de modo definitivo todos los efectos de la pena, un derecho completado en la actualidad por el "derecho al olvido" del historial judicial. Sobre esta base la Sentencia realiza la ponderación de los derechos en conflicto, atendiendo, fundamentalmente, a los siguientes factores: primero, que las personas demandantes no eran personajes públicos ni ejercieron nunca cargo público alguno, por lo que entendía que la noticia publicada en Internet carecía de interés público o histórico; segundo, que el paso del tiempo había supuesto la

pérdida de la veracidad inicial de la información difundida y, tercero, que la publicación en Internet de la antigua noticia la había dotado de un grado de difusión mucho mayor que la que obtuvo la edición impresa, más restringida en términos geográficos y de tiraje. Todo ello justificaba que prevaleciesen los derechos fundamentales a la intimidad personal y el honor y a la protección de los datos personales, sobre la libertad de información del editor.

Respecto a las medidas adecuadas para restablecer el derecho, la Audiencia Provincial añadió, a las acordadas por la Sentencia del Juzgado, la condena a Ediciones El País a cesar en el uso de los datos personales en el código fuente de la página que contenía la noticia, no pudiendo constar en ella ni los nombres ni apellidos de las personas recurrentes, ni sus iniciales, como tampoco debían constar éstos en las noticias que el diario pudiera publicar sobre el proceso.

Sentencia de la Sala de lo Civil del Tribunal Supremo de 15 de octubre de 2015

Disconforme con el pronunciamiento de la Audiencia Provincial de Barcelona, "El País" presenta un recurso de casación ante el Tribunal Supremo que da lugar a la Sentencia número 545/2015, de 15 de octubre de la Sala de lo Civil del Tribunal Supremo; siendo esta la primera vez que el Tribunal Supremo se pronuncia acerca del derecho al olvido.

El recurso de casación se fundó en dos motivos. Por un lado, en la infracción del artículo 9.5 de la Ley Orgánica 1/82, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, según el cual las acciones de protección frente a las intromisiones ilegítimas caducan transcurridos cuatro años desde que el legitimado pudo ejercitarla. Y por otro, en la infracción del artículo 7 de dicha Ley Orgánica 1/82, en relación con el artículo 2.1 del mismo texto legal y el artículo 20.1.d de la Constitución Española, y ello por entender el recurrente que los hechos recogidos en la noticia eran veraces y de interés público, cualidades en ningún caso afectadas por el transcurso del tiempo.

El primer motivo del recurso de casación se fundamenta en la caducidad de la acción del artículo 9.5 LO 1/82. En base a ello El País alega que la publicación de la noticia original tuvo lugar en los años ochenta, mientras que el proceso de digitalización de la hemeroteca

de El País finalizó en 2002, habiendo transcurrido en ambos casos más de cuatro años desde que se difundió la información, por lo que la acción estaría prescrita.

El Tribunal Supremo, no obstante, desestimó dicho motivo por considerar que "*los daños producidos por el tratamiento de los datos personales que no cumpla los requisitos que establece 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*".

A continuación, el Tribunal aborda la concreta conducta enjuiciada, esto es, el tratamiento de datos de carácter personal derivado de la digitalización del texto y su posterior puesta a disposición de los buscadores por el editor.

Para ello parte de la interpretación que del concepto de tratamiento realiza el TJUE en base al artículo 2.b) de la Directiva 95/46/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 datos personales y a la libre circulación de estos datos (interpretación fijada en la sentencia de 6 de noviembre de 2003, asunto C-101/01 Lindqvist), posteriormente mantenida en la sentencia del ya mencionado Caso Google. El TJUE considera tratamiento "*cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales*". Por lo que, "*la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole*".

En concreto, el TS declara que los editores de páginas web tienen la posibilidad de indicar a los motores de búsqueda en Internet que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores mediante el uso de protocolos de exclusión como robot.txt, o de códigos como noindex o noarchive, razón ésta por la que el diario, continúa el TS "*es responsable del tratamiento de los datos personales de las personas demandantes contenidos en la página web cuestionada, y como tal está sometido a todas las obligaciones que se derivan (…)*".

Sentada la responsabilidad del editor de la página, la sentencia analiza el conflicto existente entre el ejercicio de la libertad de información que supone la edición y puesta a disposición del público de hemerotecas digitales en Internet y el respeto a los derechos de la personalidad como la protección de datos de carácter personal, la intimidad personal

y familiar y el honor cuando la información contenida en la hemeroteca digital afecta negativamente a la reputación del afectado.

Para la ponderación de los mencionados derechos el Tribunal parte del análisis del principio de calidad de los datos, según el cual la recogida y el tratamiento automatizado de datos de carácter personal debe regirse por los principios de adecuación, pertinencia, proporcionalidad y exactitud. Estableciendo al respecto que "*un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para esa finalidad puesto que el tratamiento de los datos personales debe cumplir con los principios de calidad de datos no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento*".

Respecto al principio de veracidad el Tribunal entiende que se cumple por parte de El País y sostiene al respecto que la noticia publicada por el demandado resulta accesible tal como fue publicada, con indicación de su fecha. Por lo que el debate no reside en si los datos personales son inveraces, sino en que estos puedan no ser adecuados a la finalidad con la que fueron recogidos y tratados inicialmente.

En cuanto a la libertad de información el Tribunal hace referencia a lo asentado en este sentido por el TEDH, que reconoce la aplicación de la protección del articulo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales a las hemerotecas digitales. Afirmando en este sentido 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. Mientras que la actividad de los medios de comunicación cuando transmiten noticias de actualidad constituye la labor fundamental de la prensa en una democracia, la puesta a disposición del público de las hemerotecas digitales, con archivos que contienen noticias que ya se han publicado, es considerada por el TEDH una función secundaria. Lo expuesto genera un margen mayor para lograr el equilibrio entre los derechos en conflicto, lo que redunda en favor de los derechos de la personalidad pues el ejercicio de la libertad de información puede considerarse menos intenso[41].

[41] CORTÉS FERNÁNDEZ, B. y MARTÍNEZ DE AGUIRRE MIRAL, J. "Comentario de la sentencia del tribunal supremo de 15 de octubre de 2015, (4132/2015)". Disponible

En aras de realizar la ponderación de los derechos en conflicto el TS se hace eco de la sentencia del ya mencionado Caso Google, que dispone que "*los derechos al respeto a la vida privada y familiar y a la protección de datos de carácter personal prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona*". En base a ello el TS entiende que "*en la ponderación deben primar los derechos de la personalidad si bien no de forma absoluta, pues deberá tomarse en consideración si existe un interés superior como el interés público. Interés que puede justificar que "cuando se trata de personas de relevancia pública, una información sobre hechos que afectan a su privacidad o a su reputación, aun sucedidos mucho tiempo atrás, esté vinculada a sus datos personales en un tratamiento automatizado como el que suponen las consultas a través de motores de búsqueda en Internet que indexan los datos personales existentes en las hemerotecas digitales. Por eso, cuando concurra este interés en la información, está justificado que puedan ser objeto de tratamiento automatizado informaciones lesivas para la privacidad y la reputación, vinculadas a los datos personales, siempre que sean veraces, cuando se trata de personas de relevancia pública, aunque los hechos hayan sucedido hace mucho tiempo"*

Poniendo esta última consideración en relación con el supuesto de hecho el TS indica, muy acertadamente, lo siguiente:

"*Ciertamente eran hechos veraces. Pero la licitud del tratamiento de los datos personales no exige solamente su veracidad y exactitud, sino también su adecuación, pertinencia y carácter no excesivo en relación con el ámbito y las finalidades para las que se haya realizado el tratamiento (art. 6.1.d de la Directiva y 4.1 LOPD). Y esos requisitos no concurren en un tratamiento de estos datos personales en que una consulta en un motor de búsqueda de Internet que utilice sus nombres y apellidos permita el acceso indiscriminado a la información más de veinte años después de sucedidos los hechos, y cause un daño desproporcionado a los afectados. El tratamiento de esos datos personales pudo cumplir estos requisitos de calidad de los datos en las fechas cercanas al momento*

en: https://www.boe.es/biblioteca_juridica/comentarios_sentencias_unificacion_doctrina_civil_y_mercantil/abrir_pdf.php?id=COM-D-2015-35_Comentarios_a_las_Sentencias_de_Unificacion_de_Doctrina__Civil_y_Mercantil__Derecho_al_olvido_en_internet (Acceso 2-04-2021)

en que los hechos se produjeron y conocieron, pero 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 (en este sentido, STJUE del caso Google, párrafos 92 y 93)"[42].

Una vez determinada la intromisión ilegítima de El País en los derechos de los demandantes el TS se pronuncia acerca de las medidas concretas dirigidas a garantizar su cesación inmediata, así como prevenir intromisiones inminentes o ulteriores. Para ello el TS realiza un análisis de los distintos pronunciamientos que se han ido dictando por los tribunales inferiores.

La sentencia de primera instancia, como ya se ha indicado, estimó íntegramente la demanda acordando la adopción de medidas tecnológicas por Ediciones El País (como la utilización de códigos robots.txt o instrucciones noindex, etc.) para que la página web de su hemeroteca digital en la que aparecía la información sobre las personas demandantes que las relacionaba con el tráfico de drogas y su dependencia de tales drogas, no pudiese ser indexada por los proveedores de servicios de Internet. Medida que el TS estima correcta al entender "*que supone dar satisfacción al derecho de cancelación que la normativa de protección de datos da a los afectados por un tratamiento de datos personales que no reúna los requisitos de calidad establecidos en dicha normativa, y no afecta desproporcionadamente a la libertad de información que ampara las hemerotecas digitales en Internet. Dicha medida permite que esas informaciones gravemente perturbadoras para el honor y la intimidad de los afectados, sobre hechos ocurridos muchos años antes, no resulten vinculadas a sus datos personales en las listas de resultados de los buscadores de Internet tales como Google, Yahoo, Bing, etc., al no existir un interés público ni histórico en que tal vinculación esté a disposición del público general mediante las listas de resultados de estos buscadores*."

Disconforme con el pronunciamiento el demandado recurrió en apelación alegando que "*la libertad de información amparaba su conducta pues la noticia se contenía en la hemeroteca digital como cualquier otra, y no podía proceder al borrado o modificación del artículo pues ello equivaldría a la retirada de los archivos existentes en las*

[42] Fundamento jurídico sexto de la Sentencia número 545/2015, de 15 de octubre de 2015.

hemerotecas". Recurso que fue desestimado por la Audiencia Provincial, estimando así la impugnación de los demandantes, adoptando dos medidas: la eliminación de los datos personales de los demandantes del código fuente de la página web que contiene la noticia, suprimiendo sus nombres y apellidos, no permitiendo siquiera que consten sus iniciales, y la adopción de medidas técnicas que eviten que la información pueda ser indexada por el propio buscador interno de www.elpais.com cuando se busque información utilizando el nombre y los apellidos de las personas demandantes.

Con estos antecedentes, el TS consideró que la primera de las medidas adoptadas supone un sacrificio desproporcionado, por excesivo, del derecho a la libertad de información. El llamado "derecho al olvido digital" no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día. Para sustentar esa consideración alega que "*las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la información. Por ello, las noticias pasadas no pueden ser objeto de cancelación o alteración*." Tomando además en consideración la doctrina establecida por el TEDH, que ha considerado que "*la protección de las hemerotecas digitales por el artículo 10 del Convenio implica que las noticias pasadas contenidas en ellas, a pesar de que su contenido pueda afectar a los derechos de las personas, no pueden ser eliminadas. 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» (STEDH de 16 de julio de 2013, caso Wergrzynowski y Smolczewski c. Polonia, párrafo 65, con cita de la anterior sentencia de 10 de marzo de 2009, caso Times Newpapers Ltd -núms. 1 y 2- contra Reino Unido).*" Por tanto, concluye el TS, *"la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión (en el sentido amplio del art. 10 del Convenio de Roma, que engloba la libertad de información), que excluye las medidas que alteren su contenido eliminando o borrando datos contenidos en ellos, como puede ser la eliminación de los nombres de las personas que aparecen en tales informaciones o su sustitución por las iniciales*."

Respecto a la segunda de las medidas adoptadas en apelación el TS considera que supone un sacrificio desproporcionado de la libertad de información protegida en el artículo 20.1.d de la Constitución Española.

"El riesgo para los derechos de la personalidad de las personas afectadas por la

información guardada en la hemeroteca digital no radica tanto en que la información sea accesible a través del motor de búsqueda interno del sitio web en que se encuentra alojada, pues se trata de una búsqueda comparable a la que efectuaban quienes acudían a las viejas hemerotecas en papel, como en la multiplicación de la publicidad que generan los motores de búsqueda de Internet, y en la posibilidad de que mediante una simple consulta utilizando los datos personales, cualquier internauta pueda obtener un perfil completo de la persona afectada en el que aparezcan informaciones obsoletas sobre hechos ya remotos en la trayectoria vital del afectado, con un grave potencial dañoso para su honor y su intimidad, que tengan un efecto distorsionador de la percepción que de esta persona tengan los demás conciudadanos y le estigmatice. Es por eso que esa información debe resultar invisible para la audiencia general de los usuarios de los motores de búsqueda, pero no para la audiencia más activa en la búsqueda de información, que debe tener la posibilidad de acceder a las noticias en su integridad a través del sitio web de la hemeroteca digital."

De tal manera que el TS revoca los pronunciamientos que afectaban al contenido y funcionamiento del buscador interno de El País, y que obligaban a dicho diario, en suma, a borrar todo rastro de los nombres, apellidos e incluso iniciales de los demandantes del texto original. Texto que, además, puede seguir siendo indexado por el buscador interno del diario. Los demás pronunciamientos de las sentencias de instancia y apelación relativos a la implementación de medidas para impedir la indexación por parte de terceros (Google, Yahoo!, Bing, etc.) se mantienen, al igual que la indemnización por daños morales estimada en 7.000 euros para cada uno de los demandantes.

El afectado, por tanto, siempre que no tenga el carácter de personaje público o no exista un interés igualmente público en vincular la información a su persona, puede conseguir una suerte de "oscuridad práctica" que le aísle de las búsquedas simples. Eso sí, ningún individuo tiene derecho a reescribir las publicaciones originales o a "impedir de modo absoluto que en una búsqueda específica en la propia hemeroteca digital pueda obtenerse tal información (...)"[43].

[43] CORTÉS FERNÁNDEZ, B. y MARTÍNEZ DE AGUIRRE MIRAL, J. "Comentario de la sentencia del tribunal supremo de 15 de octubre de 2015, (4132/2015)". Disponible en: https://www.boe.es/biblioteca_juridica/comentarios_sentencias_unificacion_doctrina_civil_y_mercantil/abrir_pdf.php?id=COM-D-2015-

5.2 SENTENCIA DE LA SALA TERCERA DE LO CONTENCIOSO-ADMINISTRATIVO DEL TRIBUNAL SUPREMO DE 27 NOVIEMBRE DE 2020

Resulta del todo necesario mencionar la sentencia del Tribunal Supremo de 27 de noviembre de 2020 por tratarse de uno de los pronunciamientos más recientes en la materia.

En esta sentencia el TS entiende que el derecho al olvido digital incluye no solo las búsquedas realizadas por nombre y apellidos de una persona, sino también aquellas efectuadas únicamente por los apellidos, siempre que esa información menoscabe el derecho al honor, a la intimidad, o a la propia imagen del interesado, carezca de interés público y pueda considerarse obsoleta.

Respecto a los antecedentes de hecho del caso, la Sala aborda el caso planteado por una persona que solicitó a Microsoft la desindexación de las URLs para las búsquedas realizadas no solo por su nombre completo, sino también por sus dos apellidos. Microsoft atendió la primera petición, pero rechazó la segunda basándose en que los dos apellidos no constituyen identificador inequívoco de una persona.

La AEPD tampoco accedió a su reclamación en relación con los dos apellidos, en base a la Doctrina del TJUE que se refiere a las búsquedas efectuadas en un buscador a partir del nombre de la persona.

La Audiencia Nacional confirmó la resolución de la AEPD al considerar que, conforme a la normativa del Registro Civil, las personas son designadas por su nombre y apellidos. Según el artículo 53 de la Ley de 8 de julio de 1957, sobre el Registro Civil "*Las personas son designadas por su nombre y apellidos*". Son, por tanto, el nombre y apellidos los que en nuestro derecho interno identifican de forma inequívoca a la persona. Por lo que, afirma, "*no se produce la misma identificación cuando se trata sólo de los apellidos, con independencia de que sean más o menos frecuentes*. *De esta forma,* concluye, *habiéndose*

35 Comentarios a las Sentencias de Unificacion de Doctrina Civil y Mercantil Derecho al olvido en internet (Acceso 2-04-2021)

atendido en el caso concreto el derecho de oposición ejercitado al realizar una búsqueda por el nombre de la persona afectada, esto es, por su nombre y apellidos, resulta ajustada a Derecho la resolución de la AEPD que desestima la reclamación respecto de la desindexación a partir de una consulta efectuada sólo por los apellidos del reclamante".

El TS estima el recurso de casación alegando que la sentencia impugnada no toma en la debida consideración el carácter garantista de las normas que regulan el tratamiento de datos personales, que deben interpretarse, entiende, a la luz de la jurisprudencia formulada en relación con la protección de los derechos fundamentales y libertades públicas de las personas físicas.

No resulta coherente para el TS reconocer el derecho al olvido cuando la búsqueda se realiza a partir del nombre (completo) de una persona y negarlo cuando se efectúa sólo a partir de los dos apellidos de esa persona, pues ello implica no tener en cuenta uno de los principios generales del Derecho de la Unión Europea, que propugna la interpretación uniforme en todos los Estados miembros de la normativa comunitaria europea. No es razonable que la aplicación de la Directiva 95/46/CE esté condicionada, en estos términos, por las diversas legislaciones internas reguladoras del Registro Civil, que determinan cuáles son los elementos identificativos del nombre y el estado civil de los ciudadanos de sus respectivos Estados[44].

No debe interpretarse, continúa alegando el TS, de forma tan restrictiva la referencia al tratamiento de datos de carácter personal relativos al nombre de la «persona afectada», en el sentido de que operaría sólo en las búsquedas efectuadas a partir del nombre de pila y los dos apellidos de la persona, invocando, para ello, la legislación reguladora del Registro Civil, porque supondría contravenir el espíritu y la finalidad tuitiva de la normativa de la Unión Europea, así como la normativa nacional de protección de datos de carácter personal, que no permiten distinguir, a estos efectos, que la búsqueda se efectúe con base en los apellidos de la persona afectada o del nombre y los dos apellidos de la citada persona[45].

Concluye el tribunal considerando que el criterio mantenido en la sentencia impugnada carece de apoyo en la normativa reguladora de la protección de datos personales de la Unión Europea y en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos

[44] Fundamento de Derecho tercero de la Sentencia del Tribunal Supremo de 27 de noviembre de 2020.
[45] Fundamento de Derecho tercero de la Sentencia del Tribunal Supremo de 27 de noviembre de 2020.

de Carácter Personal, pues supondría restringir, injustificadamente, el derecho, del que es titular la persona afectada, de exigir al gestor de un motor de búsqueda la eliminación de la lista de resultados, obtenida como consecuencia de una búsqueda realizada a partir de su nombre y apellidos o únicamente a través de sus apellidos.

> *"El ejercicio del derecho de oposición, rectificación o cancelación del tratamiento de datos, y, en su caso, del derecho al olvido, reconocido en el artículo 6.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con lo dispuesto en el artículo 18 del citado texto legal, en consonancia con lo dispuesto en los artículos 12 y 14 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, faculta a la persona interesada a exigir del gestor de un motor de búsqueda que elimine de la lista de resultados, obtenida como consecuencia de una búsqueda efectuada tanto a partir de su nombre completo o de sus dos apellidos, vínculos a páginas webs, publicados legalmente por terceros, que contengan datos e informaciones veraces, relativos a su persona, cuando la difusión de dicha información, relativa a su persona, menoscabe el derecho al honor, a la intimidad, o a la propia imagen del interesado, y carezca de interés público, y pueda considerarse, por el transcurso del tiempo, obsoleta, en los términos establecidos por la jurisprudencia del Tribunal de Justicia de la Unión Europea, del Tribunal Constitucional y del Tribunal Supremo*[46]."

5.3 DOCTRINA CONSTITUCIONAL: SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 58/2018, DE 4 DE JUNIO DE 2018

Agotadas todas las vías, tras la Sentencia del TS, el Ministerio Fiscal, legitimado por el artículo 46 de la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional, interpuso recurso de amparo constitucional ante el TC que dio lugar a la Sentencia

[46] Fundamento de Derecho cuarto de la Sentencia del Tribunal Supremo de 27 de noviembre de 2020.

58/2018 de 4 de junio de 2018[47], solicitando que se otorgase parcialmente el amparo a las personas demandantes por vulneración del derecho a la protección de datos del artículo 18.4 CE, en relación con los derechos al honor y a la intimidad del artículo 18.1 CE, y se declarase la nulidad de la Sentencia del TS, únicamente en lo relativo a la revocación del pronunciamiento consistente en prohibir la indexación de los datos personales de las personas demandantes de amparo para su uso por el motor de búsqueda interno de la hemeroteca digital gestionada por El País.

El objeto del recurso es, según la sentencia de amparo, al análisis del contraste entre los preceptos constitucionales regulados en el artículo 18.4 CE, en relación con la garantía del derecho al honor, y a la intimidad de las personas (artículo 18.1 CE).

Pronunciándose al respecto afirmando que si bien es cierto que "la libertad de información constituye no sólo un derecho fundamental de cada persona sino también una garantía de la formación y existencia de una opinión pública libre y plural, capaz de adoptar decisiones políticas a través del ejercicio de los derechos de participación", este derecho no es absoluto, sino que debe ser modulado por dos elementos: por un lado, el valor del paso del tiempo a la hora de calibrar el impacto de la difusión de una noticia sobre el derecho a la intimidad del titular de ese derecho, y por otro, la importancia de la digitalización de los documentos informativos, para facilitar el acceso a la información de todos los usuarios de internet.

El TC considera que en estos casos "*podría ponerse en duda la prevalencia del derecho a la información sobre el derecho a la intimidad de una persona que, pasado un lapso de tiempo, opta por solicitar que estos datos e información, que pudieron tener relevancia pública en su día, sean olvidados". Pero para el Tribunal, "la universalización del acceso a las hemerotecas, como la universalización del acceso a la información a través de los motores de búsqueda, multiplica la injerencia en los derechos a la autodeterminación informativa (art. 18.4 CE) y a la intimidad (art.18.1CE) de los ciudadanos*".

[47] Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-9534

Por lo que, en la resolución del conflicto, considera el TC, hay que tener en cuenta el equilibrio entre las libertades informativas y el derecho a la autodeterminación informativa, donde juega un papel importante el efecto del paso del tiempo sobre la función que desempeñan los medios de comunicación y, sobre la doble dimensión (informativa o investigadora) de esa función.

El fallo concluye afirmando que debe tenerse en cuenta que los motores de búsqueda internos de los sitios web cumplen la función de permitir el hallazgo y la divulgación de la noticia y que esa función queda garantizada, aunque se suprima la posibilidad de efectuar la búsqueda acudiendo al nombre y apellidos de las personas en cuestión, que no tienen relevancia pública alguna. Por tanto, "siempre será posible si existe una finalidad investigadora en la búsqueda de información alejada del mero interés periodístico en la persona investigada, localizar la noticia mediante una búsqueda temática, temporal, geográfica o de cualquier otro tipo". Por lo tanto, no son necesarios los datos personales de los solicitantes del amparo, que nada agregan al interés de la noticia, bastando las iniciales del nombre y los apellidos[48].

CONCLUSIONES

El derecho al olvido es una vertiente del derecho a la protección de datos frente al uso de la informática (artículo 18.4 CE), motivo principal por el que se ha analizado en el presente trabajo el recorrido del derecho a la protección de datos hasta su reconocimiento como derecho fundamental. Lo que ha sucedido de una manera gradual y nivelada, partiendo de un primer concepto, la libertad informática, entendida como un derecho perteneciente al círculo de la intimidad, para terminar por reconocer el derecho a la protección de datos como un derecho cuya tutela, en tanto derecho constitucional, únicamente es posible garantizar de forma efectiva afirmando su consolidación como derecho autónomo respecto de la intimidad. El TC fue el encargado de reconocer la autonomía y el estatus de derecho fundamental del derecho a la protección de datos en la sentencia número 292/2000.

[48] Nota informativa n° 60/2018 del Tribunal Constitucional.

Como ya se ha dejado de manifiesto, el derecho al olvido tiene un origen jurisprudencial y surge como respuesta a las reiteradas vulneraciones de la privacidad que los ciudadanos venían sufriendo en el entorno de internet, manifestadas a consecuencia de la invasión que las novedades tecnológicas han provocado en los derechos fundamentales. El TJUE fue el encargado de establecer las bases normativas en la Sentencia de 13 de mayo de 2014 para la regulación posterior de este derecho.

Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Los flujos de datos personales en esas operaciones son constantes, por lo que en mi opinión es necesario que se identifique con la mayor claridad posible los riesgos y oportunidades que el mundo de la red ofrece a la ciudadanía, para de esa manera poder abordarlos y que las personas en las operaciones en las que se involucren datos personales se encuentren amparadas por la ley.

Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. Algo que considero se ha logrado, al menos en parte, al reconocerse jurisprudencialmente el derecho al olvido, y positivizarse tanto en el RGPDP como en la LOPDPGDD. El Legislador español ha entendido que el derecho al olvido es merecedor de una protección reforzada en el ámbito de internet, por lo que en el artículo 15 LOPDPG regula expresamente el derecho al olvido, que se corresponde con el derecho al olvido que se establece en el artículo 17 RGPDP, regulando, además, en el Título X ”Garantía de los derechos digitales” dos derechos al olvido digital específicos: el derecho al olvido en búsquedas de internet (artículo 93) y el derecho al olvido en servicios de redes sociales y servicios equivalentes (artículo 94).

Respecto a la consideración del derecho al olvido como derecho autónomo, si bien es cierto que algunos autores lo han puesto en duda al considerar que no es un derecho autónomo o diferenciado de los llamados derechos ARCO. El TC ha sido el encargado de dilucidar esta cuestión en la Sentencia 58/2018, de 4 de junio. Estableciendo al respecto que el derecho al olvido es una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4. CE), y es también un mecanismo de garantía

para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo.

Del análisis realizado de los pronunciamientos que he considerado como los que revisten más interés en la materia se deduce que el derecho al olvido, como todos los derechos de nuestro ordenamiento, es un derecho limitado. Su ejercicio puede entrar en colisión con el derecho a la libertad de información o expresión, por lo que en cada caso concreto se debe realizar una ponderación de los derechos en juego para así evitar emplear el derecho al olvido como un mero instrumento para la censura, y preservar de esta manera todos los derechos del ordenamiento jurídico. La ponderación de los derechos en conflicto se realiza atendiendo fundamentalmente a los siguientes factores: primero, se valora si la persona o personas demandantes son personajes públicos o ejercen algún cargo público, pues de ser así, la información que se publique puede tener un interés público o histórico y prima en este caso dicho interés. Segundo, el paso del tiempo, que puede suponer la pérdida de la veracidad inicial de la información difundida. Teniéndose en cuenta, además, entre otros, la naturaleza de la información, así como su carácter sensible para la vida privada del afectado.

En lo que respecta al ejercicio de este derecho por los particulares considero que debe facilitarse más información sobre ello de manera que se simplifique su ejercicio al interesado. Si bien es cierto que la AEPD ofrece información al respecto, como ya se ha indicado, sobre el procedimiento que tiene que seguir el interesado para lograr el borrado de sus datos personales en una determinada página web, considero que sería necesaria la publicación por ejemplo de un manual de procedimiento en el que se recoja de manera sucinta el procedimiento a seguir, los supuestos en los que cabe su ejercicio y aquellos otros en los que no, de acuerdo todo ello con la norma vigente.

A modo de conclusión final señalar que, gracias a la jurisprudencia, tanto europea como nacional, se ha conseguido cubrir un vacío que existía hasta el momento que si bien es cierto era cubierto de cierta manera mediante los derechos ARCO, con el reconocimiento jurisprudencial del derecho al olvido digital y su posterior positivización se ha reforzado enormemente el derecho a la protección de datos en el ámbito de Internet. Dando así respuesta a la protección de la intimidad que los ciudadanos en determinados momentos puedan demandar frente a la injerencia de terceros que aprovechen las plataformas digitales para adquirir una información que de otra manera no tendrían.

BIBLIOGRAFÍA

AMÉRIGO ALONSO, J. "El marco normativo de la protección de datos en España." *El Cronista del estado social y democrático de derecho. Nº 66-69.*

ARENAS RAMIRO, M. "Reforzando el ejercicio del derecho a la protección de datos", en *Hacia un nuevo Derecho europeo de Protección de Datos*, en Tirant lo Blanch, Valencia, 2015.

CHÉLIZ INGLÉS, M.C., "El derecho al olvido digital. Una exigencia de las nuevas tecnologías recogida en el futuro Reglamento General de Protección de Datos", *Revista Jurídica Iberoamericana*, n°5, 2016.

CORTÉS FERNÁNDEZ, B. y MARTÍNEZ DE AGUIRRE MIRAL, J. "Comentarios de la Sentencia del Tribunal Supremo de 15 de octubre de 2015 (4231/2015). (Disponible en https://www.boe.es/biblioteca_juridica/comentarios_sentencias_unificacion_doctrina_civil_y_mercantil/abrir_pdf.php?id=COM-D-2015-35_Comentarios_a_las_Sentencias_de_Unificacion_de_Doctrina__Civil_y_Mercantil__Derecho_al_olvido_en_internet (Acceso 2-04-2021).

JIMÉNEZ-CASTELLANO BALLESTEROS, I. "El conflicto entre el derecho al olvido digital del pasado penal y las libertades informativas: las hemerotecas digitales", *UNED Revista de Derecho Político*, n°106, 2019.

MALDONADO RAMOS, I. "De nuevo sobre el derecho al olvido", *El notario del siglo XXI*, n°93, 2020.

MARTÍNEZ LÓPEZ-SÁEZ, M. "Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: La difícil conciliación entre las libertades económicas y la protección de datos personales", *Estudios de Deusto*, Vol.65/2, 2017.

MUÑOZ DE PEDRO, A. "Principales novedades de la ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Revista del gabinete jurídico de Castilla- La Mancha*, nº 16, 2018.

MURGA FERNÁNDEZ, J.P.: "Protección de datos y los motores de búsqueda en internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido", *Revista de Derecho Civil*, n°4, 2017.

PÉREZ LUÑO, A.E. “Nuevos derechos fundamentales de la era tecnológica: la libertad Informática”. *Anuario de Derecho Público y Estudios Políticos,* nº2, 1989.

PIÑAR MAÑAS, J. L., “Protección de datos. Las claves de un derecho fundamental imprescindible”, *El Cronista del Estado Social y Democrático de Derecho,* nº 88, 2020.

POLO ROCA, A. “El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado.” *UNED, Revista de derecho político*, nº108, 2020.

RALLO LOMBARTE, A. “De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)”. UNED, *Revista de derecho político*, nº100, 2017.

SÁNCHEZ-ESCRIBANO, M.M. “Libertad informática y protección de datos: desarrollo en la jurisprudencia del tribunal constitucional y tutela penal en el delito de descubrimiento y revelación de secretos”. *Anuario Iberoamericano de Justicia Constitucional*, nº19, 2015.

SANCHO LÓPEZ, M. “Estrategias legales para garantizar los derechos fundamentales frente a los desafíos del Big Data”, *Revista General de Derecho Administrativo*, n°50, 2019.

SANCHO LÓPEZ, M. “Límites del derecho al olvido. Veracidad y tiempo como factores de ponderación”, *Revista General de Derecho Constitucional*, n°32, 2020.

SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012.

TEJERINA, O., “Por qué la nueva LOPD (LOPDGDD) nos Inquieta, nos atormenta y nos perturba”, 2018. Disponible en: https://www.internautas.org/html/10141.html (Acceso 15-04-2021).

Jurisprudencia

Sentencia del Tribunal Constitucional número 254/1993 de 20 de julio de 1993.

Sentencia del Tribunal Constitucional número 292/2000 de 30 de noviembre de 2000.

Sentencia del Juzgado de Primera Instancia número 21 de 4 de octubre de 2012.

Sentencia de la Audiencia Provincial de Barcelona número 486/2013 de 11 de octubre de 2013.

Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. Caso Google Spain versus Agencia Española de Protección de Datos.

Sentencia de la Audiencia Nacional número 5129/2014 de 29 de diciembre de 2014.

Sentencia de la Sala de lo Civil del Tribunal Supremo número 545/2015 de 15 de octubre de 2015.

Sentencia del Tribunal Constitucional número 58/2018 de 4 de junio de 2018.

Sentencia del Tribunal Supremo número 1624/2020 de 27 de noviembre de 2020.