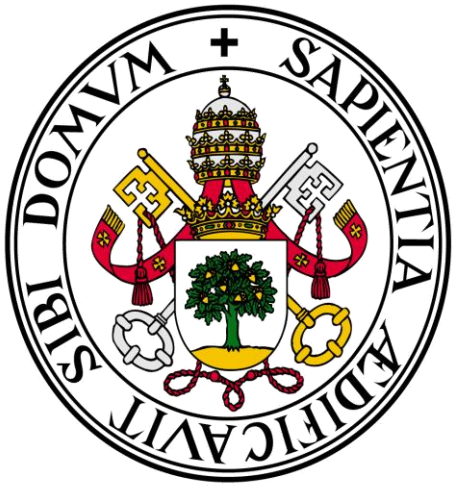

Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

Régimen jurídico – administrativo de la protección de datos

Presentado por:

Claudia Román Vaquero

Tutelado por:

Íñigo Sanz Rubiales

Valladolid, 19 de junio de 2018

ÍNDICE

7. MEDIDAS DE PROTECCIÓN DE LOS DATOS.

7.1. Medidas técnicas previas a la infracción.

7.1.1. Niveles de protección.

7.1.2. Clasificación reglamentaria de las medidas de protección.

7.2. Medidas a posteriori de la infracción.

7.2.1. Imposición de sanciones.

7.2.2. Otras consecuencias jurídicas en caso de infracción. Especial referencia a las Administraciones Públicas.

7.2.3. Consecuencias penales.

8. CASOS RECIENTES.

8.1. Infracciones por tratar o ceder datos sin consentimiento.

8.2. Infracciones en las relaciones entre privacidad y vida laboral.

8.3. Datos de carácter personal, tecnología y redes sociales.

9. UNA ESPECIAL REFERENCIA AL DERECHO AL OLVIDO.

9.1. Concepto.

9.2. Ámbitos de aplicación.

9.3. Titular.

9.4. Origen.

9.5. El derecho al olvido en el Reglamento General de Protección de Datos.

9.6. El Derecho al olvido en la normativa española.

9.7. Jurisprudencia delimitadora del derecho.

9.7.1. La doctrina del Tribunal de Justicia de la Unión Europea: el caso Google.

9.7.2. La jurisprudencia del Tribunal Supremo.

9.8. Procedimiento para su ejercicio.

10. CONCLUSIONES.

Resumen: En este trabajo se expone el régimen jurídico – administrativo de la protección de datos de carácter personal. Partiendo de su concepto, se analizarán todos sus aspectos, el origen de este derecho, sus características principales y sus principios rectores. Se enumerarán también los derechos de los titulares del derecho, a la luz tanto de la normativa española como de la comunitaria; y se indicarán los principales medios de protección de los mismos, al igual que se hará una sucinta referencia a la Agencia Española de Protección de Datos, el ente encargado del control de dicha protección. Finalmente, se tratará de un nuevo derecho en auge, el derecho al olvido, para tratar de delimitar sus caracteres y su importancia.

Todo ello, bajo la óptica del papel de los datos de carácter personal en la actual era de la información, la comunicación y la tecnología.

Abstract: This academic paper aims to expose the legal - administrative regime of personal data protection. Taking its concept as the basis of this project, all its aspects, the origin of this right, its main characteristics and its guiding principles will be analysed. Similarly, the rights of the holders of the right will also be listed, regarding both the Spanish and the Community regulations; in the same way, the main means of protection thereof will be pointed out, as well as a brief reference to the Spanish Agency for Data Protection, the entity in charge of the control of the aforementioned protection. Eventually, the right to be forgotten, a new right at its peak, will be discussed in order to try to delimit its aspects and its importance.

All of that presented through the role perspective of personal data in the current era of information, communication and technology.

Palabras clave: datos de carácter personal, derecho, protección, consentimiento, fichero, Administración Pública, tratamiento de datos, transparencia, derecho al olvido.

Key words: personal data, right, protection, consent, file, Public Administration, data processing, transparency, right to be forgotten.

Abreviaturas:

Art. – Artículo.

AEPD – Agencia Española de Protección de Datos.

CE – Constitución Española.

CP – Código Penal.

D.N.I. – Documento Nacional de Identidad.

Dr./Dra. – Doctor/Doctora.

LOPD – Ley Orgánica de Protección de Datos 15/1999.

Pág. – Página.

TJUE – Tribunal de Justicia de la Unión Europea.

RLOPD – Reglamento de la LOPD

1. INTRODUCCIÓN.

El objeto del presente trabajo se centra en el régimen jurídico – administrativo de la protección de datos de carácter personal. Este régimen será analizado partiendo del concepto de "dato de carácter personal" para, con base a dicho concepto, poder indicar todos los problemas que surgen en torno al mismo y poder comprender, así, la necesidad que tienen estos datos de contar con una especial protección.

De este modo, una vez analizada esa necesidad, podrá entrarse a conocer qué órganos son los encargados de hacer efectiva esa protección y de controlar el cumplimiento de la normativa; una normativa que, por otra parte, se encuentra en un proceso de cambio, debido a la entrada en vigor, el 25 de mayo de 2018, del nuevo Reglamento de la Unión Europea 679/2016, conocido como Reglamento General de Protección de Datos, que deroga la directiva que, hasta entonces, se ocupaba de esta materia (la Directiva 95/46/CE).

La entrada en vigor del Reglamento Europeo y las novedades que introduce, hacen necesaria una nueva regulación en materia de protección de datos en España, que se adapte a lo determinado por la normativa comunitaria. Por ello, se ha comenzado a elaborar un nuevo Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal que, no obstante, a día de hoy se encuentra en suspenso; de tal manera que, para poder determinar el régimen jurídico – administrativo aplicable a la protección de los datos de carácter personal, habrá que acudir al Reglamento Europeo y a la actual Ley Orgánica de Protección de Datos (Ley 15/1999), sin perder de vista, no obstante, el mencionado Proyecto de Ley.

La actual abundancia de instituciones y empresas que ofertan bienes y servicios, junto con el avance de las nuevas tecnologías, han conllevado lo que podría denominarse una "disminución de la intimidad", en el sentido de que hacen de los datos de quienes con ellas se relacionan, una exigencia, cuando no una necesidad.

Esto es así porque hay ciertos bienes y servicios, necesarios para la vida diaria de cualquier particular, para cuya recepción es previamente obligado que dicho particular proporcione sus datos personales. En estos supuestos, no cabe un caso contrario, es decir, no es factible que se reciba lo demandado sin haber aportado los datos personales exigidos.

Del mismo modo, el avance tecnológico ha contribuido a ese aporte de datos personales, ya prácticamente constante en la vida diaria de cualquier persona, porque se

exigen datos personales para algo tan sencillo como crearse una cuenta en una red social, una actividad que está a la orden del día, o en algunos casos de descargas de aplicaciones móviles.

En palabras del Profesor Dr. Alfonso Galán Muñoz: "*la tradicional definición del derecho a la intimidad, como derecho de corte exclusivamente negativo, se ha visto ya claramente superada por las posibilidades que nos ofrecen las modernas tecnologías de la información, tanto para captar, como para procesar o difundir datos que nos afectan muy directamente, lo que parece nos obligará a tener que replantearnos la tradicional conceptualización de dicho derecho fundamental o incluso a cambiarlo por uno más nuevo, amplio y adaptado a la nueva realidad de nuestra sociedad, como sería el denominado derecho a la privacidad".*[1]

Ahora bien, sin un nuevo concepto del derecho a la intimidad, y careciendo también de un derecho a la privacidad desarrollado como tal, los datos de carácter personal ostentan una trascendencia capital que hace preciso el otorgamiento de una protección jurídico – institucional que permita a los particulares ser titulares de una serie de derechos y garantías respecto de sus datos y, de forma complementaria, imponga a las instituciones y entidades con o sin personalidad jurídica, una serie de obligaciones para el tratamiento de los mismos, así como sanciones en caso de incumplimiento de estos deberes.

En España, además de contar con la correspondiente legislación, se creó la Agencia Española de Protección de Datos, un ente que vela por el cumplimiento de la normativa referente a los datos y proporciona a los particulares la información relativa a sus derechos, las medidas de protección con que cuentan y les facilita el acceso a la Justicia en materia de defensa de sus datos, ya que señala todos los elementos que deben aparecer en una denuncia sobre este tema, y facilita su interposición mediante su sede electrónica.

Lo que se deduce de todo esto, por tanto, es la indudable relevancia que tienen los datos de carácter personal a día de hoy, unos datos que están necesitados de una especial protección debido a las consecuencias negativas que puede llegar a tener la inobservancia de la legislación en las vidas y en la seguridad de los particulares de cuyos datos se trate.

2. MARCO NORMATIVO.

La protección de datos de carácter personal queda recogida en diversos instrumentos normativos, tanto a nivel nacional como europeo.

[1] GALÁN MUÑOZ, Alfonso. *La protección jurídica de la intimidad de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. Tirant Lo Blanch, 2014. Pág. 10.

En primer lugar, en España existe una normativa referente a los datos de carácter personal y a su protección.

La Constitución Española de 1978 no establece directamente el derecho a la protección de los datos personales de manera directa, pero este parece recogerse de manera implícita en el artículo 18.4:

> *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.*

Debe relacionarse este artículo (en adelante, art.) con otro precepto constitucional, el art. 20.4, interpretado en relación, a su vez, con el art. 20.1 d) de la Constitución:

> *1. Se reconocen y protegen los derechos: […]d) A comunicar o recibir libremente información veraz por cualquier medio de difusión.*
> *La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.*
>
> *4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.*

Siguiendo con la legislación nacional, se encuentra también la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Además, esta Ley cuenta con desarrollo reglamentario, de manera que debe atenderse también al Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la mencionada Ley Orgánica.

Del mismo modo, a esta materia, ya centrada en el ámbito de la Administración Pública, se refiere también la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en algunos preceptos.

Concretamente, hay que destacar los arts. 3.2 y 155, en sus apartados 1 y 2.

Así, el art. 3.2 establece que:

> *Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los*

datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

Finalmente, el artículo 155 de la misma ley, trata sobre las transmisiones de datos entre las Administraciones Públicas y, en sus apartados 1 y 2, determina que:

1. De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los interesados por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia, de acuerdo con la normativa reguladora de los mismos.

Por otra parte, también en Europa queda reconocido el derecho a que los datos personales sean protegidos. Destaca, primeramente, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

También en el ámbito europeo, se encuentra el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas respecto al tratamiento de sus datos personales y a la libre circulación de los mismos.

Cabe señalar que este Reglamento es de aplicación directa desde el 25 de mayo de 2018.

3. LOS DATOS.

3.1 Concepto.

Etimológicamente, el concepto de "dato" proviene del latín *datum*, "lo que se da".

Este término pretende contener toda representación simbólica de una recopilación de información sobre algo concreto, que permita su conocimiento exacto, o bien, deducir las consecuencias que se deriven de un hecho.

De esta definición se deriva que, considerados de manera individual, los datos no aportan, por sí mismos, ninguna información más allá de una situación o circunstancia. Sin embargo, en conjunto, su observación pasará a cumplir una función instruccional, e incluso instrumental, permitiendo realizar estudios comparativos en cualquier ámbito económico – social.

Hay diversos tipos de datos, destacando actualmente los numéricos o los informáticos, pero en lo referente a la protección de datos y su régimen jurídico, conviene centrarse en su variante de datos de carácter personal.

Sobre los datos de carácter personal, la propia normativa estatal aporta una noción, a efectos de delimitar el contenido y alcance interpretativo de la Ley Orgánica de Protección de Datos de Carácter Personal (en adelante, LOPD).

Así pues, desde un punto de vista estrictamente jurídico y ya centrado en el ámbito administrativo, para obtener este concepto hay que acudir al art. 3 LOPD.

3.1.1. Concepto e importancia de los datos de carácter personal.

El artículo 3 de esta ley aporta una serie de definiciones, entre las cuales, se contiene la de datos de carácter personal.

A ellos se refiere como "*cualquier información concerniente a personas físicas identificadas o identificables*".

Mediante la combinación de esta definición con el concepto general de "dato", puede concluirse que un dato de carácter personal es toda información, de cualquier tipo, que concierne a una persona física identificada, o bien, identificable.

El reglamento que desarrolla esta ley completa esta amplia definición, aunque no la delimita en gran medida, ya que continúa abarcando gran cantidad de información.

Específicamente, el reglamento considera dato personal cualquier información numérica, alfabética, acústica, fotográfica, gráfica o de cualquier otro tipo, siempre que concierna a una persona física identificada o identificable.

Siguiendo el concepto reglamentario, lo que puede deducirse respecto del contenido de "un dato" es que la información que aporta puede ser subjetiva u objetiva, de cualquier naturaleza y extensión y puede venir presentada en cualquier clase de soporte. Asimismo, debe referirse a una persona física que ha de ser identificada o identificable (esto último se tratará más adelante).

Viendo su amplitud y sus grandes posibilidades de contenido, es indudable que los datos de carácter personal están a la orden del día, ya que se encuentran presentes en gran parte de las adquisiciones de bienes y servicios que realizan las personas como consecuencia de su actividad empresarial, profesional o particular.

Por ello, gozan de singular trascendencia y están necesitados de un sistema que los proteja y los revista de una serie de garantías.

Queda reflejada esta importancia, para comenzar, en los textos comunitarios, como ocurre en el caso del art. 8 de la Carta Europea de Derechos Fundamentales. Dicho artículo reconoce el derecho de cada persona a la protección de sus datos de carácter personal:

> *1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.*
>
> *3. El respeto de estas normas estará sujeto al control de una autoridad independiente.*

La motivación de tal protección viene dada por las posibles consecuencias que pudieren derivar de una incorrecta o inadecuada utilización de dichos datos, porque el conocimiento o disposición de aquellos por parte de terceros podría implicar la violación de otros derechos, incluso fundamentales, del particular de cuyos datos se trate (como la intimidad, la igualdad y no discriminación o la libertad en sus diversas facetas).

Partiendo del mencionado precepto de la Carta Europea y siguiendo su estela, se han elaborado también directivas y reglamentos.

La más reciente es 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, sobre el tratamiento de los datos personales y a la libre circulación de estos datos.

Esta Directiva no estuvo exenta de cierta polémica en España.

El art. 7 de la Directiva, letra f), relativo al tratamiento de los datos personales, enumeraba una serie de requisitos para considerar lícito el tratamiento de los datos y, por su parte, la normativa española incorporaba una nueva exigencia para conseguir la licitud (que los datos figurasen en una fuente accesible al público); y se planteó si este añadido de la legislación nacional era o no jurídicamente correcto.

Parecía haber una dicotomía entre lo contemplado en la Directiva y los artículos 6.2 LOPD y 10.2 b) del Reglamento de esta ley (en adelante, RLOPD).

El asunto llegó a conocimiento del Tribunal de Justicia de la Unión Europea (TJUE), que resolvió en una sentencia de 24 de noviembre de 2011, declarando que el art.7 f) de la Directiva "*debe interpretarse en el sentido de que se opone a una normativa nacional que […] exige […] además que dichos datos figuren en fuentes accesibles al público*".[2]

Debido a la aplicación directa de que gozan reglamentos comunitarios, el art. 6.2 LOPD dejó de ser válido, en cuanto menoscababa dicha eficacia directa, y el Tribunal Supremo declaró nulo el artículo del RLOPD.

Merece la pena destacar, no obstante, que el conflicto subsanado por los tribunales dejó de tener sentido en mayo de este año, debido a que la Directiva 95/46 quedó derogada por el Reglamento 2016/679 del Parlamento Europeo y del Consejo, aprobado el 27 de abril de 2016 y aplicado desde el 25 de mayo de 2018, según su art. 99.2. Este, también por razón de su aplicabilidad y eficacia directas, subsana el problema en los mismos términos.

Siendo este conflicto una muestra de la consideración que ostentan y merecen los datos de carácter personal, parece lógico asumir la postura de José Luis Piñar Mañas, quien postula que la noción de dato de carácter personal es la que "*entrelaza sin fisuras la privacidad y el derecho*

[2] GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "El interés legítimo en la protección de datos*". Revista de Derecho UNED*. Nº 16, 2015. Pág. 424.

a la identidad" y continúa diciendo que, por ello, son los datos de carácter personal los que "*definen y configuran la identidad de las personas. De ahí la importancia que reviste el dato personal, íntimo o no, en la construcción de la identidad diferenciada de todas y cada una de las personas"*.[3]

Pone así Piñar de manifiesto la estrecha relación existente entre los datos de carácter personal y otros derechos fundamentales. Concretamente, de su afirmación se deriva la relación con el derecho a la identidad y el derecho a la intimidad, que se recoge en el mismo precepto constitucional que el derecho a la protección de datos personales (este último, implícito).

Sin embargo, no todos los datos se ajustan a la definición dada por el art. 3 LOPD para los datos de carácter personal, por lo que es necesario acotar este concepto haciendo referencia a ciertos datos concretos.

La LOPD, en su art. 2, declara que su ámbito de aplicación se restringe a los datos de carácter personal que se encuentren registrados en un soporte físico que los hiciere susceptibles de tratamiento, así como a toda modalidad de uso posterior de esos datos, tanto por el sector público, como por el sector privado.

Este concepto, conforme al desarrollo tecnológico acontecido en el siglo XX, en que los datos comenzaban a registrarse en soportes informáticos, quedaba anticuado. La justificación se encuentra tendiendo a su tenor literal, por el que gran cantidad de datos que, de estar almacenados en soportes físicos, tendrían la consideración de datos de carácter personal, la perdían al estar almacenados (en todo o en parte) en soportes informáticos.

Esta norma contenía una delimitación de su esfera de eficacia, que, en atención a la evolución de las nuevas tecnologías y las consiguientes necesidades sociales, quedaba relegada cada vez más a un segundo plano y, como consecuencia, una gran cantidad de datos almacenados en otros soportes no podrían quedar sujetos al ámbito protector de esta ley nacional.

---

[3] PIÑAR MAÑAS, José Luis. "*Comentario de José Luis Piñar Mañas al artículo 3: Requisitos para que los datos estén protegidos por la LOPD"* en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Varios autores. Dirigido por TRONCOSO REIGADA, Antonio. Aranzadi, 2010. Pág. 186.

Para hacer frente a las restricciones de esta norma material autolimitada, se acudió a la Directiva 95/46/CE, la cual delimitó su ámbito de aplicación de forma más amplia en el art. 3.1, incluyendo los datos total o parcialmente automatizados.

Aunque se interpretasen ambos preceptos conjuntamente, incluyéndose los datos almacenados en cualquier tipo de soporte, si se continúa analizando la literalidad de ambos, se observa que hay sendas menciones al tratamiento de los datos, que no es más que la recogida de los datos, automatizada o no, en ficheros (que serán tratados más adelante).

Este tratamiento no puede obviarse, ya que, junto al concepto de dato y dato de carácter personal, será lo que determine qué datos quedarán amparados por la LOPD.

Por lo tanto, quedarán fuera de la protección que otorga esta ley los datos o los conjuntos de datos que no se encuentren sometidos a tratamiento (es decir, almacenados en ficheros), o que no sean susceptibles de serlo, así como aquellos datos no destinados a ser almacenados en ellos.

Sin embargo, los datos no amparados por la LOPD no quedan desprotegidos, sino que habrá que acudir a otros marcos jurídicos, como el Derecho penal o el Derecho de daños, debido a los derechos e intereses personales que subyacen tras cada dato.

3.1.2 Datos no incluidos en el concepto, a efectos de la legislación.

Ahora bien, pese a todo lo analizado respecto de los datos de carácter personal, hay información que, a efectos de la legislación protectora de los datos, no se encuentra incluida en el concepto de dato personal, y es preciso conocer cuáles son esas informaciones y qué características son las que las excluyen del amparo de la LOPD.

Concretamente, hay dos aspectos que, aunque suponen la recogida y almacenaje de datos de gran importancia, no van a quedar recogidos en el ámbito de aplicación de esta ley. Son los referidos a los datos de las personas jurídicas, y a los datos de las personas fallecidas.

Primeramente, hay que referirse a los datos de las personas jurídicas. Es preferible abordarlas en primer lugar, ya que es el propio art. 3 LOPD el que descarta de forma expresa dichos datos de su ámbito de aplicación, considerando dato personal a cualquier información sobre personas *físicas*. Igualmente se pronuncia el art. 5.1 a) RLOPD.

No debe olvidarse que los datos no incluidos en la protección que otorga la LOPD, no quedan desamparados, sino que quedan protegidos por otras leyes. Así pues, la protección de los datos de las personas jurídicas queda subsumida en el Real Decreto Legislativo 1/2004,

de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Catastro Inmobiliario, concretamente en su art. 51:

> *A efectos de lo dispuesto en este título, tienen la consideración de datos protegidos el nombre, apellidos, razón social, código de identificación y domicilio de quienes figuren inscritos en el Catastro Inmobiliario como titulares, así como el valor catastral y los valores catastrales del suelo y, en su caso, de la construcción de los bienes inmuebles individualizados.*

Se concluye, por lo tanto, que los datos obtendrán una protección diferente, según quién sea su titular.

Este hecho tiene una justificación que la Agencia Española de Protección de Datos (en adelante, AEPD) supo plasmar magníficamente en su memoria del año 1999. Declara en ella, textualmente, que:

"*El fundamento de la delimitación de este ámbito de aplicación reside en que si la protección de los datos personales se refiere a la intimidad personal y familiar, no puede entenderse que las empresas gocen de la citada intimidad. Por tanto, en principio no puede ser aplicable a esas personas la protección, ni siquiera cuando su actividad se identifique plenamente con la de una persona física determinada, habida cuenta que el ámbito personal que se protege debe entenderse distinto del empresarial*".[4]

Para terminar con lo relativo a los datos de las personas jurídicas, solo resta saber cuándo se considera que una información o dato pertenece a una persona jurídica o, si por el contrario, se está ante un dato de una persona física.

Vuelve a ser la Agencia Española de Protección de Datos quien proporcione los criterios para determinarlo, esta vez en el año 2005, en la Resolución del procedimiento sancionador PS/00049/2005, de 15 de julio. En ella, remarca que los datos de las personas jurídicas no quedarán en ningún caso amparadas por la LOPD.

Además, en cuanto a los supuestos que pudieran suscitar dudas, como es el caso de las personas físicas empresarias o profesionales, mantiene que se les excluirá de ese amparo cuando su actividad pueda distinguirse de manera inequívoca de su actividad privada. Respecto de los empresarios, añade otro elemento distintivo para dicha exclusión: que su actividad se encuentre organizada en forma de empresa.

[4] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Memoria.* 1999. Pág. 119.

En segundo lugar, hay que destacar también el supuesto de los datos relativos a personas fallecidas. La no aplicación de la LOPD a estos casos viene determinada esta vez por el RLOPD, en su art. 2.4:

> *"Este reglamento no será de aplicación a los datos referidos a personas fallecidas (…)".*

La motivación de la inaplicación de la LOPD a estos supuestos procede de una estrecha conexión con el Código Civil, para el que la personalidad civil se extingue con la muerte de la persona (art. 32 del Código) y, en consecuencia, para esta rama del Derecho, el fallecido ya no es persona física. Consiguientemente, la LOPD dejará de aplicarse a los fallecidos porque el propio Derecho Civil español ya no los considerará personas físicas.

Finalmente, es reseñable frente a lo desarrollado sobre los datos de los fallecidos el hecho de que, en el caso de que dichos datos permitiesen identificar a una persona viva, sí que resultaría aplicable la LOPD, en la medida en que sí afectarían y, en cierto modo, se referirían a una persona física.

3.1.3. Datos personales no sujetos a la tutela de la LOPD

Frente a los datos que, a efectos de la LOPD, no se incluyen en el concepto, se encuentra un caso similar, pero radicalmente diferente: los datos personales que no quedan protegidos por la LOPD.

La diferencia se encuentra en que, si en el apartado anterior se trataba de datos de gran relevancia que no quedaban amparados por la LOPD, aquí de lo que se va a tratar es de datos personales referidos a personas físicas e incorporados a un fichero (o susceptibles de este tratamiento) que, aunque deberían incluirse en el ámbito de aplicación de la ley, no resultan protegidos por ella.

Estos supuestos quedan determinados en el art. 2.2 LOPD, pero merece la pena detenerse en los especificados por el reglamento, que son dos casos observables con habitualidad y que, por ello, deben ser destacados: los datos de los empresarios individuales, y los datos "de contacto". Aparecen en el art. 2.2 también, pero del RLOPD.

Prueba de la similitud con el apartado anterior es el primero de estos supuestos: los datos de los empresarios individuales.

En el apartado previo, se especificó que sus datos no quedarían subsumidos en la LOPD cuando su actividad pudiera distinguirse de manera inequívoca de su actividad privada. Ahora bien, se hacía referencia a los datos en general, del empresario en cuanto empresario; mientras que a lo que ahora hay que referirse es a los datos personales del empresario en cuanto persona física.

El modo de distinguir cuándo se está ante cada una de estas situaciones se determina en una sentencia de la Audiencia Nacional, de 29 de marzo de 2006: "*[…] Labor de diferenciación a la que cabe aplicar dos criterios distintos y complementarios: Uno, el criterio objetivo de la clase y la naturaleza de los datos tratados, según estén en conexión y se refieran a una esfera (la íntima y personal) o a otra (la profesional) de la actividad. Otro, el de la finalidad del tratamiento y circunstancias en que este se desarrolla, criterio este que operaría en aquellos casos en que alguno de los datos profesionales coincida con los particulares […]).* [5]

Lo que se pone de manifiesto con esta sentencia es: cuando el dato personal se refiera a la esfera íntima y personal del empresario, o bien, coincidiendo el dato con un dato profesional y su tratamiento y circunstancias vayan referidos a esa esfera personal, el dato quedará amparado por la LOPD. En caso contrario, quedaría fuera de su ámbito de aplicación, estándose en uno de los casos tratados en el apartado anterior.

Por otro lado, se encuentran mencionados en el RLOPD los datos "de contacto". Cabe subrayar que el reglamento establece un *numerus clausus* de los datos que pueden ser sometidos a tratamiento para poder ser considerados datos de contacto. Significa esto que, de incorporarse un dato diferente a los determinados en el listado, ya no podría hablarse de una excepción en la aplicación de la LOPD, puesto que dicha excepción no podría operar por contradecir al reglamento.

Se incluyen como datos de contacto los siguientes: nombre y apellidos, las funciones o puestos desempeñados, la dirección postal o electrónica, teléfono y número de fax profesionales.

No puede prescindirse del hecho de que se traten de datos "de contacto", esto es, los datos personales recabados solo deberán aprovecharse en cuanto datos para contactar en el

[5] PIÑAR MAÑAS, José Luis. "*Comentario de José Luis Piñar Mañas al artículo 3: Datos personales no sujetos al régimen de la tutela de la legislación de protección de datos"* en *Comentario a la Ley Orgánica*… cit. Pág. 201.

ámbito de las actividades propias de las relaciones profesionales y empresariales y nunca con otros fines diferentes.

3.1.4. Supuestos cuya inclusión en el concepto es dudosa.

Para poder terminar de perfilar por completo el concepto de dato de carácter personal, habrá que hacer referencia a una serie de informaciones relativas a las personas físicas que suscitan la siguiente duda: ¿deben o no incluirse en el concepto de dato personal?

Pese a que algunas de esas informaciones, aunque es cierto que contienen datos personales, o de su interpretación pudieren deducirse estos, no plantean esa duda por su naturaleza o su soporte (un ilustrativo ejemplo son los dibujos infantiles en las pruebas neuro - psiquiátricas, que aportan datos sobre el ánimo de los niños, a los que médico y progenitores podrían acceder), hay una serie de casos más concretos que sí permiten plantearse de manera más seria su inclusión o no en el concepto.

Llaman la atención 4 tipos de informaciones en este sentido: el número de teléfono, el número del Documento Nacional de Identidad (en adelante, DNI), las imágenes y la dirección IP.

La disyuntiva relativa a la inclusión del número de teléfono en el concepto hace referencia a los teléfonos de las personas físicas, y se concreta en si es el número, por sí solo, el que constituye un dato personal o si, además, se necesita que esté adscrito a un titular.

Una sentencia de la Audiencia Nacional, de 26 de enero de 2005 [6], afirmó al respecto que un número de teléfono puede calificarse de dato personal siempre que a través del mismo pudiera identificarse a su titular, aun no estando asociado a la misma o a cualquier otro dato que permita su identificación.

Debe añadirse a esta cuestión el número de teléfono móvil. Es otra sentencia de la Audiencia Nacional la que alude a este supuesto. El 17 de septiembre de 2008 declaró que, en caso de no quedar acreditado "*que a través del número de teléfono móvil se haya identificado al titular del mismo o que a partir del número fuese posible tal identificación*",[7] no podrá encajar el número de teléfono móvil en el concepto que aporta el art. 3 LOPD de dato de carácter personal.

[6] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, Sección 1. 26-01-2005. ROJ: SAN 308/2005. Nº Recurso: 1258/2002. Ponente: María Luz Lourdes Sanz Calvo.

[7] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, sección 1. 17-09-2008. ROJ: SAN 3250/2008. Nº Recurso: 353/2007. Ponente: Elisa Veiga Nicole.

Coincide la Audiencia Nacional, por lo tanto, en que para poder considerar un número de teléfono como un dato de carácter personal, es necesario que se adscriba o permita la identificación de una persona.

Aunque es una postura correcta y asumible en el caso de los números de teléfono "fijos", hay que tener en cuenta la fecha la sentencia que trata de los números de móvil, ya que es anterior a la creación de aplicaciones y plataformas que se sirven de este y, a partir del cual, pueden obtenerse otros datos de las personas físicas que las utilizan.

Quizá el ejemplo más ilustrativo de esta obsolescencia sea la aplicación WhatsApp. Creada en el año 2009 y utilizada a nivel mundial, esta aplicación de mensajería instantánea se basa en los números de teléfono móvil para la creación de cuentas en la aplicación. La propia aplicación, a través del número de teléfono móvil de la cuenta, accede a la agenda de contactos del dispositivo móvil (en la que figuran nombres, apellidos, números de teléfono, e incluso, cuentas de correo electrónico) y así permite el envío y la recepción instantánea de mensajes entre el usuario de la cuenta y sus contactos.

De este modo, la aplicación ya tiene acceso tanto al número de móvil del usuario, como a varios datos personales de sus contactos. Además, la propia aplicación permite la opción de que el usuario introduzca un nombre que le identifique cuando envíe mensajes a contactos que no tengan en su agenda a ese usuario como contacto; permite poner una imagen como "fotografía de perfil" de la cuenta y en ocasiones visionar las fotografías que los contactos del usuario hayan establecido como perfil; y finalmente, permite la creación de grupos en los que el usuario y, tanto sus contactos como otras personas a quien puede no conocer siquiera, intercambien mensajes, figurando los números de móvil y, si los hubiera, sus nombres de usuario y siendo ambos datos visibles para todos los integrantes de dichos grupos.

Lo que con esto se pretende demostrar es que, mediante WhatsApp y las numerosas aplicaciones existentes del mismo estilo, es simplemente mediante el número de teléfono móvil por el que se puede tener acceso a datos de las personas físicas sin conocer la adscripción del número a esas personas, y puede accederse también a su nombre o incluso conocer su apariencia física y, por lo tanto, debería considerarse el número móvil un dato de carácter personal por sí solo, ya que el Derecho debe adaptarse a la realidad y las necesidades sociales y acomodarse a la evolución de las nuevas tecnologías, con el fin de evitar lagunas normativas que conlleven la impunidad de posibles vulneraciones de derechos.

Otra clase de información sobre cuya inclusión en el concepto de dato de carácter personal se duda es el número de DNI.

Atendiendo al art. 1, apartados 1, 2 y 3 del Real Decreto 1553/2005, de 23 de diciembre, regulador de la expedición del documento nacional de identidad y sus certificados de firma electrónica, se encuentran la definición y la finalidad de dicho documento:

> *1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.*
> *2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo.*
> *3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.*

En origen, la AEPD mantuvo para el número de DNI la misma posición que venía manteniendo para los números de teléfono: solamente tendría el carácter de dato personal si implicase su adscripción a una persona física, la cual, fuese la titular de dicho número.

Sin embargo, hay que atender al concepto de dato personal que aportan tanto la LOPD como su reglamento, así como a la propia noción que Piñar Mañas aporta del término, en tanto vínculo entre privacidad e identidad, y deben relacionarse con la finalidad que el Real Decreto 1553/2005 otorga a esta información numérica. Dicho fin no es otro que la acreditación de la identidad del titular del número.

Es en base a esta relación concepto – finalidad, por lo que la AEPD modifica su postura y, en tanto el DNI identifica por sí solo y de manera plena a su titular, debe quedar incluido en el concepto de dato de carácter personal y subsumirse a la LOPD.

Una muestra cercana de la relevancia que tiene el número de DNI para, por sí solo, identificar a su titular, es el propio campus virtual de la Universidad de Valladolid. Dicha plataforma exige dos requisitos para acceder a su contenido: la identificación por medio del número de DNI y una clave elegida por el titular del mismo e interesado en acceder a los contenidos de la plataforma. Esto sucede también para otras plataformas de la Universidad de Valladolid, como SIGMA, el portal de servicios, o el correo electrónico que proporciona la Universidad a sus alumnos y profesores. Sirva esto, pues, como ejemplificación de la necesidad de que el número de DNI sea efectivamente reconocido como un dato de carácter personal y sea, por ello, protegido por la LOPD y su reglamento.

En tercer lugar, se habla de la imagen como información de dudosa inclusión en el concepto. Así, para la solucionar esta cuestión debe recordarse el art. 5 RLOPD, que define el dato de carácter personal como "*cualquier información […] gráfica, fotográfica […] concerniente a personas físicas identificadas o identificables*". Es, pues, el propio artículo el que considera la imagen un dato de carácter personal.

Siguiendo de nuevo a Piñar Mañas, este es tajante al respecto. Tras corroborar la literalidad de este art. 5 RLOPD, añade: "*no creo que sea necesario insistir más en este tema. La imagen es un dato personal desde el momento en que pueda identificar a una persona".* [8]

A modo de apunte, manteniendo la concisión y exactitud de su afirmación, es útil la misma para reiterar la idea de considerar el número de teléfono móvil por sí solo un dato de carácter personal que debe proteger la LOPD, por el hecho de que ciertas plataformas permitan acceder a una imagen de la persona física mediante su dicho número.

En último lugar, en conexión con el desarrollo tecnológico, se ha planteado si considerar o no la dirección IP un dato de carácter personal.

La IP es un sistema de nomenclatura, por el cual, las máquinas (principalmente, los ordenadores) pueden conectarse entre sí. Así, puede definirse la IP como un sistema numérico utilizado como identificador único online.

Esta IP puede ser pública, lo cual implica que puede cambiar para el mismo dispositivo, o bien, privada, que implica que el dispositivo en cuestión va a mantener su IP porque esta ha sido contratada de manera fija con el proveedor de línea.

Es la IP pública, la IP resultado del puente que forman los routers entre Internet y cada dispositivo conectado a la red, la que se ofrece con cada conexión. Esta IP es asignada por el operador de Internet y es a partir de ella de la que pueden llegar a obtenerse datos, y de la cual, se duda su inclusión en el concepto de dato de carácter personal.

Su inclusión en el concepto es un tema que continúa debatiéndose actualmente, pero es reseñable la consideración que le otorga la AEPD, que en 2003 declaró que: "*en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal […] que permitan identificarlo[…]y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia*

[8] PIÑAR MAÑAS, José Luis. "*Comentario de José Luis Piñar Mañas al artículo 3: Algunos supuestos de informaciones respecto de las que se ha planteado su inclusión o no en el concepto de dato personal"* en *Comentario a la Ley Orgánica*… cit. Pág. 205.

del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos". [9]

Destaca la distinción que señala la AEPD entre direcciones IP fijas y dinámicas y, a pesar de que ambas terminarán, en la mayoría de los casos, considerándose datos de carácter personal, sitúa Piñar Mañas la diferenciación entre ambas clases en la mayor o menor facilidad con la que conseguir datos personales partiendo de cada tipo de dirección IP. Así pues, manifiesta que: "*la primera puede considerarse apenas sin problemas como un dato personal. La segunda solo en la medida en que pueda realmente identificar a una persona, lo que en no pocas ocasiones exigirá completar la información de la IP con otra relevante que permita identificar no solo al ordenador […] sino al usuario".* [10]

3.1.5 Los datos especialmente protegidos.

Para terminar de perfilar los caracteres y el contenido de los datos personales, hay que hacer una última precisión, ya que es preciso conocer que, dentro del amplio espectro de datos de carácter personal, aparece una clase que goza de un excepcional amparo: los datos especialmente protegidos.

A ellos alude el art. 7 LOPD, y son, en esencia, las informaciones sobre los elementos a que se refiere el art. 16.2 de la Constitución: ideología, religión y creencias. El art. 7 LOPD añade a este elenco, además, la información sobre la afiliación sindical, el origen racial, la salud y la vida sexual. Se trata de datos cuya recogida y tratamiento implican una especial injerencia en el ámbito más privado de la esfera personal de los particulares y, por ello, necesitan un nivel de protección más amplio y garantista que el resto de datos personales.

Este listado de informaciones puede dividirse en dos grupos de datos especialmente protegidos, en función de la protección y garantías en su tratamiento: por un lado, ideología, religión, creencias y afiliación sindical solo pueden obtenerse mediando consentimiento expreso y por escrito de la persona a quien alude dicha información, teniendo siempre derecho a no prestarse la misma; por otro, el origen racial y la información sobre la salud y

[9] PIÑAR MAÑAS, José Luis. "*Comentario de José Luis Piñar Mañas al artículo 3: Algunos supuestos de informaciones respecto de las que se ha planteado su inclusión o no en el concepto de dato personal"* en *Comentario a la Ley Orgánica*… cit. Pág. 207.

[10] PIÑAR MAÑAS, José Luis. "*Comentario de José Luis Piñar Mañas al artículo 3: Algunos supuestos de informaciones respecto de las que se ha planteado su inclusión o no en el concepto de dato personal"* en *Comentario a la Ley Orgánica*… cit. Pág. 210.

la orientación o vida sexual, solo podrán recabarse y recogerse en ficheros con consentimiento expreso (no necesariamente por escrito) y por razones de interés general).

3.2. ¿De quién pueden obtenerse los datos?

Una vez delimitado el amplísimo concepto de dato de carácter personal, pueden ya analizarse los siguientes elementos relativos tanto a los datos, como al acto de su recogida para su posterior tratamiento: titulares, modo de recogida, almacenamiento…

Puesto que la normativa referida a estos datos no cesa de precisar que se tratan de informaciones sobre personas físicas identificadas o identificables, parece lógico continuar el análisis del "dato" concretando quiénes son esas personas físicas identificadas o identificables, y delimitar otros conceptos trascendentes a efectos del tratamiento de los datos de carácter personal: afectados o interesados.

3.2.1. Personas identificadas o identificables.

Pese a que la LOPD menciona a estas personas identificadas o identificables, no aporta un concepto que determine qué son ni quiénes pueden considerarse tales.

Por lo tanto, atendiendo a la visión de Carlos María Romeo Casabona[11], una persona identificada sería aquella para quien existe una correspondencia entre su identidad y cualquier dato o rasgo identificador (biológico, cultural o socioeconómico) siempre y cuando la identidad de esa persona sea conocida.

En cuanto a las personas identificables, ya que no hay una correspondencia cierta y clara entre una identidad y unos datos, va a ser necesario indagar en busca de dicha vinculación. Esto será posible debido a que lo característico de una persona identificable es que puede averiguarse su identidad y, por tanto, es una persona de identidad desconocida pero susceptible de ser identificada.

Para poder identificar a una persona, no obstante, deben utilizarse unos medios que ni la LOPD, ni su reglamento ni el Reglamento 2016/679 prevén. Lo único que al respecto establecen estas normas es que dichos indeterminados medios deberán ser utilizados de forma razonable, sin desproporciones en cuanto a plazos y gastos. Estos requisitos, a falta

[11] ROMEO CASABONA, Carlos María. "*Comentario de Carlos María Romeo Casabona al art. 3: persona identificada o identificable",* en *Comentario a la Ley Orgánica*… cit. Págs. 227 y 228.

de mayor especificación, se entenderán cumplidos en atención a la identidad de la persona y la finalidad de su identificación.

3.2.2. Los afectados o interesados.

Los afectados o interesados aparecen definidos en el art. 3 LOPD como las personas físicas titulares de los datos objeto de tratamiento. Es esta una definición que no aporta nada nuevo, ya que lo único que determina es que son los titulares de los datos de carácter personal que se recogen y almacenan en ficheros.

A pesar de ello, es interesante el hecho de que existen una serie de exclusiones a este concepto: las personas jurídicas, las personas fallecidas y los no nacidos no se consideran por la normativa como titulares de datos de carácter personal.

Ya se ha tratado el motivo de esta exclusión para las personas jurídicas y los fallecidos, pero puede resultar sorprendente el hecho de que los datos de los no nacidos sí se consideren datos de carácter personal, pero, simultáneamente, no tengan la cualidad de titulares de los mismos.

Los datos que pueden referirse a los no nacidos son aquellos sobre su filiación biológica y sobre su estado de salud, siendo informaciones que no pueden esperar hasta el nacimiento de la persona para ser protegidas. El motivo es que tienen un carácter excepcionalmente sensible y, no obstante, son susceptibles de difundirse a terceras personas (normalmente, a la familia de ese *nasciturus*), justificando esto el hecho de que se consideren datos especialmente protegidos.

3.3. ¿Quién y para qué puede obtener los datos?

Estas cuestiones son, en cierto modo, sencillas de responder. En primer lugar, cualquiera puede obtener datos, ya sea persona física, jurídica o ente sin personalidad jurídica. Cualquier particular puede almacenar datos personales sobre otras personas físicas, y lo mismo ocurre con las empresas o las Administraciones Públicas.

Responder a la segunda cuestión supone no poder entrar en detalles, ya que los fines con que se recogen y almacenan datos son tan numerosos y variados que sería imposible enumerarlos todos. Pero, por poner algunos ejemplos, los datos pueden obtenerse como requisito previo a la prestación de un servicio, a efectos de notificaciones, para realizar operaciones comerciales, para determinar la identidad de una persona…

Ahora bien, los datos pueden obtenerse y utilizarse de forma legítima, acorde a lo previsto por la legislación, o con fines ilegítimos, en cuyo caso deben preverse sanciones administrativas y consecuencias penales, ya que no debe olvidarse que lo que subyace tras los datos es una persona física titular de una serie de derechos que deben ser protegidos y reparados en caso de vulneración.

Habrá que ver, pues, estas situaciones de obtención y tratamiento legítimo, los medios de protección de sus datos con que cuentan los particulares, y qué ocurre en caso de inobservancia de la normativa establecida a estos efectos.

3.4. Modo de obtención de los datos: necesidad de consentimiento.

Para obtener los datos de una persona física de manera legítima es preciso que ella los aporte y que, además, otorgue permiso para su tratamiento, cumpliéndose en ambos casos una serie de requisitos. No obstante, habrá supuestos tasados en que el consentimiento no sea necesario, y supuestos en que deba reunir algunas características adicionales que lo doten de validez.

3.4.1. Art. 6 LOPD.

La exigencia de consentimiento de la persona cuyos datos se van a recabar aparece reflejada en el art. 6.1 LOPD, que establece que:

> *1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.*

Este artículo consta de un total de 4 apartados que se relacionan también con la necesidad del consentimiento, pero en un sentido negativo, ya que tratan de la excepción a esta necesidad, la revocación del consentimiento y la oposición del interesado al tratamiento de sus datos. Por lo tanto, el resto del artículo 6 se analizará más adelante.

3.4.2. Consentimiento inequívoco y consentimiento tácito.

La exigencia de consentimiento del art. 6.1 LOPD lo es, *ex lege*, de un asentimiento inequívoco del afectado. No obstante, esto no supone que el consentimiento deba, imperativamente, prestarse de manera expresa o por escrito.

El consentimiento, con carácter general (pues ya se ha visto cómo las informaciones relativas a la ideología, las creencias y la religión, así como la afiliación sindical exigen

consentimiento escrito), no se somete a requisitos formales. Con vistas a poder considerarse tal, solo deberá ajustarse a la definición de consentimiento que aporta el art. 3 h) LOPD:

> *Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.*

Del tenor literal del art. 3 h) LOPD se desprende la misma idea, dado que no exige en ningún momento que se manifieste de manera escrita o expresa el beneplácito del afectado a la hora de recoger y tratar sus datos.

En cuanto al consentimiento tácito, una vez determinado como posible, hay que precisar dos aspectos: su concepto y cómo interpretar el silencio del interesado.

El consentimiento se entenderá otorgado de manera tácita cuando la persona "*no manifiesta de modo directo su voluntad sino que realiza una determinada conducta que por presuponer necesariamente tal voluntad, es valorada como declaración por el ordenamiento jurídico"*.[12]

El caso del silencio del particular es un supuesto cuya validez como consentimiento tácito ha estudiado el Tribunal Supremo y cuya conclusión ha reflejado en diversas sentencias ya desde mediados del pasado siglo. De este modo, el Tribunal Supremo "*considera el silencio como declaración de voluntad cuando, dada una determinada relación entre dos personas, el modo usual de proceder implica el deber de hablar, ya que el que si puede hablar no lo hace, se ha de respetar que consiente en aras a la buena fe"*.[13]

Como muestra de esta histórica jurisprudencia, puede citarse el siguiente fragmento de la sentencia del Tribunal Supremo 169/1957, de 24 de enero[14] - a la que Fernández López hace referencia –, correspondiente a su primer "considerando" y que viene a declarar posible el consentimiento tácito y, a su vez, la interpretación casuística que debe hacerse del silencio:

"CONSIDERANDO que el consentimiento […] puede ser manifestado de modo expreso por una o ambas partes […], o bien tácitamente cuando de su comportamiento o de sus declaraciones resulta implícita

[12] FERNÁNDEZ LÓPEZ, Juan Manuel. "*Comentario de Juan Manuel Fernández López al artículo 6: El consentimiento del afectado"* en *Comentario a la Ley Orgánica*… cit. Pág. 456.
[13] FERNÁNDEZ LÓPEZ, Juan Manuel. "*Comentario de Juan Manuel Fernández López al artículo 6: El consentimiento del afectado"* en *Comentario a la Ley Orgánica*… cit. Pág. 456.

[14] Sentencia del Tribunal Supremo, Sala I, de lo Civil. 24-01-1957. ROJ: STS 169/1957. Primer Considerando. Ponente: Francisco Bonet Ramón.

su aquiescencia, no debiendo confundirse con el consentimiento tácito el simple silencio, pues […], este acuerdo no puede resultar de un comportamiento meramente negativo de una de las partes, […], sino que debe manifestarse con palabras o con hechos; mas cuando el silencio pueda juntarse a hechos positivos precedentes a una actividad anterior de la parte silenciosa o a particulares situaciones subjetivas u objetivas, también este silencio cualificado puede concurrir como elemento útil para apreciar la voluntad de la parte misma".

3.4.3. Requisitos para la obtención y validez del consentimiento.

Hay que volver al mencionado art. 3 h) LOPD para conocer qué requisitos debe reunir el consentimiento para ser válidamente otorgado y, en consecuencia, poder ser recogido y tratado.

Dice este artículo que el consentimiento es "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"*, de forma que podrá considerarse válido el consentimiento que reúna esta serie de características.

Así pues, el consentimiento ha de proceder de una exteriorización, a través de cualquier medio, de la facultad de dirigir y ordenar la propia conducta. Esta exteriorización debe producirse en ausencia de cualquier clase de coacción y deberá referirse únicamente a uno o varios tratamientos concretos, junto al fin para el que se recogen y el resto de circunstancias que puedan darse en ese concreto tratamiento – lo cual, refleja la imposibilidad de otorgar un consentimiento genérico –.

Además, aunque parezca una obviedad, el tratamiento que se consiente debe ser de los datos de carácter personal propios de quien consiente y previa información sobre el motivo y finalidad de recogida y almacenamiento de esos datos, entre otros elementos (el derecho y deber de información se tratará más adelante).

3.4.4. Prueba del consentimiento.

Probar que se ha obtenido un consentimiento válido conllevará distinto grado de dificultad, en función del tipo de consentimiento prestado, siendo más difícil de probar el consentimiento tácito.

Para probar el consentimiento expreso bastará con recurrir a cualquier manifestación realizada por el interesado, a los medios de prueba tradicionales o a los actos propios del afectado. Tanto más fácil será la prueba cuando el consentimiento se manifestase por escrito.

Sin embargo, la prueba del consentimiento tácito entraña una especial complejidad, caracterizada por la inversión de la carga de la prueba.

Frente al principio que implica que quien afirma debe probar, en materia de protección de datos, acorde al art. 12.3 RLOPD[15], deberá demostrar el consentimiento quien sea responsable del tratamiento de los datos (disponiendo para ello de cualquier medio lícito, incluso de la prueba indiciaria). Así, si el interesado negase haber otorgado su consentimiento, deberá probar lo contrario el responsable del tratamiento y, si no lo negase, deberá acreditar que se obtuvo informando previamente al afectado de todo cuanto exige la legislación.

3.4.5. Excepciones a la necesidad de obtener consentimiento.

Pese a la necesidad de obtener datos de carácter personal previo consentimiento del interesado que propugna el art. 6.1 LOPD, el segundo apartado de este artículo contiene una serie de supuestos excepcionales en los que este consentimiento no será imperativamente exigido a la hora de recopilar y almacenar los datos de carácter personal:

> *2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*

Estas figuras, para estar exentas de la necesidad de consentimiento, deben cumplir una serie de requisitos, que variarán según ante aquella de que se trate:

a) Para que los datos recogidos por las Administraciones Públicas no se condicionen al consentimiento del interesado, deberá estarse ante una recogida con vista al ejercicio de las funciones propias de dicha Administración, siendo estas las que vengan determinadas en una

[15] Art. 12.3 RLOPD: "*Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho*".

norma comunitaria o una norma con rango de ley (art. 10.3 RLOPD) y, al mismo tiempo, dicha Administración deberá actuar dentro de su ámbito competencial, atendiéndose en este aspecto a la normativa existente sobre competencias y atribución competencial de las Administraciones.

b) Cuando los datos de las partes sean necesarios para mantener o cumplir contratos, precontratos, relaciones administrativas o laborales, se entenderá que el consentimiento se prestó ya en el momento de perfeccionamiento de dicho contrato. De no ser así, si fuese constantemente necesario que las partes prestaran consentimiento para todos o la mayoría de aspectos de sus contratos o relaciones, el cumplimiento sería retrasado de manera prácticamente indefinida o bien, imposible.

c) También alude el precepto a la protección de intereses vitales del interesado en los términos del art. 7.6 LOPD. El referido artículo establece:

> *No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.*
>
> *También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.*

Los apartados 2 y 3 que se citan en el art. 7.6 LOPD no se refieren sino a los datos especialmente protegidos (que, a su vez, reflejaban derechos fundamentales de carácter íntimo) y lo que realmente debe interpretarse respecto de esta excepción, siguiendo a Juan Manuel Fernández López, es: siempre que el tratamiento de los datos responda a un interés vital del afectado, habrá de realizarse una ponderación entre el derecho a la protección de los datos personales y el derecho fundamental (interés vital) afectado, preponderando siempre

ese interés vital y no siendo necesario el consentimiento del interesado, a fin de lograr una más rápida y efectiva protección de ese derecho fundamental en riesgo.[16]

d) En último lugar, se mencionan los datos que aparecen en fuentes accesibles al público. Esto quiere decir que no será necesario consentimiento del afectado siempre y cuando sus datos figuren en un fichero cuya consulta pueda realizarse por cualquier persona – esto es, una fuente accesible al público – y exista un interés legítimo en el responsable del tratamiento que solo pueda verse satisfecho mediante la obtención de estos datos.

Nuevamente, la mención de un interés legítimo hará necesaria una ponderación de los derechos en presencia, para valorar cuál de ellos debe ceder en favor del otro.

El otro requisito que exige el art. 6.2 LOPD en este ámbito es que los datos se recojan en fuentes accesibles al público, siendo la propia ley, en el art. 3 j) la que establece un *numerus clausus* de fuentes de este tipo:

> *Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.*

Ilustrativa de este supuesto es la mencionada polémica suscitada por la Directiva 95/46/CE y su art. 7 f), en relación con la excepción de consentimiento del interesado en caso de interés legítimo y datos en fuentes accesibles al público del art. 6.2 LOPD y debe recordarse que el TJUE (a raíz de una cuestión prejudicial del Tribunal Supremo español) sentenció el 24 de noviembre de 2011 que la exigencia de la ley nacional de que el dato figurase en una fuente accesible al público era un añadido no determinado en la Directiva y, por lo tanto, dicho inciso, en atención a la eficacia directa de la (hoy derogada) Directiva, carecería de aplicabilidad.

Lo reflejan especialmente bien Guasch Portas y Soler Fuensanta. cuando realzan que, *"en base a la Sentencia del Tribunal Supremo de ocho de febrero de 2012, sólo deben darse dos requisitos*

[16] FERNÁNDEZ LÓPEZ, Juan Manuel. "*Comentario de Juan Manuel Fernández López al artículo 6: Supuestos excepcionados del consentimiento"* en *Comentario a la Ley Orgánica*… cit. Pág. 468.

para que un tratamiento de datos sea lícito: que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y que no prevalezcan los derechos y libertades fundamentales del interesado (esencialmente los derechos de los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea: derecho a la intimidad y a la protección de datos personales)". [17]

Avanzando hasta el día de hoy, debe entenderse que lo determinado por el TJUE sobre de la derogada Directiva y las fuentes accesibles al público del art. 6.2 LOPD se aplicará en los mismos términos también al Reglamento 2016/679.

Finalmente, debe recordarse que el art. 6.2 LOPD, *in fine*, establece un requisito que debe cumplir cada una de estas figuras*:* estas excepciones serán aplicables única y exclusivamente cuando no se produzcan vulneraciones a derechos y libertades de las personas físicas cuyos datos se tratan.

3.4.6. Consentimiento relativo a datos sobre menores de edad.

Los menores son personas especialmente vulnerables que necesitan de una protección reforzada de sus derechos e intereses.

Los datos personales afectan a los derechos de las personas y, partiendo de la idea anterior, habrá que determinar si son los menores los titulares de sus datos de carácter personal y si pueden o no prestar consentimiento para que sus datos se recojan y almacenen en ficheros.

La primera idea planteada es la titularidad. Para abordar la titularidad de los datos de carácter personal y poder relacionarla con el consentimiento, debe atenderse a la capacidad del menor y no a los propios datos en sí mismos. Esto quiere decir que a la hora de calificar como titular de los datos al menor se atenderá al momento del consentimiento, ya que indudablemente son titulares de sus propios datos de carácter personal desde el momento en que nacen, como ya se ha expuesto.

Respecto de la capacidad del menor de edad, es interesante la reflexión que realiza María Belén Andreu Martínez, por razón la falta de criterios concretos que permitan fijar de manera exacta el grado de capacidad y madurez que ostente el menor de edad:

[17] GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "El interés legítimo… cit. Pág. 437.

"*[…] entendemos que se pueden retener como edades clave los 12 años […] y los 16 años (a partir de la cual se puede ampliar enormemente el ámbito de actuación del menor), quedando la franja de los 13 – 15 años como aquella en que las condiciones de madurez juegan un papel determinante a la hora de fijar su capacidad […] encontrándose mucho más limitado en los aspectos patrimoniales […]".* [18]

Plasmando la imprecisión referente a una exacta determinación de la capacidad del menor, alude a los aspectos patrimoniales y la limitación de la capacidad para ellos, porque nuestro Derecho, por regla general, permite poco margen de actuación a los menores de edad en materia patrimonial si no cuenta con la intervención o el consentimiento de sus representantes legales y, dado que ciertos datos personales del menor, como las imágenes, pueden ser objeto de negocios patrimoniales (véase los niños que actúan como modelos en campañas de marcas textiles), en ocasiones el consentimiento respecto del tratamiento de los datos de los menores deberán aportarlo sus padres o tutores.

Las situaciones en que deberán aportar el consentimiento los representantes del menor quedan reflejadas en el art. 13.1 RLOPD. Así, es a través de la unión de este con la anterior reflexión mediante lo que se puede responder a la segunda de las cuestiones planteadas: si pueden o no los menores prestar consentimiento para el tratamiento de sus datos. Dice el art. 13.1 RLOPD:

> *"Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores."*

Se deduce de ello que el consentimiento de los menores de edad podrá ser otorgado exclusivamente por ellos mismos, siempre y cuando sean mayores de 14 años y las leyes no prevean asistencia de sus representantes legales. En este sentido se ha manifestado también la AEPD, matizando que los menores deberán ser informados de forma sencilla, clara y con un lenguaje destinado a su fácil y entera comprensión[19].

---

[18] ANDREU MARTÍNEZ, María Belén. "*Capítulo III: El consentimiento del menor para el tratamiento de sus datos personales"* en *La Protección de Datos Personales de los Menores de Edad.* Aranzadi, 2013. Pág. 73.

[19] Gabinete Jurídico de la Agencia Española de Protección de Datos. *Informe 0046/2010.* Págs. 2 y 3. Disponible en:
<https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2010-0046_Tratamiento-de-datos-de-menores.-Consentimiento-y-deber-de-informaci-oo-n.pdf.>
[Consulta: 10 de febrero de 2018].

Ahora bien, dado que el menor es una persona especialmente protegida, debe concluirse este tema con una idea básica: a la hora de aportar el consentimiento para el tratamiento de datos de carácter personal de un menor, primará en cualquier caso su interés, quienquiera que otorgue el consentimiento y, en definitiva, el representante no podrá obviar consultar al niño previamente (si este tiene capacidad suficiente para entender y aprobar o no la decisión). Consecuentemente, cuando el menor alcance la mayoría de edad, será libre de revocarlo[20].

Hay que hacer también mención al consentimiento de los menores en su uso de las redes sociales. Estas son el instrumento básico de socialización en la actualidad también para las personas menores de edad, y permiten la conexión en tiempo real entre menores, pero también de los menores con personas adultas e, incluso, con personas jurídicas.

Por este motivo, al tratar de su consentimiento en relación a los datos que pudiesen llegar a introducir en sus redes sociales a la hora de creación de cuentas o perfiles (y como paso previo a una posible posterior publicación por el propio menor de sus datos en la red), habrá de tenerse en cuenta algo más que el interés superior del menor y, dependiendo de su edad, su consentimiento o el de sus representantes legales: deberán adoptarse tambien ciertas medidas por parte de los prestadores del servicio tecnológico, como llevar a cabo verificaciones de la edad, adaptar la información al entendimiento y capacidades del menor, no solicitar datos sensibles, o evitar publicidad inadecuada para su edad.

Estos aspectos sobre la especial protección a los datos de los menores son también un aspecto esencial del nuevo Reglamento Europeo, tal y como manifiesta a lo largo de sus Considerandos iniciales.[21]

3.5. ¿Dónde se almacenan los datos? Los ficheros.

3.5.1. Concepto.

Los datos recogidos van a parar a los ficheros, definidos en el art. 3 b) LOPD como:

---

[20] PÉREZ LUÑO, Antonio-Enrique. *"Comentario de Antonio-Enrique Pérez Luño al artículo 6: El consentimiento de los menores y sus peculiaridades"* en *Comentario a la Ley Orgánica*… cit. Pág. 483.

[21] ANDREU MARTÍNEZ, María Belén. "*Capítulo IV: El tratamiento de los datos personales de menores en determinados ámbitos y la aplicación del principio del consentimiento"* en *La Protección de Datos*… cit. Págs. 101 y 107.

> *"Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".*

Puede deducirse de esta definición que el fichero es susceptible de constituirse en cualquier soporte, eliminándose así cualquier clase de ambigüedad en cuanto a la interpretación del término (confusión causada por la tradicional imagen asociada al término "fichero").

Asimismo, se destaca que el conjunto de datos debe estar organizado. Lo que esto quiere expresar es que debe poder accederse a los datos que contiene el fichero siguiendo un criterio lógico, que normalmente será numérico o alfabético.

Resume de forma sucinta y clara las implicaciones del concepto legal Concepción Conde Ortiz, quien considera que "*solo podrá considerarse fichero aquel conjunto de datos susceptibles de utilización mediante sistemas automáticos o manuales que permitan diferenciar los datos y acceder a ellos de alguna manera útil*". [22] Esta afirmación ha de suscribirse por su sencilla síntesis de las características que la ley, no tan visiblemente, expone que debe reunir un fichero de datos para considerarse tal.

Únicamente podría aportarse un matiz a este concepto, matiz que tampoco incorpora la observación de Conde Ortiz: la unidad del fichero. Que un fichero sea unitario implica, por una parte, que su contenido se compone de una serie de datos uniforme, es decir, relacionados entre sí en referencia a una materia común (en este caso, a la persona titular de los mismos); por otro lado, que el fichero no podrá dividirse sin que su información básica pierda calidad de modo tal, que dicha calidad quede destruida.[23]

Son todas estas características las que permiten identificar un conjunto de datos como fichero, pero existen otros elementos asociados al fichero que permiten distinguirlos en varias clases, como pueden ser su titular, el carácter de los datos que contiene, o su accesibilidad.

Especialmente relevante es la distinción de los ficheros en función de su titular o responsable, recogida expresamente en el art. 5 RLOPD, aunque no en la ley que desarrolla.

---

[22] CONDE ORTIZ, Concepción. *La protección de datos personales*: *un derecho autónomo con base en los conceptos de intimidad y privacidad.* Dykinson, 2005. Pág. 76.

[23] DAVARA RODRÍGUEZ, Miguel Ángel. "*Comentario de Miguel Ángel Davara Rodríguez al artículo 3: El fichero de datos y el fichero informático"* en *Comentario a la Ley Orgánica*… cit. Págs. 216 y 217.

3.5.2. Ficheros privados.

Los ficheros privados aparecen definidos en el art. 5 l) RLOPD como "*ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica*".

De esta definición reglamentaria se puede obtener una idea básica: los ficheros de titularidad privada son aquellos cuyo responsable es una persona o entidad de derecho privado, o bien, una corporación de derecho público que no vincula ese fichero al ejercicio de sus potestades públicas.

Ahora bien, antes de continuar con los ficheros públicos, aparece en el concepto de "fichero privado" un término que es necesario aclarar: "responsable". Es necesario aclarar este concepto debido a que, en relación al fichero, se encuentran dos figuras: el responsable del fichero y el responsable del tratamiento.

La diferenciación entre ambos la estableció el Tribunal Supremo, en una sentencia dictada por la Sala Tercera, de lo Contencioso - Administrativo, el 5 de junio de 2004:

"Así, el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir, quien tiene capacidad de decisión sobre la totalidad de los datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica. Se trataría de todos aquellos supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento". [24]

El responsable del fichero y el responsable del tratamiento son dos aspectos de esta materia que, aun diferenciados, gozan de gran trascendencia respecto del concepto de fichero. Muestra de esta relevancia es la reflexión de Davara Rodríguez: "*el fichero […] puede*

[24] Sentencia del Tribunal Supremo, Sala III, de lo Contencioso – Administrativo. 05-06-2004. Nº Resolución: 3896/2004. Nº Recurso: 39/2004. Fundamento de Derecho Tercero. Ponente: Francisco González Navarro. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_supremo/common/pdfs/Sentencia-del-Tribunal-Supremo-05-06-2004.pdf> [Consulta: 15 de febrero de 2018]

delimitar obligaciones y responsabilidades tanto del responsable del fichero o del tratamiento de sus datos […]".[25]

Hecha esta clara diferenciación, podrán comprenderse mejor los conceptos reglamentarios, referidos a los responsables de los ficheros.

3.5.3. Ficheros públicos.

Es también el art. 5 RLOPD el que proporciona la definición de fichero público, en este caso, en el apartado m). Así, debe entenderse por fichero público todo fichero que tenga como responsable a "*los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público*".[26]

En definitiva, los ficheros de titularidad pública son aquellos cuyo responsable es ente de derecho público, o bien, una corporación de derecho público que vincula ese fichero al ejercicio de sus potestades públicas.

3.5.4. Finalidad de los ficheros.

Los datos personales, según el art. 4.1 LOPD, *"sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".*

Del artículo se deduce que la finalidad para la que se recogen y utilizan los datos de carácter personal es un aspecto esencial, ya que es la relación entre la finalidad del fichero y la naturaleza de los datos recabados la que justifica la existencia del fichero y la que, en gran medida, determina la legitimidad del mismo.

---

[25] DAVARA RODRÍGUEZ, Miguel Ángel. "*Comentario de Miguel Ángel Davara Rodríguez al artículo 3: A modo de conclusión"* en *Comentario a la Ley Orgánica*… cit. Pág. 225.

[26] En este precepto, hay que atender al concepto de Administración Pública que aporta el art. 2 de las leyes 39/2015 y 40/2015: *Tienen la consideración de Administraciones Públicas la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2 anterior – a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas –.*

Esto es así hasta tal punto que, en ocasiones, será la propia legislación la que determine la finalidad del fichero.

Hay cuatro aspectos destacables en relación a la finalidad: el tratamiento, la determinación, la explicitud y la legitimidad.[27]

En primer lugar, el tratamiento. Lo define el art. 3 c) LOPD:

> *"Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

El tratamiento de datos implica la recogida, el mantenimiento y el "tratamiento" – en cuanto trabajo o procesamiento lícito y permitido – de los datos de carácter personal que el interesado ha consentido proporcionar (permitiendo también, con el mismo consentimiento, este tratamiento).

En segundo lugar, la determinación. Esta supone que no se admitirán los ficheros con una finalidad vaga o general, es decir, cuya finalidad no sea concretada y delimitada.

La explicitud, por su parte, implica que el interesado debe conocer la finalidad del fichero, porque esto será lo que le permita decidir si presta o no su consentimiento.

La legitimidad a que el artículo hace referencia no es otra cosa que el ajuste a la Constitución y la Ley; es decir, poco importa el consentimiento del interesado si la finalidad del fichero no se acomoda a la legalidad.

Por lo tanto, toda vez que se crea un fichero con un objetivo concreto, legítimo y determinado, serán ajustados a la ley tanto su existencia, como el tratamiento de los datos de carácter personal que contiene.

En definitiva, la finalidad influye en todo el proceso de tratamiento de los datos de carácter personal y debe respetarse durante toda la vida del fichero, desde el momento de la

[27] TRONCOSO REIGADA, Antonio. "*Comentario de Antonio Troncoso Reigada al artículo 4: El principio de calidad a partir de dos pilares: la finalidad del fichero y los datos registrados"* en *Comentario a la Ley Orgánica*… cit. Pág. 342.

recogida de los datos por consentimiento del afectado, durante la utilización de dichos datos y, en su caso, en la cancelación. [28]

4. LA NECESIDAD DE PROTEGER LOS DATOS. PRINCIPIOS RECTORES DE LA PROTECCIÓN.

Es innegable, a la vista de todo lo anterior, que los datos de carácter personal tienen una gran relevancia, que se acrecienta en la actualidad, era de la "*big data"*, con la proliferación de redes sociales y direcciones web que precisan de ciertos datos de carácter personal de sus usuarios. Por este motivo, aumenta la exposición de los datos personales y es mucho más sencillo acceder a los datos de cualquier persona sin un gran esfuerzo.

Siguiendo a Elena Gil González, "*big data es un término que alude al enorme crecimiento en el acceso y uso de información automatizada. Se refiere a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos. No es una tecnología en sí misma, sino más bien un planteamiento de trabajo para la obtención de valor y de beneficios como consecuencia del tratamiento de los grandes volúmenes de datos que se están generando día a día*" [29], y los algoritmos que menciona, lo que permiten es convertir la ingente cantidad de datos en información concreta sobre los titulares de esos datos, que no tienen por qué ser, en un principio, de carácter personal (véase, la localización y las tecnologías como los GPS; o los "*likes"* en redes sociales)[30].

Este auge tecnológico basado en datos, junto con las relaciones humanas y las prestaciones de servicios necesarios suponen poner en jaque los derechos asociados a los datos de carácter personal, principalmente los derechos al honor, la intimidad, la propia imagen y la dignidad. Se afirma, por ello, que "*la preocupación por la recolección de datos personales y sobre la pérdida de su control aparece al mismo tiempo en que el desarrollo tecnológico permitió la automatización del tratamiento de los datos personales".*[31]

---

[28] TRONCOSO REIGADA, Antonio. "*Comentario de Antonio Troncoso Reigada al artículo 4: El principio de calidad a partir de dos pilares: la finalidad del fichero y los datos registrados"* en *Comentario a la Ley Orgánica*… cit. Pág. 344.

[29] GIL GONZÁLEZ, Elena. *Big data, privacidad y protección de datos.* Agencia Estatal Boletín Oficial del Estado. Madrid, 2016. Pág. 17.

[30] GIL GONZÁLEZ, Elena. *Big data, privacidad y protección de datos*… cit. Pág. 18.

[31] GARRIGA DOMÍNGUEZ, Ana. *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua.* Dykinson, 2016. Pág. 90.

Así, se concibió – no exento de polémica – lo que hoy se conoce como derecho a la protección de datos; un derecho fundamental (en tanto se incardina en el art. 18 CE) que daría respuesta a la inquietud respecto de las lesiones que el tratamiento y cesión de datos pudiesen ocasionar a los derechos de las personas.

La controversia surgió no tanto por la necesidad de proteger los datos, sino por el modo en que parece recogerse este derecho en la Constitución dentro del catálogo de derechos fundamentales.

El artículo 18.4 de la Constitución se incardina dentro del precepto general dedicado a la protección de la intimidad y la discusión de la doctrina se centró en determinar si se recoge un derecho derivado de la intimidad y parte del derecho a ella, o si por el contrario, lo que refleja de manera implícita es un derecho autónomo y complementario del derecho a la intimidad.

La intimidad consiste en "*el poder concedido a la persona sobre el conjunto de actividades que forman su círculo íntimo, poder que le permite excluir a los extraños de entrometerse en él y de darle una publicidad que no desee el interesado",* [32] según Albaladejo y, según la concepción del Tribunal Supremo, en "*el derecho a mantener intacta, desconocida, incontaminada e inviolada la zona íntima, familiar o recoleta del hombre"* [33].

Antes de continuar, cabe destacar que, para abordar esta cuestión, hay que tener en cuenta que se comenzó a debatir en época preconstitucional, y que desde entonces, ha tenido lugar una evolución tanto normativa como jurisprudencial.

Ambas concepciones ponen de manifiesto la trascendencia y especial cuidado que, ya en los años 70, se trataba de poner en este derecho y su defensa, por lo que era indiscutible que ciertos datos referidos al ámbito personal (los datos de carácter personal) debían protegerse. No obstante, "*es cuando surge la informática y la posibilidad del tratamiento automatizado de los datos y su transmisión cuando aparece una nueva relación entre datos y personas y el sujeto necesita ser protegido más allá de las normas referentes a la intimidad". [34]*

---

[32] ALBALADEJO GARCÍA, Manuel. *Derecho Civil. Introducción y Parte General. Vol. II.* Bosh, 1977. Pág. 59.

[33] Sentencia del Tribunal Supremo, Sala II, de lo Penal. 08-03-1974. ROJ: STS 1813/1974. Fundamento de Derecho Tercero. Ponente: Luis Vivas Marzal.

[34] CONDE ORTIZ, Concepción. *La protección de datos personales*: *un derecho*… cit. Pág. 25.

De esta última afirmación, en relación con la citada problemática sobre la naturaleza del derecho a la protección de datos, puede deducirse ya que la balanza se inclina hacia la teoría del nacimiento de un derecho autónomo.

Sin embargo, surge otra cuestión. Al no aparecer reconocido de manera explícita en el art. 18.4, aparece la duda de si es un derecho constitucional o, si bien, tiene un origen diferente – concretamente, jurisprudencial –. Ambas teorías tienen tanto partidarios como detractores.

En este punto, es pertinente seguir la línea de Conde Ortiz, quien asume la posición de un derecho autónomo de origen jurisprudencial

Sitúa su punto de partida en una sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Federal Alemán, de la que deriva la garantía del afectado para decidir sobre la difusión y uso de sus datos de carácter personal. [35]

La influencia de esta sentencia germana y de las ulteriores dictadas en el mismo sentido se dejó notar en España una década más tarde, con una sentencia del Tribunal Constitucional de 20 de julio de 1993 que, no obstante, no clarificaba en demasía la existencia del derecho a la protección de datos. Hubo que esperar, pues, hasta el año 1998, cuando el Tribunal Constitucional, en una sentencia dictada el 13 de enero de ese año, manifestó que "*el art. 18.4 CE no solo entraña un específico instrumento de protección de los derechos de los ciudadanos […] sino que además consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona […]*".[36]

Reseñable de esta declaración es la reciente existencia del derecho a la protección de datos como derecho autónomo, ya que – pese a esta sentencia – no será hasta el año 2000, con las sentencias del Tribunal Constitucional 290/2000 y 292/2000, cuando se reconozca definitivamente la existencia del derecho a la protección de datos de forma autónoma como derecho distinto del derecho a la intimidad.

Por lo tanto, es a partir de ese momento en el que realmente se comienza a apreciar la existencia de este nuevo derecho, además fundamental, cuando surge la necesidad de otorgarle una serie de medidas de protección y de garantías para asegurar su respeto y protección. Estas medidas y garantías se configuran como una serie de derechos de los

[35] CONDE ORTIZ, Concepción. *La protección de datos personales*: *un derecho*… cit. Pág. 39.

[36]CONDE ORTIZ, Concepción. *La protección de datos personales*: *un derecho*… cit. Pág. 42.

interesados y de obligaciones para los responsables de ficheros y su tratamiento, cuyo punto común de referencia se encuentra en una serie de principios rectores: calidad de los datos, información, tratamiento, transparencia, principios de las transmisiones y cesiones de datos, deber de secreto y ponderación de intereses.

Mención especial merece, en este punto y antes de pasar a ver esos principios rectores, la Carta de Derechos Fundamentales de la Unión Europea.

Esta, reconoce también este derecho a la protección de datos personales como un derecho fundamental en el ámbito comunitario, en el art. 8 (ya mencionado en el apartado relativo al marco normativo).

Las disposiciones de la Carta se dirigen a las instituciones y órganos de la Unión Europea y a los Estados miembros, pero a estos únicamente cuando apliquen el Derecho de la Unión. Este ámbito de aplicación aparece recogido en el art. 51 de la Carta y es un precepto que permite determinar también el carácter de fundamental respecto del derecho a la protección de datos de carácter personal y, en consecuencia, la necesidad de aportar una especial defensa a estos datos.

4.1. Calidad de los datos.

La calidad de los datos aparece recogida en el art. 4 LOPD:

> *1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*
> *2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.*
> *3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.*
> *4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.*

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Constituye el artículo 4 LOPD un conjunto heterogéneo de reglas que se agrupa bajo esta denominación de "*calidad de los datos*", tratándose con todas ellas una serie de exigencias que debe cumplir el fichero en dos vertientes: en la justificación de la existencia del fichero – es decir, la finalidad, ya vista – y en su proceso de vida.

Es por ello necesario conocer, de manera sucinta, la incidencia del principio de calidad en cada momento de la vida del fichero.

4.1.1 En la declaración.

La declaración es el paso previo a la recogida de datos personales en el fichero, y supone cumplir los requisitos de explicitud, legitimidad y determinación, es decir, analizar la finalidad del tratamiento y de los datos que serán su objeto, pero de manera previa a la recogida de los mismos.

El principio de calidad, en esta fase, implica que la finalidad para la que los datos se van a recoger en el fichero deberá ser legítima, estar suficientemente determinada y explícita, y la tipología de los datos será adecuada a la finalidad del fichero y en ningún caso excesiva.

De vulnerarse el principio de calidad en esta fase, las consecuencias variarán en función del fichero que se pretendiese crear. Si el fichero fuere público, puede implicar la nulidad; si

fuere privado, la negativa del Registro Central de Protección de Datos a su inscripción y, consiguientemente, su no creación.

4.1.2. En la recogida de los datos.

La recogida de datos es el proceso de obtención de los datos de carácter personal que se incluirán en el fichero, de forma que deja de hablarse de cada uno de esos datos recogidos como de un "dato personal", para pasar a hacer referencia a todos en conjunto bajo el nombre de fichero. No obstante, en este momento de la vida del fichero, también se incluye el almacenamiento de los datos, no solo su obtención.

El principio de calidad implica también, en la obtención de los datos, el cumplimiento de los requisitos de legitimidad, explicitud y determinación, pero se añaden además otros dos requisitos: lealtad y licitud, que se resumen en dar cumplimiento al principio de información.

Por otro lado, en la fase de almacenamiento de los datos, se concreta este principio de calidad en la facilitación de derechos al interesado, especialmente el derecho de acceso a sus propios datos de carácter personal – sin olvidar nunca la legitimidad, la explicitud y la determinación –.

La vulneración del principio de calidad en esta fase implica la comisión de infracciones de la LOPD, de leves a muy graves – como la obstaculización de manera sistemática del ejercicio de derechos de acceso, rectificación, oposición y cancelación, por ejemplo –. [37]

4.1.3. En el uso del fichero.

El uso del fichero es la utilización que se hace de los datos en él insertos, desde su recogida hasta su cancelación, debiéndose respetar igualmente el principio de calidad de los datos porque su vulneración puede dar lugar también a infracciones de la LOPD.

Se concreta en tres exigencias: tratar los datos solo para la finalidad prevista, la determinación de quiénes pueden (exclusivamente) acceder al fichero y el mantenimiento de los datos veraces y exactos en el momento de su recogida y durante toda la vida del fichero.

[37] TRONCOSO REIGADA, Antonio. "*Comentario de Antonio Troncoso Reigada al artículo 4: E principio de calidad durante el proceso de vida del fichero"* en *Comentario a la Ley Orgánica*… cit. Pág. 365.

4.2. El deber de información a los interesados. Correlativo derecho de estos.

4.2.1. El deber de información.

Toda persona tiene derecho a conocer la existencia y finalidad de cualquier fichero de datos, a su responsable y qué datos concretos de los que es titular se encuentran registrados en el mismo. Esto es lo que hace que el tratamiento sea leal y lícito, como ya se ha mencionado.

Por lo tanto, desde el momento de creación de un fichero, existe un deber de información de los responsables para con los interesados; un deber recogido en el art. 5 LOPD. La pauta fundamental se encuentra en el apartado 1 de este artículo, concretamente en su primer párrafo:

> *Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
> *a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
> *b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
> *c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
> *d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
> *e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

De este deber, se pueden desglosar tres aspectos: su contenido, algunas exenciones en su cumplimiento, y el modo de practicarlo para considerarlo cumplido.

4.2.1.1. Contenido.

El contenido del deber de información se incardina en la correspondiente cláusula informativa, que habrá de proporcionarse al interesado en el momento de solicitarle sus datos y su consentimiento para la inclusión de los mismos en el fichero. Los aspectos sobre los que debe informarse, así como el modo en que debe hacerse, vienen contenidos en el propio precepto.

No obstante, solo tendrán carácter de información obligatoria en todo caso: la existencia del fichero o del tratamiento de los datos; la identidad y dirección de los responsables y la finalidad y los destinatarios de los datos.[38]

4.2.1.2. Excepciones al deber de información.

Hay ciertas excepciones en las que este deber de información no es necesario que se practique, referidas a la obtención de los datos del afectado mediante persona distinta a él.

Así, la regla general – contenida en el art. 5.4 LOPD – es la información al interesado de forma expresa, precisa e inequívoca de los aspectos obligatorios, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos cuando no se hubiesen recabado de este interesado y siempre que no se le hubiese informado de manera previa.

A esto, la LOPD establece una serie de excepciones en su art. 5.5 que es necesario conocer: cuando el tratamiento de los datos tenga fines estadísticos, históricos o científicos, ya que se considera que esta finalidad no es incompatible con aquella para la que se prestó consentimiento; o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, estándose en cada caso al criterio de la AEPD. Lo que se requiere en ambos casos es las situaciones se amparen en una norma con rango de ley. [39]

4.2.1.3. Práctica.

Este deber de información debe cumplirse de manera que pueda luego ser probado por los responsables del fichero, tal y como establece el art. 12.3 RLOPD, por lo que la mera información verbal al interesado no es un medio adecuado ni válido para cumplir el deber impuesto por la LOPD.

Por ello, los métodos más usuales para informar a los afectados de forma que pueda quedar constancia de que dicha información les fue proporcionada, son los siguientes: cláusulas informativas incluidas en los impresos o cuestionarios de recogida de datos,

---

[38] CANALES GIL, Álvaro. "*Comentario de Álvaro Canales Gil al artículo 5: Contenido del deber de información"* en *Comentario a la Ley Orgánica*… cit. Pág. 410.
[39] CANALES GIL, Álvaro. "*Comentario de Álvaro Canales Gil al artículo 5: Excepciones a la práctica del deber de información*" en *Comentario a la Ley Orgánica*… cit. Pág. 422.

grabaciones en caso de contactos telefónicos, cláusulas informativas online o carteles anunciadores. [40]

Todos estos métodos deberán ser claros, inteligibles y proporcionar toda la información necesaria sobre el fichero o tratamiento para que pueda considerarse cumplido el deber de los responsables.

4.2.2. Responsabilidad por incumplimiento del deber de información.

La LOPD no especifica qué consecuencias pueden derivarse para los responsables del fichero y su tratamiento por el incumplimiento del deber de información.

Sin embargo, no se puede sino coincidir con Díaz Revorio cuando afirma que las pautas para conocer estas consecuencias pueden determinarse a partir de la siguiente idea: el derecho de información constituye un elemento integrado dentro de otro derecho de magnitud superior, el derecho a la protección de datos, que es además un derecho fundamental. [41]

Hay que diferenciar, por lo tanto, los supuestos en que la información se obviase por completo – lo que constituiría una vulneración del derecho fundamental y permitiría acudir tanto al art. 44 LOPD y atender a sus infracciones, como a los específicos procesos de amparo ordinario por vulneración de derechos fundamentales –; y los supuestos en que la información aparece pero defectuosa o incompleta – estándose solo ante alguna de las infracciones ya mencionadas que contempla la LOPD –.

De la falta específica de consecuencias en la LOPD puede concluirse que, en caso de incumplimiento del deber de información, deberá estarse a cada caso concreto y sus características. Solo esto va a permitir determinar si hay o no vulneración de un derecho fundamental y las posibles consecuencias que se deriven de cada supuesto.

4.2.3 Derecho a la información de los interesados.

Tras lo expuesto en relación con el deber de información, es incuestionable que los afectados son titulares de un derecho a la protección de sus datos, conformado por un

[40] CANALES GIL, Álvaro. "*Comentario de Álvaro Canales Gil al artículo 5: Forma de practicar el deber de información*" en *Comentario a la Ley Orgánica*… cit. Págs. 412 y 413.
[41] DÍAZ REVORIO, Francisco Javier. "*Comentario de Francisco Javier Díaz Revorio al artículo 5: Los requisitos de la información*" en *Comentario a la Ley Orgánica*... cit. Pág. 447.

conjunto de derechos de forma que la vulneración de uno solo de ellos puede conformar la vulneración del derecho fundamental en su conjunto.

Esto es lo que sucede con el derecho a la información de los interesados, un derecho que es un "complemento indispensable" del derecho a la protección de datos[42] porque este tiene como pilar fundamental el consentimiento, y es indispensable *saber* a qué se consiente, por lo que es básico otorgar este derecho de información al interesado y protegerlo como medio de protección indirecta tanto a su consentimiento como, en definitiva, a su derecho fundamental.

4.3. Tratamiento de los datos.

Visto ya el concepto que aporta el art. 3 c) LOPD de tratamiento de los datos, lo único que puede añadirse en relación al mismo son los requisitos que debe cumplir para considerarse lícito.

Estos requisitos encuentran su raíz en la jurisprudencia del Tribunal Supremo, concretamente en una sentencia de 8 de febrero de 2012[43] y son:

Primero, que ese tratamiento sea imperioso e ineludible para la satisfacción del interés legítimo del responsable del tratamiento (o, en su caso, de aquellos a quienes se comunicasen los datos).

Segundo, que no prevalezcan los derechos y libertades fundamentales del interesado, especialmente el derecho a la intimidad o el derecho a la protección de datos personales. [44]

4.4. Transparencia.

La transparencia es un principio al que se ha de circunscribir la actuación de la Administración, que se manifiesta en el derecho de acceso del afectado al fichero en que se contiene su información.

---

[42] DÍAZ REVORIO, Francisco Javier. "*Comentario de Francisco Javier Díaz Revorio al artículo 5: Características generales del art. 5 LOPD*" en *Comentario a la Ley Orgánica...* cit. Pág. 436.

[43] Sentencia del Tribunal Supremo, Sala III, de lo Contencioso - Administrativo. 08-02-2012. ROJ: STS 585/2012. Nº Recurso. 23/2008. Fundamento de Derecho Tercero. Ponente: Juan Carlos Trillo Alonso.

[44] GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "El interés legítimo… cit. Pág. 437.

No aparece mencionado en la regulación estatal, pero el Reglamento 2016/679 establece al respecto que "*el principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro*".

Este principio, en último término, implica algo tan básico como que los ciudadanos puedan participar en mayor medida en los procesos de toma de decisiones, y garantiza *"mayor eficacia, legitimidad y responsabilidad de la Administración frente a los ciudadanos en un sistema democrático"*.[45]

Para poder comprender completamente la necesidad de proteger los datos, ha de hacerse una breve referencia a la legislación sobre transparencia, distinta del principio de trasparencia.

Esto es necesario porque las legislaciones sobre protección de datos y transparencia se contraponen, de manera que un exceso de transparencia puede vulnerar la efectiva protección de datos de carácter personal, y viceversa.

Se trata de una pugna entre la LOPD y la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno, dirigida a las Administraciones Públicas, poderes públicos y otras entidades del sector público.

De manera sucinta, esta batalla entre la privacidad y la transparencia tiene por objeto determinar si debe predominar la privacidad de los datos personales, o por el contrario, debe primar el objeto de la Ley 19/2013 que, como establece su art.1, no es otro que "*ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias derivadas de su incumplimiento*".

El resultado de esta contraposición no es sencillo de determinar. En palabras de Gema María Ortega Expósito, "*los órganos judiciales y administrativos se han pronunciado al respecto, tratando de calibrar en cada caso esos intereses enfrentados (publicidad y privacidad), tarea que no resulta fácil, dada la complejidad que supone discernir cuál podría ser el elemento preponderante para alcanzar una efectiva*

[45] PIÑAR MAÑAS, José Luis. *Transparencia, acceso a la información y protección de datos.* Varios autores. Dirigido por PIÑAR MAÑAS, José Luis. REUS, S.A. 2014. Pág. 49.

transparencia dentro del respeto a los derechos personalísimos y otros bienes jurídicos constitucionalmente protegidos".[46]

4.5. Transmisiones y cesiones de datos.

A la cesión de datos se refiere la LOPD expresamente, definiéndola en el art. 3 i) como "*toda revelación de datos realizada a una persona distinta del interesado",* de la cual deberá informarse al interesado, tal y como indica el art. 27 de la misma ley.

A la transmisión, por su parte, se refiere solamente en el art. 44.2 d), relativo a las infracciones. No obstante, puede entenderse la transmisión como una actuación similar en esencia a la cesión de datos.

Lo que se refleja en ambos casos, es que datos de los ficheros pueden ser transmitidos o cedidos, siempre y cuando cumplan todos los principios y obligaciones establecidos, ya que, en caso contrario, se verían vulnerados derechos fundamentales de los afectados y se incurriría en infracciones.

Es reseñable, debido a la amplitud del concepto, la extensa posibilidad de situaciones que podrían llevar a incurrir en una infracción por estos motivos, como pone de manifiesto una Sentencia de la Audiencia Nacional de 23 de junio de 2017: "*El concepto jurídico de cesión regulado en nuestra normativa de protección de datos es de gran amplitud, […] reconocida por el Tribunal Supremo […]; si determinados datos se encuentran en poder del titular o responsable del fichero, cualquier comunicación de los mismos a una persona distinta del interesado o afectado, constituye cesión en sentido técnico*". [47]

4.6. El deber de secreto.

El deber de secreto aparece reflejado en el art. 10 LOPD, que establece:

> *El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto*

[46] ORTEGA EXPÓSITO, Gema María. "Transparencia versus Protección de Datos II: Conclusiones".
Disponible en: <http://www.elderecho.com/tribuna/administrativo/Proteccion-Datos-transparencia-cesion-datos_11_1034680001.html> [Consulta: 14 de junio de 2018].
[47] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, sección 1. 23-06-2017. ROJ: SAN 2567/2017. Nº Recurso: 74/2016. Fundamento de Derecho Quinto. Ponente: María Luz Lourdes Sanz Calvo.

profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Se deduce del precepto que el deber de secreto es un principio que prohíbe revelar a terceros cualquier dato de carácter personal sometido a tratamiento.

Es un deber colectivo, que alcanza a todo aquel conocedor de la información. Por lo tanto, corresponderá al responsable del fichero formar y concienciar a todo aquel con acceso a dichos datos, para instar al cumplimiento de este deber.

La afirmación anterior encuentra su justificación en el hecho de que, muchas veces, se incumple el deber por puro desconocimiento o por desliz, siendo la consecuencia la comisión de una infracción.

Dependiendo de la tipología de los datos, distingue Troncoso Reigada entre infracciones leves, graves o muy graves, y recaerán no en el empleado, sino en el responsable del fichero. Ahora bien, considera Troncoso Reigada razonable que este pueda luego iniciar un procedimiento sancionador contra dicho empleado. [48]

Un último e importante aspecto a tener en cuenta acerca del deber de secreto es que supone, en consecuencia, un derecho para los interesados hasta tal punto, que tendrán la posibilidad de exigir su cumplimiento.

4.7. La ponderación de los intereses.

Dada la estrechísima relación existente entre los datos de carácter personal y los derechos fundamentales del titular de los datos, es innegable que, en el momento en el que el responsable quiera tratarlos o cederlos de acuerdo a sus intereses, estos entrarán en conflicto con los derechos fundamentales del interesado asociados a dichos datos.

Habrá que realizar, por ello, una ponderación entre el interés legítimo del responsable del tratamiento y los derechos fundamentales del afectado, para determinar cuál es el que prevalece. En este sentido, muchos de los informes jurídicos de la AEPD determinan que

[48] TRONCOSO REIGADA, Antonio. *La Protección de Datos Personales: En busca del equilibrio*. Tirant Lo Blanch, 2011. Págs. 497 – 499.

los derechos del interesado prevalecerán sobre el interés legítimo del responsable o de quien quiera obtener la información.[49]

Para una correcta ponderación, deberán evaluarse: el interés del responsable del tratamiento, el impacto que la realización del interés supondría para el titular de los datos, el balance provisional de la situación resultante y las garantías adicionales que pudieren aplicarse para evitar impactos indebidos en los titulares de los datos.[50]

4.8. El GT 29.

Relevante papel es el que juega el llamado Grupo de Trabajo del Artículo 29 (en lo sucesivo, GT 29), creado por la derogada Directiva 95/46/CE.

Es un órgano consultivo independiente, compuesto por un Supervisor Europeo de Protección de Datos y por las Autoridades de Protección de Datos de todos los Estados miembros – España forma parte desde el año 1997 –, y en el que podrán participar como observadores las autoridades análogas de los Estados candidatos a pertenecer a la Unión Europea. [51]

Es necesario hacer referencia a este órgano porque, en el ámbito europeo, es quien aporta información y directrices acerca de la protección de datos de carácter personal y de las obligaciones que ostentan los responsables de los ficheros y de su tratamiento. Proporciona sus directrices a través de diversos documentos, que van desde opiniones, recomendaciones y dictámenes, hasta los informes anuales que elabora, con las novedades de cada Estado miembro en materia de protección de datos. Destaca el dictamen 06/2014, que ha proporcionado una gran base para poder llevar a cabo ponderaciones correctas entre interés legítimo de una de las partes y los derechos y libertades de la otra. [52]

---

[49] GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "El interés legítimo… cit. Págs. 425 y 426.

[50] GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "El interés legítimo... cit. Pág. 429.

[51] Agencia Española de Protección de Datos. Canal de documentación. Documentos de trabajo del grupo del artículo 29. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/index-ides-idphp.php> [Consulta: 1 de marzo de 2018].

[52] GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "El interés legítimo… cit. Pág. 438.

5. LOS DERECHOS DE LOS INTERESADOS FRENTE A LA UTILIZACIÓN ILÍCITA DE SUS DATOS.

Los interesados, a la hora de proteger sus datos y frente a las agresiones que estos pudieran sufrir, cuentan con una serie de derechos reconocidos en el Título III LOPD, entre los que destacan los denominados derechos *"ARCO"* (acceso, rectificación, cancelación y oposición), y que es preciso conocer para comprender el régimen de protección de datos personales establecido por el ordenamiento jurídico español. Se trata de una serie de derechos instrumentales que, en su conjunto, constituyen la efectiva protección de los datos de carácter personal a la que tienen derecho los interesados.

5.1. Derecho de acceso.

Recogido en el art. 15 LOPD, supone que el afectado podrá solicitar y obtener la información que precise acerca de sus datos en tratamiento, incluyendo el origen y las comunicaciones hechas o por hacer respecto de los mismos. Además, la LOPD garantiza por medio del art. 15 que esta obtención de información será gratuita para el interesado.

5.2. Derecho de rectificación.

Recogido, pero no definido, en el art. 16 LOPD, por derecho de rectificación debe entenderse lo dispuesto en el art. 31 RLOPD, siendo, por ello, el derecho que tiene todo interesado a que se modifiquen aquellos datos de que es titular en el caso de que resulten ser inexactos o incompletos.

Es, pues, el derecho a corregir errores en los propios datos y así poder asegurar la certeza y garantizar la exactitud de la información que está siendo objeto de tratamiento.

5.3. Derecho de cancelación.

Recogido también en el art. 16 LOPD, debe acudirse nuevamente al art. 31 RLOPD para obtener el concepto.

Se entiende por derecho de cancelación el derecho del interesado a que se suprima del fichero cualquiera de sus datos por ser inadecuado, excesivo, inexacto o incompleto.

La ley añade que esto se dará sin perjuicio del "bloqueo de los datos", es decir, de la identificación y reserva de los datos de forma que solo puedan ser tratados por las

Administraciones públicas, Jueces y Tribunales, por razón de posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de las mismas.

5.4. Derecho de oposición.

El derecho de oposición no se encuentra en la LOPD, pero es nuevamente su reglamento quien se ocupa de reflejarlo y definirlo, esta vez en su artículo 34.

Así, se entiende por derecho de oposición el derecho del afectado a que se cese o no se produzca el tratamiento de sus datos de carácter personal en tres situaciones.

Podrá ejercitarse cuando: el consentimiento del afectado no fuere necesario para dicho tratamiento; el fichero tenga finalidad de actividades publicitarias o comerciales, o cuando el tratamiento tenga como fin la toma de una decisión referida al afectado y se base solo en el tratamiento automatizado de los datos – es decir, basada solo en un tratamiento destinado a evaluar determinados aspectos de su personalidad –.

5.5. Derecho a indemnización.

Este derecho no se refiere en sí mismo a los datos de carácter personal del afectado, sino que aparece recogido en el art. 19 LOPD como medio de reparación derivado de la lesión de los derechos del interesado, bien el derecho a la protección de datos; bien los derechos fundamentales a que este se encuentra ligado – especialmente, honor e intimidad personal y familiar –; o cualquiera de sus derechos o bienes.

Implica el derecho del interesado a ser indemnizado cuando ha sufrido una lesión o daño en sus bienes o derechos por razón del incumplimiento, por parte de los responsables del fichero, de la LOPD.

5.6. Derecho a no aportar datos y documentos en poder de las Administraciones Públicas.

Cuando una Administración pública ya está en poder de ciertos datos y documentos relativos a un ciudadano – especialmente si se encuentran registrados en soportes electrónicos –, este afectado tendrá derecho a que el órgano competente que necesite dichos datos o documentos y no los posea, los recabe por medios electrónicos de aquella Administración que los posea, aun siendo un órgano de una Administración pública diferente.

El interesado está exento de aportar nuevamente los datos y documentos, siendo la Administración actuante quien deba recabarlos.

Ahora bien, este derecho es instrumental, ya que los datos y documentos sobre los que podrá ejercerse son aquellos conexos a una actividad administrativa sustanciada electrónicamente.[53]

5.7. El procedimiento de tutela de estos derechos.

Recogido en los artículos 117 a 119 RLOPD, mediante este procedimiento se podrán hacer valer los derechos mencionados, a fin de obtener una protección adecuada de los datos de carácter personal y de ver amparados todos los derechos de que este complejo derecho fundamental se compone.

Así, el interesado instará la iniciación del procedimiento expresando de manera clara qué preceptos de la LOPD considera vulnerados y su pretensión al respecto. La reclamación la recibirá la AEPD y la trasladará al responsable del fichero para que alegue lo que estime conveniente – para lo cual, tendrá un plazo de quince días –.

Tras ese plazo, se aportarán informes, pruebas, tendrá lugar una audiencia tanto al afectado como al responsable del fichero y, finalmente, la AEPD resolverá acerca de la reclamación en un plazo máximo de seis meses desde la entrada de la reclamación en la AEPD. Además, en ausencia de resolución, el interesado podrá interpretar que se ha estimado su reclamación, ya que dicho silencio administrativo se considerará positivo.

En cuanto a dicha resolución, si resultase estimatoria, el responsable del fichero será requerido para hacer efectivo el ejercicio del derecho tutelado del interesado. Para ello, tendrá diez días desde que se le notifique la resolución, debiendo informar por escrito a la AEPD de su cumplimiento en igual plazo.

6. LA ADMINISTRACIÓN COMPETENTE: LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Respecto de la Agencia Española de Protección de Datos, no se expondrá más que un marco general acerca de qué es y qué funciones cumple respecto a la protección de datos de carácter personal, puesto que centrarse también su organización supondría ocupar una

[53] HERNÁNDEZ CORCHETE, Juan Antonio. *Transparencia, acceso a la información*… cit. Pág. 132.

importante extensión en esta exposición y no aportaría elementos relevantes al estudio del régimen jurídico de la protección de datos de carácter personal. Sin embargo, debido a la importancia que tiene el órgano en la materia, sí es imprescindible conocer qué es y a qué se dedica en este sentido.

La importancia de la AEPD se observa a raíz de todo lo ya expuesto, por lo que se torna fundamental saber qué es exactamente dicha entidad, así como delimitar sus funciones en materia de datos de carácter personal.

La AEPD, tal y como establece el art. 35 LOPD, es un ente de derecho público, una autoridad estatal en materia de protección de datos. Cuenta con personalidad jurídica propia y con plena capacidad pública y privada.

Ahora bien, en cuanto autoridad estatal independiente y a pesar de contar con un estatuto propio (aprobado por el Real Decreto 428/1993, de 26 de marzo), su cauce para relacionarse con el Gobierno es el Ministerio de Justicia.

Actúa de forma independiente del resto de Administraciones públicas, velando por el cumplimiento del conjunto normativo relativo a la protección de datos de carácter personal y controlando, igualmente, dicho cumplimiento. Por lo tanto, se dedica a garantizar y tutelar el derecho a la protección de datos de carácter personal y, consecuentemente, el conjunto de derechos instrumentales ya estudiados.

6.1. Origen y justificación de su creación.

La Agencia surgió en el año 1992, iniciando su actividad dos años más tarde, en 1994.

Surge, por lo tanto, a principios de la década de los noventa, seis años después de la adhesión de España a la actual Unión Europea.

En aquel momento, España ya preveía la limitación del uso de la informática para proteger los derechos fundamentales de los ciudadanos, y ya es sabido que el Tribunal Constitucional determinó que debe inferirse del mismo precepto – art. 18.4 de la Constitución, del año 1978 – la existencia de un derecho fundamental y autónomo a la protección de datos; guiándose por la doctrina de 1983 del Tribunal Constitucional Alemán.

Por lo tanto, en Europa existía ya la idea de un derecho a proteger, relativo a los datos de carácter personal de los ciudadanos, una idea que se fue extendiendo y que se plasmó de

forma clara en un Convenio del Consejo de Europa, concretamente el Convenio 108, y que se fue perfeccionando hasta llegar a la derogada Directiva 95/46/CE.

En ella, el Considerando 62 establecía como necesaria la "*creación de una autoridad de control que ejerza sus funciones con plena independencia […]"*, reforzando dicha idea de independencia en su art. 28.1.

Por lo tanto, la justificación de la creación de la AEPD se encuentra en la confluencia de ambos factores. Por un lado, el asentamiento – en los ámbitos comunitario y nacional – de la idea de existencia de un derecho fundamental a la protección de datos y de la necesidad de una efectiva salvaguarda del mismo; por otra parte, la plasmación de dicha idea en las disposiciones de la Directiva 95/46/CE, cuya finalidad es, en último término, permitir una defensa de este derecho frente a cualquier posible vulneración, incluso frente a los actos de las Administraciones públicas (deduciéndose esto de la nota de independencia).

6.2. Funciones.

La función de la AEPD es, de forma genérica, el control del cumplimiento de la normativa vigente en materia de protección de datos de carácter personal para, de esta forma, garantizar y tutelar a los ciudadanos su derecho fundamental.

No obstante, esta función genérica puede desglosarse en diversas ocupaciones, recogidas en el art. 37 LOPD, y en algunas de ellas pone especial atención a los diversos destinatarios de las mismas.

Así, sus funciones principales son: dictar instrucciones y recomendaciones para adecuar los tratamientos automatizados, en auge actualmente, a los principios de la LOPD y también para la correcta aplicación de las disposiciones legales y reglamentarias en esta materia; informar de los Proyectos de normas de desarrollo de la LOPD y de cualquier Proyecto normativo sobre esta materia; elaborar una Memoria Anual a presentar ante las Cortes; cooperar con órganos y organismos internacionales y comunitarios en materia de protección de datos y representar a España en cualquier foro internacional que se celebre sobre este asunto.

Además, focalizando en los destinatarios de algunas de sus funciones, debe distinguirse entre funciones referidas a los derechos de los ciudadanos y funciones referidas a todo aquel que trate los datos.

En atención a los interesados, atiende sus peticiones y reclamaciones; les informa de los derechos que la ley les reconoce en materia de protección de datos de carácter personal; promueve campañas de difusión de dicha información a través de los medios; y vela por la transparencia de los ficheros de datos de carácter personal.

Finalmente, en cuanto a los responsables de ficheros, del tratamiento y a quienes tratan los datos, emite las autorizaciones requeridas por ley; autoriza las transferencias internacionales de datos; recaba la información que precise de los responsables de los ficheros; en caso de ilegalidad, ordena el cese del tratamiento y la cancelación de los datos y, si esto no fuere suficiente, ejercerá la potestad sancionadora prevista en la LOPD.

Debe mencionarse en este punto, relativo al ente encargado del control del cumplimiento de la LOPD, una nueva figura que surge con el Reglamento Europeo de Protección de Datos: el delegado de protección de datos[54].

No se integra, propiamente, en la AEPD, pero debe conocerse, al menos, qué es esta figura y qué va a suponer en el ámbito de la protección de datos de carácter personal.

Por lo tanto, hay que atender al Considerando 97 del Reglamento Europeo, que establece que el Delegado de Protección de Datos es una especie de "colaborador necesario" para el responsable de la protección de datos de carácter personal, cuando sea una autoridad pública (excepto el poder judicial).

Deberá ser alguien con "*conocimientos especializados del derecho y la práctica en materia de protección de datos"*, así como una figura cuyo funcionamiento será independiente.

Cabe señalar que la mención a la autoridad pública queda justificada en el art. 37.1 a), que establece que cuando el tratamiento de datos lo realice una "autoridad y organismo público" – para determinar estos conceptos hay que acudir a la legislación nacional de cada Estado Miembro –, se deberá designar un delegado de protección de datos.

Así, sucintamente, puede determinarse esta figura como una especie de "delegado del cumplimiento" del nuevo Reglamento.

[54] JIMÉNEZ ASENSIO, Rafael. "El delegado de protección de datos: perfil y encuadre en las organizaciones públicas (en especial en los entes locales)". Págs. 9 y 11.
Disponible en: <https://rafaeljimenezasensio.files.wordpress.com/2018/03/articulo-dpd-4.pdf> [Consulta: 14 de junio de 2018].

7. MEDIDAS DE PROTECCIÓN DE LOS DATOS.

7.1. Medidas técnicas previas a la infracción.

Los derechos y deberes de interesados y responsables del fichero y su tratamiento son, como se ha visto, una vía fundamental para que cualquier afectado por un tratamiento de datos pueda alcanzar una efectiva salvaguarda de su derecho a la protección de sus datos de carácter personal.

Sin embargo, no es la única vía, ya que la LOPD establece, en su art. 9, la necesidad de la adopción – por el responsable del fichero – de una serie de medidas de seguridad, un conjunto de medidas técnicas y organizativas cuyo fin es evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos y los riesgos a que se exponen.

7.1.1. Niveles de protección.

A falta de una mayor especificación legal, es el RLOPD el que proporciona una mayor determinación en lo relativo a las medidas de seguridad a adoptar para conseguir una mayor y mejor protección de los datos de los interesados.

Para ello, en los artículos 80 y 81, el reglamento determina tres niveles diferentes de protección, que deberán aplicarse a los ficheros y los tratamientos en función de su distinta naturaleza y vulnerabilidad. Estos niveles son: básico, medio y alto.

El nivel básico es imperativo para cualquier fichero o tratamiento.

El nivel medio será de implantación para aquellos ficheros que traten de comisión de infracciones (administrativas o penales); sobre información de solvencia patrimonial y crédito; los que se encuentren bajo responsabilidad de las Administraciones tributarias por ejercicio de sus potestades; los que se encuentren bajo responsabilidad de entidades financieras para la prestación de sus servicios; los que se encuentren bajo la responsabilidad de la Seguridad Social o mutuas de accidentes por ejercicio de sus competencias; y aquellos cuyos datos permitan definir y evaluar la personalidad, características y comportamientos de los ciudadanos.

Finalmente, el nivel alto deberá aplicarse a los ficheros o tratamientos referidos a los datos especialmente protegidos; a los referidos a datos recabados para fines policiales sin consentimiento de los afectados; y a aquellos cuyos datos se deriven de actos de violencia de género.

7.1.2. Clasificación reglamentaria de las medidas de protección.

Los tres niveles de protección son aquellos que, en cada caso y en función del fichero y su contenido, deberán cumplir las medidas adoptadas. El RLOPD clasifica las diferentes medidas en función de los niveles ya mencionados, pero es más sencillo seguir la clasificación tradicional para conocerlas y aportar algunos ejemplos para cada nivel de seguridad.[55]

Tradicionalmente, las medidas se han clasificado en tres grupos: técnicas, administrativas – organizativas, y físicas.

Las medidas técnicas son mecanismos implementados en el interior de las redes y sistemas de información para contrarrestar las amenazas que sufren los programas y datos desde las propias redes.

Ejemplos de estas medidas son: la autenticación de usuarios o el control de acceso a los datos – en el nivel básico –; el registro de incidencias o el cifrado de datos – en el nivel medio –; o las copias de respaldo y recuperación – en el nivel alto –.

Por otra parte, se encuentran las medidas administrativas – organizativas. Estas se configuran en torno a normas y procedimientos dictados por responsables y gestores de la seguridad de la información. Son las medidas más relevantes y son más numerosas que las medidas técnicas.

Ejemplos de estas, son: el establecimiento de funciones y obligaciones del personal – en el nivel básico –; la designación de responsables de seguridad o las auditorías – en el nivel medio –; y el establecimiento de sistemas de gestión y distribución de soportes y documentos – en el nivel alto –.

Finalmente, las medidas físicas. Estas buscan proteger los ficheros y equipos de almacenamiento de datos de amenazas del entorno natural y físico en que estos se encuentran situados, como incendios, inundaciones o hurtos.

El único ejemplo de medida física que recoge el reglamento es el control de acceso físico al lugar donde se encuentre el fichero o equipo de almacenamiento, que responde al nivel básico, aunque podrían citarse otros ejemplos, como los sistemas de detección y extinción de incendios, sistemas de evacuación, sistemas de alarma o arcos de detección de ciertos objetos.

[55] RIBAGORDA GARNACHO, Arturo. "*Comentario de Arturo Ribagorda Garnacho al artículo 9: La seguridad de la información"* en *Comentario a la Ley Orgánica*… cit. Pág. 745.

7.2. Medidas a posteriori de la infracción.

Los preceptos de la LOPD, como los de cualquier otro conjunto normativo, son susceptibles de ser obviados, de no cumplirse, lo que da lugar a la comisión de infracciones.

En el marco de la LOPD, estas infracciones llevan aparejadas una responsabilidad civil, que se concreta en el ya mencionado derecho a indemnización del afectado, y una responsabilidad que puede ser penal, o bien, administrativa.

Pero, antes de conocer las consecuencias de las infracciones, es preciso conocer, aun de manera esquemática, las clases de infracciones que se contemplan en la LOPD. Estas se recogen en el art. 44 LOPD y son sancionadas únicamente con multas cuyas cuantías se gradúan en el art. 45.

Así, las infracciones pueden ser leves, graves o muy graves.

Las infracciones leves se regulan en el art. 44.2, siendo sancionadas con multa de 900 a 40.000 € y tanto infracción como sanción prescriben en un año desde la comisión y desde el día siguiente al que adquiera firmeza la resolución sancionadora, respectivamente.

Las infracciones graves se regulan en el art. 44.3, se sancionan con multa de 40.001 a 300.000 €, e infracción y sanción prescriben en dos años.

Finalmente, las infracciones muy graves se contienen en el art. 44.4, se sancionan con multa de 300.001 a 600.000 € y tanto infracción como sanción prescriben en tres años.

Las infracciones siguen la misma clasificación y los mismos plazos de prescripción también en el Reglamento 2016/679 – arts. 83 y 84 – y en el Proyecto de LOPD española de 2018 – arts. 70 – 78 –.

7.2.1. Imposición de sanciones.

El procedimiento sancionador aparece contenido en el art. 48 LOPD – desarrollándose en el RLOPD –, en los arts. 77 – 82 del Reglamento Europeo y en los arts. 63 a 69 del Proyecto de LOPD.

Siguiendo el RLOPD, concretamente sus arts. 127 y 128, el procedimiento sancionador se iniciará por un acuerdo que contendrá los siguientes extremos:

a) La identificación de los presuntos responsables.

Es necesario aclarar que los sujetos que pueden ser responsables de una infracción son los responsables del fichero y del tratamiento, aunque el art. 70 del Proyecto de LOPD "*añade,*

además, a los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea, a las entidades de certificación y a las entidades acreditadas de supervisión de los códigos de conducta".[56]

b) La descripción de los hechos imputados, su calificación y las sanciones que pudieran corresponder.
c) El órgano competente, que será el Director (o Presidente, según el Proyecto de LOPD).
d) Posibilidad del responsable de reconocer su responsabilidad voluntariamente.
e) Instructor, secretario y régimen de recusación de ambos.
f) Derecho del responsable a alegar, a la audiencia en el procedimiento y a proponer pruebas.
g) Proposición de medidas provisionales.

El procedimiento deberá resolverse en el plazo determinado por la normativa para cada procedimiento sancionador, computando en días hábiles – tal y como aclara el Proyecto de LOPD en su Disposición Adicional Tercera –, desde el acuerdo de inicio y hasta la notificación de la resolución o la acreditación de intento de notificación.

Si no hay resolución o no se comunica en estos plazos, el procedimiento caduca y se archivan las actuaciones.

Los apercibimientos y procedimientos sancionadores en esta materia son algo muy habitual. En el año 2016 (a que en la web de la AEPD no se encuentra aún la memoria anual de 2017), se registraron un total de 10.523 denuncias y reclamaciones y, de entre ellas, fueron resueltas 8.112 denuncias de las cuales, 2.471 eran reclamaciones de tutela de derechos.

Además, un ámbito importante en el tema de reclamaciones y denuncias es el ámbito de las teleoperadoras, ya que dicha memoria plasma que *"en el sector de los directorios de telecomunicaciones se aprecia un incremento de las denuncias relacionadas con la publicación de datos; generalmente en directorios telefónicos de Internet. En 2016 la proporción ya llega al 1,3% del total de denuncias, cuando en los años anteriores no llegaban al 1%. Lo significativo es que la mayoría de los directorios denunciados son responsabilidad de compañías que no tienen establecimiento en España y cuyo funcionamiento no se ajusta a la normativa prevista en la normativa española para la elaboración de guías*

[56] DAVARA FERNÁNDEZ DE MARCOS, Laura. Las "10 + 1" Claves del Proyecto de Ley Orgánica de Protección de Datos. *Diario La Ley, Sección Ciberderecho*. 5 de diciembre de 2017. Pág. 10.

telefónicas". [57] Esto, junto a las recientes condenas a Facebook y WhatsApp por tratar y ceder datos sin consentimiento, permite reflexionar sobre la dureza de las sanciones en la materia.

7.2.2. Otras medidas administrativas. Especial referencia a las Administraciones Públicas.

Las consecuencias administrativas de la comisión de infracciones de la LOPD son las multas que prevé el artículo 45.

Ahora bien, todas estas sanciones pecuniarias impuestas ante la inobservancia de los principios y de los derechos del interesado, quedan fijadas en la LOPD formando una amplia horquilla en la que la cuantía deberá ser determinada por la autoridad correspondiente.

Para llevar a cabo esta determinación hay que atender a una serie de circunstancias, que refleja el art. 45 LOPD, y que son: el carácter continuado de la infracción, el volumen del tratamiento, la vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal y el volumen de su negocio, los beneficios que obtuvo gracias a la infracción, los perjuicios causados al afectado, la intencionalidad, la reincidencia, y cualquier otra circunstancia que pudiera resultar trascendente para la graduación y fijación de la cuantía.

Además, el Reglamento Europeo indica otras circunstancias no previstas en la LOPD a tener en cuenta cuando resulte de aplicación la normativa europea, de manera que se aplicará la sanción precedente en la escala a la que correspondiese cuando: se regularizase la conducta irregular de manera diligente, cuando fue la conducta del afectado la que indujo a infringir la normativa, el infractor reconociese espontáneamente su culpabilidad o si la infracción fue anterior a una fusión por absorción de empresas no pudiendo imputarse a la absorbente la infracción. [58]

Finalmente, hay que hacer referencia al apercibimiento. Introducido en el art. 45. 6 LOPD por la Ley 2/2011 de Economía Sostenible, se dudó si el apercibimiento era realmente una verdadera sanción de carácter administrativo.

[57] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Memoria.* 2016.

[58] LÓPEZ ÁLVAREZ, Luis Felipe. *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo.* Lefebvre - El Derecho, S.A. 2016. Pág. 181.

Aunque para autores como Consuelo de los Reyes Marzal Raga, el apercibimiento es una sanción de menor gravedad que la multa,[59] el apercibimiento implica acordar la no apertura del procedimiento sancionador y apercibir al infractor para que, en el plazo que el órgano sancionador determine, adopte las medidas correctoras pertinentes. Esto tendrá lugar cuando los hechos sean constitutivos de infracción leve o grave y si el infractor no hubiera sido apercibido o sancionado en ocasiones anteriores. De modo que se constituye como una especie de aviso previo a la apertura de un procedimiento sancionador si la infracción continúa produciéndose.

Respecto del Reglamento General de Protección de Datos, el apercibimiento aparece contemplado en el Considerando nº 148; y en el Proyecto de LOPD, en el art. 77.2.

Por su parte, las Administraciones Públicas, además de poder sufrir las consecuencias administrativas expuestas, cuentan con un régimen específico, recogido en el art. 46 LOPD, en el art. 77.1 del Proyecto de LOPD (que enumera a qué Administraciones se aplica) y en el art. 83.7 del Reglamento 2016/679, aunque no de manera expresa.

Establece el art. 46 LOPD:

> *"1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.*
>
> *2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.*
>
> *3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.*

[59] MARZAL RAGA, Consuelo de los Reyes. *El apercibimiento: una nueva sanción en materia de protección de datos de carácter personal.* Tirant Lo Blanch, 2015. Pág. 14.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

El art. 46 establece una excepción al régimen sancionador general con el objetivo de reflexionar acerca de si la actuación llevada a cabo por el sujeto público fue acertada o si, por el contrario, conviene corregirla de cara al futuro y al precedente administrativo.

Este argumento no es el único que sirve para fundamentar el distinto régimen sancionador a que se someten las Administraciones en materia de infracciones de la LOPD. Hay que tener en cuenta que, en muchas ocasiones, solo con medidas correctivas será suficiente para enmendar el daño (como se verá en un ejemplo más adelante) y no condicionar futuras resoluciones contrarias a los derechos de los afectados.

Igualmente, en cuanto a las sanciones a imponer, serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas, concretamente en la Ley 40/2015 de Régimen Jurídico del Sector Público, de 1 de octubre, artículos 32 a 37 sobre responsabilidad patrimonial de las Administraciones Públicas. La razón es que las multas establecidas en materia de protección de datos de carácter personal, en el régimen general, pueden alcanzar altas cuantías que ciertas Administraciones, como las locales, podrían no hacer frente por carecer de la capacidad económica necesaria, resultando afectados en ese caso todos los ciudadanos y no solo el interesado, contraviniendo esto el interés general.

Por estos motivos, se manifiesta necesario este especial régimen para las Administraciones Públicas que cometen alguna infracción en materia de protección de datos de carácter personal.

7.2.3. Consecuencias penales.

Las infracciones de la normativa referente a la protección de datos de carácter personal pueden dar lugar a responsabilidad penal, es decir, pueden constituir delitos.

Antes de acudir al Código Penal (CP) para conocer qué delitos se relacionan con los datos de carácter personal, es necesaria una matización: las acciones imprudentes o cometidas por error no serán consideradas delictivas, salvo que se pruebe la intención de causar daños al interesado o a un tercero o, al menos, beneficiarse de los datos obtenidos. [60]

[60] LÓPEZ ÁLVAREZ, Luis Felipe. *Protección de datos personales: adaptaciones necesarias* … cit. Pág. 173.

Pasando ya a los concretos delitos en que entra en juego la protección de datos de carácter personal, se mencionan en diversos delitos, pero gozan de especial trascendencia en el descubrimiento y revelación de secretos.

En primer lugar, en las coacciones, hay que acudir al art. 172 ter 1, 3º CP:

> *"Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana: […]*
> *3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella."*

En segundo lugar, en el descubrimiento y revelación de secretos, habrá que atender a los artículos 197 apartados 2 – 6 y 198 CP:

> *"2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.*
>
> *3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*
> *Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.*
>
> *4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:*

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o
b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.
Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años."

Por su parte, el art. 198 CP establece:

"La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años."

Además, en caso de que estos delitos los cometiese una persona jurídica, se les impondrá multa de seis meses a dos años e incluso se les podría imponer alguna de las penas recogidas en el art. 33.7 b) a g), como disolución de la persona jurídica, clausura del local, suspensión de actividades o intervención judicial hasta cinco años. [61]

Finalmente, en el ámbito de los daños, habrá que atender a los arts. 264.3 y 264 bis CP.

[61] LÓPEZ ÁLVAREZ, Luis Felipe. *Protección de datos personales: adaptaciones necesarias* … cit. Pág. 175.

El art. 264 indica que quien, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años, y que la pena aumentará a pena de prisión de dos a cinco años y multa del tanto al décuplo si el delito lo cometió una organización criminal o se ocasionaron daños graves.

A esto, el apartado 3 añade que:

> *"Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".*

Por su parte, el art. 264 bis, donde habrá que atender también al apartado tercero, añade que:

> *1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:*
>
> *a) realizando alguna de las conductas a que se refiere el artículo anterior;*
> *b) introduciendo o transmitiendo datos; o*
> *c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.*
> *Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.*
>
> *2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.*
>
> *3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona*

para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero."

En definitiva, es claro que la protección de datos de carácter personal no es un asunto que deba tomarse a la ligera, ya que incluso las sanciones a las infracciones que pudieran parecer nimias conllevarán una sanción administrativa (bien apercibimiento, bien multa), darán lugar a una indemnización y, en último término, pueden constituir un delito.

8. CASOS RECIENTES.

Una vez vistos todos estos aspectos acerca de la protección de datos, es indudable que es un derecho cuya existencia se torna imprescindible. Igualmente, su defensa adquiere, cada vez, mayor relevancia frente a los avances tecnológicos y a una legislación proclive a la transparencia, ya que ambas crean un riesgo para el derecho a la protección de datos de carácter personal y para los derechos fundamentales a que este aparece íntimamente ligado.

Estos riesgos, en muchas ocasiones, se transforman (para los afectados) en efectivas vulneraciones y es por ello que los órganos jurisdiccionales han conocido de numerosos asuntos en los que se alegaba, precisamente, la vulneración del derecho a la protección de datos personales. Destaca que las resoluciones sobre esta cuestión han aumentado conforme ha ido avanzando la tecnología y se ha ido requiriendo un número mayor de datos personales para muchas actividades diarias.

Los problemas que pueden surgir en atención a los datos de carácter personal, son numerosos y de distinta índole. Por ello, es interesante conocer algunos de ellos.

8.1. Infracciones por tratar o ceder datos sin consentimiento.

Un primer ejemplo se encuentra en la Sentencia 2567/2017 de la Sección Primera de la Audiencia Nacional, de 23 de junio de 2017.

En este supuesto, se resuelve un recurso contencioso administrativo interpuesto por Orange España, S.A. La empresa había sido condenada al pago de una multa por infracción grave de la LOPD. Concretamente, se consideró que había infringido en art. 11.1 LOPD en relación con el art. 6.1 de la misma ley; es decir, por comunicar datos de carácter personal a un tercero sin contar con el consentimiento del afectado.

Dicha condena se fundamentó en los siguientes hechos:

Orange España, S.A. "*trató los datos de la denunciante […] en relación con un servicio de telefonía, que según la actora produjo un impago de facturas por importe de 307,72 €, […] sin que conste que se originara esa deuda […]*". [62] Posteriormente, formalizó en escritura pública una compraventa y cesión de créditos con la entidad Salus Inversiones y Recuperaciones S.L., siendo Orange la cesionaria y, en dicha cesión, se incluía la mencionada deuda de la denunciante.

En consecuencia, la entidad Salus, procedió a incluir en un fichero los datos asociados a dicha deuda, es decir, los datos personales de la denunciante.

Ella, al tener noticia de estos hechos, solicitó la cancelación de sus datos. No obstante, se denegó la cancelación y la denunciante acudió a la AEPD, alegando la inclusión de sus datos en un fichero sin haberse relacionado previamente con esta entidad y que desconocía la compraventa – en que se incluía la deuda – que había tenido lugar.

Es el recurso de Orange el que la mencionada sentencia resuelve, y lo hace en sentido desestimatorio del recurso porque "e*n definitiva se ha producido, un supuesto de cesión de datos a terceros sin consentimiento del afectado y sin habilitación legal, […] resultando acreditada la infracción imputada a la recurrente*". [63]

Esta resolución muestra uno de los problemas relativos a la protección de datos de carácter personal que es el "tráfico" o comercio de datos de carácter personal, así como el peligro que supone el desconocimiento del interesado acerca de estas prácticas, ya que supone una pérdida de control sobre sus datos personales y, en consecuencia, pone también en peligro otra serie de derechos.

Cuestión distinta se plantea en otro caso de que conoció el mismo órgano y respecto del que dictó también sentencia, en este caso estimatoria.

Los hechos probados de la resolución recurrida aportan un conciso resumen de la situación:

> "*Para la celebración de las bodas de plata de la XXXV promoción de la Academia General Militar de Zaragoza se creó una comisión a efectos de la*

[62] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, Sección 1. 23-06-2017. ROJ: SAN 2567/2017. Nº Recurso: 74/2016. Fundamento de Derecho Segundo. Ponente: María Luz Lourdes Sanz Calvo.

[63] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, Sección 1. 23-06-2017. ROJ: SAN 2567/2017. Nº Recurso: 74/2016. Fundamento de Derecho Sexto, *in fine*. Ponente: María Luz Lourdes Sanz Calvo.

organización del evento que se celebraría en marzo de 2002. Para informar de los actos previstos para la celebración, se formó una comisión formada por algunos miembros de dicha promoción quienes elaboraron un listado informático con los datos de nombre, apellidos, dirección postal y Armé de unos 400 miembros de la promoción. Dichos datos se obtuvieron de las agendas personales de los propios miembros de promoción. […]Para gestionar el evento se firmó un contrato con la agencia de viajes Norte Sur, S.A. […] Para dicha gestión la Comisión hace entrega a la agencia del listado con los datos de los miembros de la promoción. La agencia de viajes se compromete a utilizar dichos datos con la única finalidad de realizar la gestión encomendada, no cederlos a otras personas o entidades, debiendo destruirlos o de volverlos a la Comisión cuando finalice su tarea. […] La agencia de viajes Norte Sur, S.A. envió a los miembros de la XXXV promoción de la Academia General Militar de Zaragoza, cuyos datos constaban en el referido listado, una carta con información sobre la celebración y organización del evento. No consta la utilización de dichos datos para otras actividades diferentes de -las pactadas con la mencionada Comisión. Terminada la relación contractual, el listado de datos fue destruido". [64]

La AEPD consideró que se había producido una vulneración del principio de consentimiento, ya que se habían obtenido datos y se habían cedido a la agencia de viajes sin consentimiento de los interesados, y por ello, impuso una multa que se recurrió. Dicho recurso es el que aquí se trata.

En este caso, la Audiencia Nacional estimó el recurso, en base a lo siguiente:

"*El argumento central de los recurrentes consiste en entender que su acción está excluida del régimen de protección de la ley 15/1999, amparándose en la previsión del artículo 2.2.a). Según este precepto están excluidos del ámbito de aplicación de la ley los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.*

[64] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, Sección 1. 15-06-2006. ROJ: SAN 3077/2006. Nº Recurso: 521/2004. Fundamento de Derecho Primero. Ponente: Carlos Lesmes Serrano.

[…]Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos.

En un caso como el enjuiciado —elaboración de un fichero para celebrar las bodas de plata de una promoción de la Academia General Militar- la finalidad del tratamiento no excede del ámbito que acabamos de expresar pues tiene por objeto mantener los lazos de amistad y compañerismo creados durante el período formativo mediante la celebración de un acto puntual de confraternización de todos los miembros de una determinada promoción con ocasión del veinticinco aniversario de su jura de bandera". [65]

Pese a no ser tan reciente, este supuesto tiene interés porque refleja un caso contrario al anterior, pero relacionado: la cesión de datos de carácter personal. Muestra que no será siempre vulneradora del derecho a la protección de datos, inclusive si no se cuenta con el consentimiento de los afectados.

Por lo tanto, antes de alegar una vulneración del derecho a la protección de datos de carácter personal, habrá de tenerse la cautela de comprobar qué supuestos establecen las leyes como vulneradores de ciertos derechos, constitutivos de infracción y, por encima de todo, de comprobar los conceptos y definiciones que aportan los textos legales de diferentes situaciones.

8.2. Infracciones en las relaciones entre privacidad y vida laboral.

Ahora bien, no todos los problemas que pueden aparecer en relación a los datos de carácter personal se centran en las cesiones de los mismos, sino que hay otras cuestiones relativas a este derecho que, además, pueden relacionarse directamente con otros derechos fundamentales, como el derecho a la intimidad o privacidad.

Ejemplo de esto se encuentra en una sentencia del Tribunal Constitucional, la sentencia 39/2016, de 3 de marzo [66]. En este caso, el departamento de seguridad de Inditex instaló un sistema informático para controlar la caja y, a raíz de ello, se detectó un conjunto de

[65] Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Madrid, Sección 1. 15-06-2006. ROJ: SAN 3077/2006. Nº Recurso: 521/2004. Fundamento de Derecho Tercero. Ponente: Carlos Lesmes Serrano.

[66] Periódico EuropaPress (2017). *El TC avala el despido de una empleada de Inditex grabada cuando robaba dinero de la caja*. Disponible en: http://www.europapress.es/economia/laboral-00346/noticia-tc-avala-despido-empleada-inditex-grabada-cuando-robaba-dinero-caja-20160410124443.html. [Consulta: 14 de junio de 2018].

irregularidades respecto a los ingresos. Consecuentemente, se procedió a la instalación de una cámara que controlase dicha caja sin informar a los trabajadores.

La demandante y recurrente en amparo en este supuesto es una trabjadora del establecimiento, que fue despedida disciplinariamente porque, a través de dicha cámara, fue vista tomando dinero de la caja vigilada por el dispositivo en diversas ocasiones. "*La trabajadora en su demanda sostuvo que en el centro de trabajo no existía comunicación al público ni carteles comunicativos de la existencia de cámaras de videograbación, ni tampoco comunicación a la Agencia de Protección de Datos*" [67]. Alegó, entre otras cosas, la vulneración del art. 18.4 de la Constitución, basándose en que *"[…] en casos como el presente se exige ineludiblemente la información previa al trabajador. En el ámbito laboral, no existe razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE, sin que sea suficiente que el tratamiento de datos resulte en principio lícito o que pueda resultar eventualmente proporcionado al fin perseguido, debiendo el control empresarial asegurar en todo caso la debida información previa. Insiste la recurrente en que en el ámbito del contrato de trabajo, como núcleo de los derechos y deberes derivados del contrato, cuando se produce una sanción disciplinaria a trabajador por incumplimiento de éste, con sanción basada en imágenes captadas por las cámaras de videovigilancia instaladas en el puesto de trabajo, deben de respetarse la protección de datos de carácter personal y su derecho a la información. El tratamiento de los datos sin haber informado al trabajador sobre la utilidad de supervisión laboral asociada a las capturas de su imagen, a la que se ha de añadir la insuficiencia de la existencia de distintivos anunciando la instalación de cámaras y la captación de imágenes y de la notificación de creación del fichero a la Agencia Española de Protección de Datos, para su validez, exige la necesidad de información previa, expresa, precisa, clara e inequívoca a los trabajadores sobre la captación de imágenes, su finalidad de control de la actividad laboral y su posible utilización para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo. De no hacerse así, a su juicio, se vulnera el art. 18.4 CE. Señala que la protección de datos y el derecho de información en el ámbito laboral acarrea la inexistencia de razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE, sin que sea suficiente que el tratamiento de datos resulte en principio lícito o que pueda resultar eventualmente proporcionado al fin perseguido"* [68].

Lo que en este caso se plantea es la confluencia del derecho a la protección de datos y el derecho a la intimidad, junto con los derechos de los trabajadores. La protección de datos

[67] Sentencia del Pleno del Tribunal Constitucional. 03-03-2016. ECLI:ES:TC:2016:39. Nº recurso: 7222/2013. Antecedente 2 c). Ponente: Encarnación Roca Trías.
[68] Sentencia del Pleno del Tribunal Constitucional. 03-03-2016. ECLI:ES:TC:2016:39. Nº recurso: 7222/2013. Antecedente 3. Ponente: Encarnación Roca Trías.

aparece porque la imagen es un dato de carácter personal, pero al entrar en conflicto con el ámbito laboral, habrá de atenderse también a la proporcionalidad de las medidas que el empresario toma en atención a la ordenación de sus recursos. Por tanto, en este tipo de casos habría de llevarse a cabo una ponderación para determinar si la medida fue adecuada, o bien, vulneradora de la intimidad, tal y como manifiesta la resolución.

En el supuesto concreto, tras llevar a cabo dicha ponderación, el Tribunal considera que "*el sistema de videovigilancia captó la apropiación de efectivo de la caja de la tienda por parte de la recurrente que por este motivo fue despedida disciplinariamente. Por tanto, el dato recogido fue utilizado para el control de la relación laboral. No hay que olvidar que las cámaras fueron instaladas por la empresa ante las sospechas de que algún trabajador de la tienda se estaba apropiando de dinero de la caja. En consecuencia, teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE*." [69] Por lo tanto, resolvió de manera desestimatoria.

Llama poderosamente la atención el hecho de poder llegar a escudarse en la protección de datos de carácter personal cuando se llevan a cabo conductas reprobables. En este caso, el resultado fue insatisfactorio para la demandante, pero hay casos en que esta defensa ha dado resultado.

Así lo muestra la sentencia de 9 de enero de 2018, dictada por el TJUE, en la que se ha condenado a España por no proteger la privacidad de varias cajeras de un supermercado, despedidas igualmente por ser captadas, robando productos, a través de una cámara de videovigilancia cuya existencia les era ajena. "*El fallo recuerda que no se cumplió la Ley de Protección de Datos Personales, que incluye "la obligación de informar previa, explícita, precisa e inequívocamente" a los empleados*". [70]

[69] Sentencia del Pleno del Tribunal Constitucional. 03-03-2016. ECLI:ES:TC:2016:39. Nº recurso: 7222/2013. Fundamento Jurídico 4. Ponente: Encarnación Roca Trías.

[70] Periódico ABC (2018) *Estrasburgo condena a España por no proteger la privacidad de cinco cajeras grabadas mientras robaban*. Disponible en: http://www.abc.es/economia/abci-estrasburgo-condena-espana-no-proteger-privacidad-cinco-cajeras-grabadas-mientras-robaban-201801091234_noticia.html. [Consulta: 29 de marzo de 2018].

Cabe destacar que el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal de 2018 "*incluye expresamente la posibilidad de que el empleador video-vigile a sus empleados*" [71], concretamente en el art. 22.

Fuera de estos llamativos supuestos, es bastante probable que en la era tecnológica y de la transparencia, no obstante, el derecho a la protección de datos de carácter personal esté cediendo con cada vez más frecuencia ante otros derechos. Reflejo de ello es, también, otra sentencia del TJUE, que determinó que las empresas "*tienen derecho a leer los correos electrónicos y mensajes instantáneos enviados desde la oficina*" y que "*no es descabellado que un empleador quiera verificar que los trabajadores estén completando sus tareas profesionales durante las horas de trabajo*". [72]

La nota de sensatez fue aportada en un voto particular. Fue el magistrado Paulo Sergio Pinto de Alburquerque quien se manifestó contra este pronunciamiento, entendiendo que *"los trabajadores no abandonan su derecho a la privacidad y a la protección de datos cada mañana a las puertas de su lugar de trabajo".*[73]

Sin embargo, hay ocasiones en que sí debe ceder, permitiéndose la preponderancia de otros derechos. Reciente prueba de ello ha dado el caso del Trabajo de Fin de Máster de Cristina Cifuentes, del que no hay ninguna constancia.

Al requerirse a la Universidad Rey Juan Carlos la publicación de los documentos que mostrasen la realización y aprobado por la señora Cifuentes de su máster, la Universidad se amparó en el derecho a la protección de datos y en que no tenía el consentimiento de la interesada para publicar dichos documentos.

Cabe resaltar, no obstante, que difícilmente pueda recoger ese trabajo algún dato de carácter personal más allá del nombre y apellidos de su autora, quien es, por otra parte, una política reconocida a nivel nacional. Por lo tanto, en este supuesto se intenta subsumir en la legislación protectora de los datos de carácter personal un documento que no contiene esta clase de datos.

---

[71] DAVARA FERNÁNDEZ DE MARCOS, Laura. Las "10 + 1" Claves del Proyecto de Ley Orgánica... cit. Pág. 15.

[72] Periódico El Español (2016) *Por qué Estrasburgo avala que una empresa lea los correos de sus trabajadores.* Disponible en*:* https://www.elespanol.com/mundo/20160114/94490559_0.html [Consulta: 29 de marzo de 2018].

[73] Periódico El Español (2016) *Por qué Estrasburgo avala que una empresa lea los correos de sus trabajadores.* Disponible en*:* https://www.elespanol.com/mundo/20160114/94490559_0.html [Consulta: 29 de marzo de 2018].

Ahora bien, en el momento de realización del trabajo habría de tener todas las asignaturas del máster aprobadas, y en el momento de realización del trabajo, en el expediente académico aparecían dos "No presentado", a lo que el rector de la Universidad ha respondido que se debió a un error informático ya solventado, y se ampara también en la protección de datos para no aportar prueba alguna que sustancie su versión.

Destaca que para este aspecto concreto, sí podría entrar en juego la protección de datos, porque "*entran en juego muchos derechos: libertad de información, protección de datos o derecho de acceso a la información pública. Pero hay un aspecto que lo decanta todo: el alto perfil político de Cifuentes y su rol institucional*". [74] Cuestión aparte es que, si entrase en juego la protección de datos, bastaría con el consentimiento de la señora Cifuentes para que dichos datos pudieren hacerse públicos y se aclarase la situación.

Estos dos casos, contrapuestos, constituyen un claro ejemplo de cómo es necesaria una ponderación casuística y concienzuda, de manera que un derecho tan importante hoy en día por todas sus implicaciones no debe ceder ante cualquier otro según qué circunstancias, porque puede llevar a abusos y conductas con graves consecuencias.

8.3. Datos de carácter personal, tecnología y redes sociales.

Finalmente, otro gran problema a abordar viene relacionado con la "publicidad" de los datos. Con "publicidad", en relación a este problema, no hay que pensar en los datos recogidos en fuentes accesibles al público, sino en el hecho de que cualquier persona, por cualquier método (legítimo o no) tenga acceso a los datos de carácter personal de un afectado y pueda utilizarlos en cualquier sentido y con cualquier fin.

Ya sea por cuestiones laborales, familiares o de amistad, en los últimos dos años se han ido sucediendo varios casos en los que alguien ha obtenido ciertos datos de carácter personal para llevar a cabo actuaciones que interfieren directamente con otros derechos de los afectados.

Un primer ejemplo tuvo lugar el 29 de febrero de 2016, cuando una joven comenzó a recibir mensajes de WhatsApp de un repartidor de la empresa MRW. Este, tras entregarle un paquete, tenía acceso a ciertos datos de la chica, como su número de teléfono y la dirección

[74] Periódico El Diario.es (2018) *Los expertos desmienten a la Universidad: la protección de datos no impide publicar las pruebas del máster de Cifuentes*.
Disponible en: https://www.eldiario.es/politica/contradicen-universidad-proteccion-publiquen-Cifuentes_0_753125320.html [Consulta: 30 de marzo de 2018].

de su domicilio y comenzó a enviarle mensajes con la intención de ligar con ella. Ante tal situación, la joven tuvo que ponerse en contacto con la empresa para formalizar una queja (que al final no interpuso).

Además, la joven publicó una captura de pantalla en la plataforma Twitter y recibió respuesta de otras personas que habían pasado por el mismo suceso: una chica también recibió mensajes de un repartidor (la empresa para la que trabajaba, en este caso, se desconoce), y otra cuenta cómo un empleado de un banco, tras realizar una transacción, le dio su número de teléfono y le pidió que lo llamara. Al no recibir llamada alguna de la mujer, comenzó a enviarle mensajes por WhatsApp. Manifiesta dicha joven que, posteriormente, tuvo noticia de que el empleado del banco había tenido el mismo comportamiento con otra chica. [75]

La misma situación volvió a vivirse, esta vez en Bristol, el 15 de enero de este mismo año, cuando un repartidor de la empresa Just-Eat llevó comida a domicilio a una joven y, al rato, comenzó a enviarle mensajes, igualmente con intención de ligar con ella. La joven también publicó los mensajes en Twitter, y recibió respuesta de jóvenes que habían pasado por lo mismo.[76]

Otra muestra de lo peligroso que es el fácil acceso a los datos personales se dio en Lucena, Córdoba.

Los hechos tuvieron lugar entre 2011 y 2016, cuando un funcionario de la delegación de la Agencia Tributaria de la localidad descubrió que su mujer le había sido infiel.

Ante esta situación, decidió utilizar sus conocimientos informáticos y beneficiarse de su puesto de trabajo, dado que le permitía acceder a ciertas bases de datos – entre ellas, la base de datos confidenciales de los contribuyentes de la Agencia Tributaria, a la que accedió de manera efectiva hasta en siete ocasiones –. Cruzando esta base de datos y una base de datos policial, consiguió una serie de datos identificativos y localizó el teléfono y la dirección

[75] El Periódico (2016). *Una mujer denuncia el acoso de un mensajero de MRW por whatsapp.* Disponible en: https://www.elperiodico.com/es/extra/20160303/mujer-denuncia-acoso-mensajero-mrw-whatsapp-4945790. [Consulta: 30 de marzo de 2018].

También en: Web Cribeo (2016). *Denuncia que un repartidor de MRW intenta ligar con ella por Whatsapp y ESTO es lo que sucede.* Disponible en: http://cribeo.lavanguardia.com/fast_news/9689/denuncia-que-un-repartidor-de-mrw-intenta-ligar-con-ella-por-whatsapp-y-esto-es-lo-que-sucede. [Consulta: 30 de marzo de 2018].

[76] Periódico La Vanguardia (2018). *Acusa a un repartidor de acosarla después de entregarle un pedido de comida.* Disponible en: http://www.lavanguardia.com/comer/al-dia/20180117/4476235061/acusa-a-un-repartidor-de-acosarla-despues-de-entregarla-un-pedido-de-comida.html. [Consulta: 30 de marzo de 2018].

de correo electrónico del amante de su esposa; y como este estaba casado, obtuvo también los de su mujer.

Mediante estos datos, comenzó a llamar y enviar mensajes humillantes y amenazantes a la pareja y a enviar cartas anónimas y correos electrónicos en el mismo tono, incrementando la dureza y frecuencia de las comunicaciones hasta provocar que la mujer necesitase ayuda psicológica.

Además, también accedió al correo electrónico del supuesto amante, cambió la contraseña de la cuenta y accedió al contenido de las conversaciones entre el titular del correo y su infiel esposa.

Este funcionario actuó hasta que, en 2013, el matrimonio consideró insostenibles los contactos y su contenido y decidió presentar una denuncia contra él, que fue condenado a indemnizarlos con 175000 €, a un año y seis meses de prisión y multa de 1464 € por dos delitos contra la intimidad, a tres meses de prisión por un delito contra la integridad moral y a suspensión de empleo durante tres años y a no acercarse a la mujer menos de mil metros ni comunicarse con ella durante seis años. [77]

Situación similar se vivió en 2017 en Santander, cuando un médico accedió al historial clínico de un paciente que había sido amante de su esposa.

Dicho historial es información confidencial y este médico accedió a ella a pesar de que el afectado no era su paciente y a este tipo de datos sensibles únicamente pueden acceder los profesionales sanitarios autorizados. Los usos de la historia clínica deben utilizarse únicamente para garantizar asistencia sanitaria adecuada al paciente y siempre que exista relación asistencial, no concurriendo dicha circunstancia en este caso, si bien es cierto que el médico no utilizó ni divulgó dichos datos en ningún momento. [78]

---

[77] Periódico El País (2016). *Un cargo de Hacienda usó datos fiscales para acosar al amante de su esposa*. Disponible en: https://elpais.com/ccaa/2016/11/13/galicia/1479063232_187698.html. [Consulta: 1 de abril de 2018].

También en: Periódico La Voz de Galicia (2016). *El funcionario de Hacienda que acosó a un matrimonio porque el marido se acostó con su mujer se libra de la cárcel pero pagará casi 19.000 euros*. Disponible en: https://www.lavozdegalicia.es/noticia/santiago/santiago/2016/11/16/funcionario-hacienda-acoso-matrimonio-marido-acosto-mujer-libra-carcel-pagara-19000-euros/00031479295864146318451.htm. [Consulta: 1 de abril de 2018].

[78] Periódico Europa Press (2017). *El médico que accedió al historial del amante de su mujer lo achaca a motivos de salud*. Disponible en: http://www.europapress.es/cantabria/noticia-medico-accedio-historial-amante-mujer-achaca-motivos-salud-20170516153911.html. [Consulta: 1 de abril de 2018].

Finalmente, aunque los casos anteriores hacían referencia a particulares que obtenían datos de carácter personal, hay que hacer referencia necesariamente a un supuesto en que aparece implicada una Administración Pública y que, además, ha tenido consecuencias a partir de su resolución.

En Boecillo, en octubre de 2016, un vecino denunció al Ayuntamiento por haber creado un grupo de WhatsApp en el que fue incluido sin haber dado su permiso o consentimiento.

Dicho grupo de WhatsApp fue creado por el Ayuntamiento de la localidad con el fin de incluir a los vecinos e informarlos sobre cualquier acción o actuación que pudiese conllevar el interés vecinal. Se incluyó a doscientas cincuenta y cinco personas, entre ellas el denunciante, y los números de teléfono móvil de todos ellos eran visibles para el resto de vecinos integrantes de dicho grupo.

El denunciante alegó que en ningún momento prestó su consentimiento para ser incluido en un grupo en que su número de teléfono resultase público, y que los datos personales que tiene el Ayuntamiento son únicamente para "*cuestiones de solicitud de licencias urbanísticas, tasas e impuestos municipales y denuncias por diversas causas*" [79], y no para cualquier otro fin.

Ante esta situación, el denunciante fue eliminado del grupo el mismo día de su creación, lo que motivó que la AEPD, a pesar de la resolución que dictó al respecto, no impusiera medidas correctoras al Ayuntamiento. (Sirva esto como ejemplo para el mencionado régimen del art. 46 LOPD).

No obstante, en dicha resolución – la Resolución 03041/2017 –, la AEPD manifiesta:

a) Que: "*en dichas capturas aparecen los números de teléfono móvil de los participantes que realizan los comentarios mostrados, cuyos perfiles, con la información de carácter personal obrante en los mismos, resultaba accesible a los integrantes del grupo creado. […] Exponen que el número de teléfono es un dato de carácter personal*". [80]

[79] Periódico El País (2017). *Protección de Datos resuelve que es ilegal incluir a personas en grupos de WhatsApp sin su consentimiento.* Disponible en: https://elpais.com/tecnologia/2017/12/20/actualidad/1513786075_415535.html. [Consulta: 1 de abril de 2018].

[80] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución nº 03041/2017. Antecedentes Primero y Cuarto. Págs. 1 y 2. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/admon_publicas/ap_2017/common/pdfs/APP-00023-2017_Resolucion-de-fecha-20-11-2017_Art-ii-culo-10-9-LOPD.pdf. [Consulta: 2 de abril de 2018].

b) Que: el "*artículo 10 regula de forma individualizada el deber de secreto de quienes tratan datos personales, dentro del título dedicado a los principios de protección de datos, lo que refleja la gran importancia que el legislador atribuye al mismo. Este deber de secreto pretende que los datos personales no puedan conocerse por terceros, salvo de acuerdo con lo dispuesto en otros preceptos de la LOPD […].En este caso, ese deber de secreto comporta que el Ayuntamiento de Boecillo, responsable de los datos personales de sus vecinos, no puede revelarlos a terceros, salvo con consentimiento de los afectados o en los casos autorizados por la ley […].En este procedimiento se ha acreditado que el Ayuntamiento de Boecillo ha divulgado los datos personales de los vecinos de ese municipio y del resto de personas incluidos en el grupo de WhatsApp […] toda vez que sus números de teléfono móvil eran visibles para todos los demás miembros del grupo, así como los datos identificativos de los mismos que aparecían asociados a su condición de participantes del grupo. Dado que ha existido una vulneración en el deber de guardar secreto por parte del Ayuntamiento de Boecillo en relación con datos personales de los vecinos incluidos en el grupo de WhatsApp, se considera que ha incurrido en […] infracción […]. El hecho constatado de la difusión de datos personales fuera del ámbito del afectado, establece la base de facto para fundamentar la imputación de la infracción del artículo 10 de la LOPD*". [81]

Lo que ambas afirmaciones expresan tiene una gran trascendencia:

Por un lado, ante la disyuntiva planteada acerca de si el número de teléfono móvil debe ser o no considerado un dato de carácter personal, la AEPD afirma que sí lo es.

Por otro, la resolución resulta aplicable a toda Administración Pública en cuanto son susceptibles de cometer la misma infracción y, por lo tanto, las Administraciones Públicas y los organismos públicos que incluyan números en grupos de WhatsApp sin consentimiento expreso del titular de la línea estarían actuando contra la LOPD.

Ahora bien, un matiz importante a esto último es que no constituirá una infracción cuando un particular agregue, sin contar con consentimiento expreso, a sus familiares y amigos a un grupo de WhatsApp, incluso si los familiares y amigos agregados son desconocidos entre sí.

Así pues, todos estos casos proporcionan una visión muy reducida de un amplísimo problema: en una era en que, para prácticamente cualquier actividad, se requiere que el interesado proporcione sus datos de carácter personal, será necesaria una protección de los mismos mucho más fuerte en ciertos aspectos – sin olvidar tampoco la pugna con la

[81] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución nº 03041/2017. Fundamentos de Derecho V y VI. Págs. 11 y 12.

transparencia – para garantizar que los datos sean objeto de un tratamiento para cuyo fin, y no para ningún otro, se otorgó el consentimiento. El motivo es que, de no ser así, se comprueba asiduamente la gran cantidad de vulneraciones que se producen al derecho a la protección de datos y a muchos otros derechos que, sin duda, deben ser también protegidos ante cualquier tipo de intromisión, cesión o tratamiento ilegítimo, porque solo así la persona tendrá plena seguridad de encontrarse protegida en relación a todo lo que pueda llegarse a saber sobre ella sin su consentimiento.

9. UNA ESPECIAL REFERENCIA AL DERECHO AL OLVIDO.

"*A diario nos traspasan unas mil miradas, pero eso no basta: se institucionalizará además una mirada única, para que no nos abandone ni por un instante, […] la imagen de nuestra vida se archivará en su totalidad para que pueda ser utilizada en cualquier momento en caso de conflicto legal o cuando lo exija la curiosidad pública".* [82]

Es de sobra conocido ya el riesgo que el avance tecnológico actual ha supuesto para la privacidad, la intimidad y los datos de las personas.

Sin embargo, de entre todas las formas en que puede presentarse un fichero de datos de carácter personal, sin duda sobresale uno, que destaca frente a los demás tanto por su inmensa capacidad de almacenamiento, como por el fácil acceso que a él tienen gran cantidad de personas alrededor del mundo: internet.

Internet es una red es capaz de almacenar toda la información que en ella se comparte y, al mismo tiempo, hace realmente sencillo acceder a ella, ya que dicha información se ha mantenido de manera permanente hasta, prácticamente, la actualidad.

Por lo tanto, es uno de los mayores peligros para los derechos fundamentales a la intimidad, el honor, la libertad de pensamiento y de expresión, así como para la reputación personal.

El mantenimiento constante de todo tipo de informaciones puede afectar a estos derechos y la preocupación de los ciudadanos sobre esta materia ha aumentado exponencialmente, debido a la conservación de sus datos de carácter personal unida a la gran

[82] KUNDERA, Milan. *La inmortalidad.* RBA Editores, S.A., 1992. Págs. 36 y 37.

dificultad que, hasta ahora – con la jurisprudencia reciente y el nuevo Reglamento Europeo de Protección de Datos – entrañaba la eliminación de los datos de la red.

Internet, en definitiva, podría suponer el fin del "olvido", no poder "borrar el pasado" y no permitir, en consecuencia, el "derecho a equivocarse y aprender", es decir, el libre desarrollo de la personalidad.

Es por eso que el derecho al olvido "pretende garantizar la privacidad, el libre desarrollo y la evolución de las personas, evitando la persecución constante del pasado. Así, cuando hablamos de "*derecho al olvido" hacemos referencia a posibilitar que los datos de las personas dejen de ser accesibles en la web, por petición de las mismas y cuando estas lo decidan; el derecho a retirarse del sistema y eliminar la información personal que la red contiene*".[83]

9.1. Concepto.

Equiparado en el Reglamento General de Protección de Datos al derecho de supresión, no aparece definido expresamente, no obstante, ni en este ni en la LOPD.

No obstante, puede decirse que el derecho al olvido es la manifestación de los derechos de cancelación o supresión y oposición, aplicada a los buscadores de internet; es decir, *"el derecho de las personas a impedir que datos personales propios circulen por internet sin su consentimiento".*[84]

9.2. Ámbitos de aplicación del derecho.

Dada la importancia que está cobrando actualmente el derecho al olvido, cabe cuestionarse acerca de su aplicabilidad, puesto que hay grandes ficheros que comparten información a nivel mundial, son de fácil acceso y, en algunos incluso es el propio afectado quien proporciona de forma voluntaria sus datos personales; y, en todos los supuestos, puede arrepentirse posteriormente de la información que sobre él aparece de forma pública.

Por ello, es necesaria una breve exposición de la aplicabilidad del derecho al olvido en tres grandes ámbitos: las hemerotecas, los motores de búsqueda, y las redes sociales.

---

[83] SIMÓN CASTELLANO, Pere. *El régimen constitucional del derecho al olvido en internet.* Huygens editorial, 2011.Pág. 395.

[84] ORZA LINARES, Ramón M. El "derecho al olvido" contra la muerte de la privacidad. *Revista de la Escuela Jacobea de Posgrado.* Nº 12. Junio 2017. Pág. 16.

Respecto de las hemerotecas, como ya se ha visto, la aplicabilidad del derecho al olvido viene directamente relacionada con los datos personales que se introducen en los motores de búsqueda y los enlaces a que estos llevan.

No obstante, siguiendo el criterio de la AEPD, lo que reflejan las hemerotecas digitales no puede permanecer eternamente en la "memoria digital" en función del derecho a la libertad de información veraz siempre que dicha información ya no sea relevante en el momento actual, o bien, deberán tomarse las medidas oportunas para que las publicaciones no permitan una identificación del afectado.

Sin embargo, lo que verdaderamente llama la atención respecto del derecho al olvido en las hemerotecas online es la contradicción que supone la aplicación del mismo en este ámbito: modificar o eliminar una información en virtud del ejercicio del derecho al olvido, ¿implica que deba destruirse también cualquier ejemplar del diario conservado en una hemeroteca física, junto a toda la información adicional que contienen? ¿Debe eliminarse solamente dicha información de todos los ejemplares físicos? A todas luces, este hecho sería inadmisible y, prácticamente, imposible de realizar.

Por otra parte, respecto a los motores de búsqueda, estos "*combinan una tecnología de búsqueda fácil con ingentes cantidades de información*". [85] El problema surge, por lo tanto, debido a la gran facilidad que otorgan estos motores para conocer cualquier tipo de dato de carácter personal del afectado que esté inserto en la red. No obstante, también se ha visto ya la postura de la AEPD y del TJUE al respecto: el afectado podrá solicitar la supresión u olvido de dicha información, ya sea porque los datos aparecen habiendo sido obtenidos de manera ilegítima, o legítima pero careciendo ya de relevancia o utilidad. Finalmente, para proteger aquellos datos a que remite el buscador cuando estos figuran en una fuente de acceso público, gozarán del derecho de oposición cuando exista una causa que justifique la necesidad de evitar el tratamiento de estos datos.

Finalmente, en cuanto a las redes sociales, son quizá el mayor peligro en relación al derecho al olvido.

Cada vez existe una mayor afición a compartir absolutamente todos y cada uno de los momentos de la vida diaria. Gustos, aficiones, pensamientos e incluso la propia ubicación son compartidos a través de imágenes, textos y vídeos que, además de reflejar la vida privada,

[85] SIMÓN CASTELLANO, Pere. *El régimen constitucional*… cit. Pág. 402.

aportan una imagen de cara al público que influye en la reputación personal y, en último término, en el honor y dignidad de la persona.

En este contexto es en el que aparece el derecho al olvido como una figura de gran utilidad, puesto que la enorme cantidad de información compartida en la "cultura del *like"* - y, junto con ella, los datos de carácter personal que pueda contener – sale de la esfera de control del usuario/interesado y es en ese momento en el que comienza el problema.

Esta información puede descontextualizarse; modificarse; utilizarse para cualquier tipo de finalidad; el propio usuario puede cambiar de parecer o arrepentirse de la misma… y la perpetuidad de esta información en la red social podría dar lugar a un condicionamiento o a un perjuicio de su futuro.

La problemática se centra en que, en estos supuestos, el consentimiento para el tratamiento de los datos sería máximo: es el propio afectado quien ha procedido a la publicación de los mismos y, aunque ejercitasen el derecho de supresión, este quizá no pudiera ser plenamente efectivo, ya que, como manifiesta Simón Castellano: *"mientras la información fue pública ésta no sólo fue expuesta en la tribuna pública, sino que también fue susceptible de ser copiada o descargada por diferentes usuarios a nivel global, lo que puede impedir una eliminación total y efectiva de la información".* [86]

9.3. Titularidad.

El titular de este derecho puede ser una persona física, pero también puede serlo una persona jurídica o una institución ya que, hoy en día, prácticamente cada mínima actuación es susceptible de generar datos almacenables en internet.

9.4. Origen.

El derecho al olvido implica la limitación o el impedimento de la difusión de cualquier dato de carácter personal a través de internet, siempre que la información sea obsoleta o no tenga relevancia ni interés público, sin perjuicio de que la publicación original fuese legítima.

Su origen se encuentra en la derivación "*de los viejos de derechos de acceso, rectificación, cancelación y oposición que venían siendo reconocidos por las legislaciones de protección de datos de los diversos países en relación con los bancos de datos informatizados. No obstante, su conceptualización posee unas*

[86] SIMÓN CASTELLANO, Pere. *El régimen constitucional*… cit. Pág. 401.

características propias que lo distinguen de los anteriores y que le permiten adaptarse a las nuevas exigencias y tecnologías de la sociedad de la información".[87]

9.5. Derecho al olvido en el Reglamento General de Protección de Datos, 2016/679.

Antes de hablar del derecho al olvido en el Reglamento Europeo 2016/679, es necesario destacar la inclusión del derecho en el propio Reglamento, ya que "*el Reglamento Europeo es la primera normativa en materia de protección de datos que regula, bajo esa denominación, el derecho al olvido*". [88]

Partiendo de esta base, puede continuarse en lo que al derecho al olvido respecta.

Es un derecho que se ha visto reforzado en el Reglamento General de Protección de Datos (el Reglamento 2016/679) precisamente mediante la ampliación del derecho de supresión, debido a que se encontraba en el punto de mira europeo ya desde el año 2014.

El Reglamento Europeo se refiere al derecho al olvido en el art. 17 como derecho de supresión:

> *1. El interesado tendrá 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 concurra alguna de las circunstancias siguientes:*
> *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;*

[87] ORZA LINARES, Ramón M. El "derecho al olvido" contra la muerte de la privacidad… cit. Pág. 13.

[88] DAVARA FERNÁNDEZ DE MARCOS, Laura. Las "10 + 1" Claves del Proyecto de Ley Orgánica... cit. Pág. 7.

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.
2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
e) para la formulación, el ejercicio o la defensa de reclamaciones.

Es un artículo extenso que no aporta, realmente, demasiados datos que permitan definir este derecho con precisión. Por ello, es conveniente conocer la concepción de quien se ha dedicado al estudio del derecho al olvido, así como la concepción jurisprudencial acerca del mismo. Solo esto permitirá un acercamiento más profundo al derecho al olvido en internet.

Siguiendo a Pere Simón Castellano, para comprender el derecho al olvido habrá de escogerse como punto de partida el momento en que los datos personales referidos a una concreta persona o institución son recogidos por una página web. Dicha información, posteriormente, podrá ser tomada de esa web y replicada en diferentes páginas webs, repositorios y en los propios índices de los buscadores.

Será en este momento en el que los datos de carácter personal se encuentren ya en internet y exista la posibilidad de ejercitar, no solo los derechos de rectificación y oposición, sino también el derecho al olvido, ese derecho a limitar o eliminar de internet la información personal ya obsoleta o inútil.

No obstante, no debe caerse en el error de identificar el derecho al olvido con el derecho de cancelación (recogido en el art. 16 de la LOPD de 1999 y en el art. 31 de su reglamento). Esto, sin embargo, se torna en una tarea complicada en relación a ciertas bases de datos oficiales, "*que normalmente son excluidas de la regulación general y suelen presentar numerosas dificultades a la hora de cancelar o, simplemente, de rectificar los datos recogidos*". [89] Esto es así porque, realmente, aunque no existen diferencias sustanciales entre ambos derechos, el derecho al olvido no es un derecho en sí, sino un conjunto de derechos, una manifestación de los derechos ARCO. Se configura especialmente como "*una proyección del derecho de cancelación y el derecho de oposición, dependiendo de cada caso*". [90]

Plantea problemas también el derecho a la libre comunicación de información veraz, un problema que se ve acentuado con el desarrollo de la tecnología.

Si los datos publicados son ciertos, aunque estuvieran obsoletos, no podrían ejercitarse los derechos de rectificación u oposición.

Además, incluso aunque pudieran llegar a ejercitarse, surge un nuevo obstáculo, debido también al desarrollo tecnológico, esta vez, unido a la globalización. Los servidores de internet o las empresas que llevan las páginas webs en que se contienen los datos de carácter personal, usualmente, tendrán su sede en un país diferente al del interesado, cambiando también las leyes aplicables en materia de protección de datos. De este modo, el ejercicio de un derecho puede convertirse en un asunto con un cariz jurídico internacional.

---

[89] SIMÓN CASTELLANO, Pere. *El régimen constitucional*… cit. Pág. 374.

[90] Blog El Español (2015) *Lo que es (y lo que no es) el "derecho al olvido"*. Disponible en: <http://blog.elespanol.com/actualidad/que-es-el-derecho-al-olvido-y-que-no-es/> [Consulta: 14 de junio de 2018].

En consecuencia, puede discernirse que el derecho al olvido es un derecho difícil de delimitar sin entrar en colisión con otros derechos ya reconocidos en la normativa de protección de datos personales, y que la complejidad para comprenderlo aumenta en el momento en que se trata de definir de forma concreta y de determinar un contenido exhaustivo.

Entra en juego aquí la necesidad de acudir a la jurisprudencia, para poder delimitar y concretar la conceptualización del derecho al olvido.

9.6. El derecho al olvido en la normativa española.

El derecho al olvido es un derecho novedoso, que se ha incorporado a la legislación española a partir de la entrada en vigor del Reglamento Europeo de Protección de Datos.

Aparece de manera implícita siguiendo la línea comunitaria, cuando se regula el derecho de supresión en el art. 15 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, de 24 de noviembre de 2017, siendo novedoso precisamente porque no se contemplaba en la LOPD de 1999.

Merece aclaración su aparición "de manera implícita", porque "l*a expresión "derecho al olvido" está contemplada en el Reglamento Europeo pero no en el Proyecto de Ley en el que, en todo momento, se refiere a él como "derecho de supresión". Más allá de la denominación, cabe destacar que el artículo 15 del Proyecto de Ley se remite por completo a lo dispuesto por el Reglamento Europeo en este sentido*". [91] Así, cada vez que en España se hace referencia al derecho al olvido, deberá entenderse por tal el derecho de supresión; aunque esto no siempre será conmutativo.

Surge, junto al nuevo derecho, la cuestión relativa a si puede entenderse o no que sea un derecho fundamental constitucional; es decir, la cuestión sobre la vinculación o no del derecho al olvido a algún precepto constitucional.

El principal motivo de esta duda se encuentra en el conflicto que se produce entre el derecho al olvido y el derecho a la libertad de comunicación de información veraz.

En este sentido, Simón Castellano manifiesta que los interesados podrán, en virtud del derecho al olvido, "*exigir la supresión, ocultación y cancelación de la información personal que contiene la web, con indiferencia si ha sido publicada por el propio afectado o por terceros, siempre y cuando la misma no*

[91] DAVARA FERNÁNDEZ DE MARCOS, Laura. Las "10 + 1" Claves del Proyecto de Ley Orgánica... cit. Pág. 7.

responda a un interés público vigente. En otros términos, el derecho al olvido también incluiría aquellas noticias publicadas antiguamente –en prensa, boletines y diarios oficiales, resoluciones judiciales, etc. –, que contienen datos personales e información que puede dañar la dignidad […] y que no responden a la finalidad por la que fueron publicadas, el interés público". [92]

Dicha afirmación muestra la importancia de determinar si el derecho al olvido es o no un derecho fundamental. Esto es así porque, en caso de colisionar con el derecho a la comunicación de información veraz, el resultado sería distinto según la consideración que tuviera el derecho al olvido.

Si el derecho al olvido no se considerase un derecho fundamental, sería clara la prevalencia del derecho a la información, que es un derecho fundamental reconocido en el art. 20 de la Constitución.

No obstante, en el caso de que el derecho al olvido pudiera considerarse un derecho fundamental, sería necesario realizar una ponderación acerca de qué derecho debería prevalecer en cada caso concreto.

Siguiendo nuevamente a Simón Castellano, de existir un encaje constitucional para el derecho al olvido, este tendría lugar en el art. 18.4 de la Constitución, íntimamente relacionado con el derecho a la protección de datos de carácter personal.

Dado el amplísimo concepto de "dato de carácter personal"[93], es sencillo comprender la relación del derecho al olvido con los datos personales que el art. 18.4 de la Constitución contempla.

La regulación en materia de protección de datos es aplicable a toda aquella información que permita identificar a una persona, quedando incluida también toda la información que aparezca en internet sobre esa persona. Esta información, de quedar reflejada a perpetuidad en la red, puede afectar a una serie de derechos fundamentales de que el interesado es titular (como el derecho al libre desarrollo de la personalidad, a la dignidad y al honor) y es por ello que surge la necesidad de plantearse esta importante cuestión.

En esta línea, *"la AEPD ha recordado que los individuos no deben resignarse ni deben verse expuestos eternamente al tratamiento de sus datos personales, muchas veces contenidos en noticias del pasado*

[92] SIMÓN CASTELLANO, Pere. *El régimen constitucional*… cit. Pág. 396.

[93] Concepto expuesto a lo largo de las páginas 8 a 21 de esta exposición.

que se perpetúan en la web, cuando las noticias o los hechos no tengan relevancia pública o no versen sobre un personaje público". [94]

Por lo tanto, desde la perspectiva de la AEPD, el derecho al olvido sí ha quedado subsumido en el derecho fundamental a la protección de datos, dado que el derecho ha comenzado a ser reconocido fundamentándose precisamente en el derecho a la protección de datos de carácter personal.

Puede concluirse, pues, que el derecho al olvido puede reconocerse – a juicio de la AEPD – como un derecho fundamental siempre que se reconozca dentro del derecho a la protección de datos de carácter personal y que cumpla los principios, ya vistos, que rigen en la regulación del mismo. Solo así, el derecho al olvido alcanzaría el rango de derecho fundamental y, en consecuencia, la máxima protección constitucional.

9.7. Jurisprudencia delimitadora del derecho.

9.7.1. La doctrina del Tribunal de Justicia de la Unión Europea: el caso Google.

El actual auge del derecho al olvido procede del año 2014. El 13 de mayo de ese año, el TJUE dictó la llamada "Sentencia Google", caso paradigmático en la que la Agencia Española de Protección de Datos tuvo un papel importante.

Es la sentencia dictada en el Caso Google vs. AEPD Y Mario Costeja.

En este caso, Mario Costeja consideró lesiva para su honor la información sobre su persona que aparecía en internet, ya que al introducir su nombre en el buscador de Google, aparecía su nombre junto a dos anuncios del diario *La Vanguardia,* del año 1998, relativos a un embargo por deudas del señor Costeja a la Seguridad Social.

El señor Costeja responsabilizaba de esta lesión a la página web y al buscador de Google por facilitar el acceso a dichos datos al proporcionar el enlace de la web. Por ello, reclamó en 2010 ante la AEPD, argumentando que dicha información carecía ya de relevancia alguna.

La AEPD, en su Resolución de fecha 30 de julio de 2014, consideró que no era posible eliminar la información que aparecía en la hemeroteca online del diario y requirió a Google

[94] SIMÓN CASTELLANO, Pere. *El régimen constitucional*… cit. Pág. 397.

a no mostrar la información que afectaba al reclamante en relación al anuncio que aparecía en la página web del diario *La Vanguardia*.

Google, por su parte, alegaba que dicho diario era único y completo responsable, y que su buscador era simplemente un instrumento sin responsabilidad en el contenido de las páginas web a que dirigía en función de la búsqueda. En definitiva, que ni controlaba los datos que aparecía, ni era responsable de los datos o su tratamiento.

Así las cosas, se presentó (por la Audiencia Nacional) una cuestión prejudicial para que resolviera el TJUE, relativa al alcance de los artículos 2, letras b) y d), 4, apartado 1, letras a) y c), 12, letra b) y 14, párrafo primero, letra a) de la, entonces vigente, Directiva 95/46/CE; igualmente, del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea; y que determinase si la Resolución de la AEPD respetaba la Directiva y la Carta.

El TJUE resolvió, manifestando en su sentencia que "*la actividad de un motor de búsqueda, que consiste en hallar información publicada o subida en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de "tratamiento de datos personales", en el sentido del mencionado artículo 2 letra d)*". [95]

Así, el TJUE consideró a Google responsable del tratamiento de los datos del señor Costeja y determinó que estaba obligado a eliminar, de los resultados obtenidos a partir de la búsqueda del nombre del señor Costeja, los vínculos a las páginas web publicadas por terceros que contuviesen información relativa a este, incluso aunque esa información no se borrase previa o simultáneamente de dichas páginas web.

En definitiva lo que estableció el TJUE fue que el tratamiento de datos que realizan los motores de búsqueda deberá someterse a las normas de protección de datos de la Unión Europea. Además, como se desprende de la actuación del señor Costeja y la resolución a su favor, el interesado tendrá derecho a solicitar que, cuando se realice una búsqueda de su nombre en internet, los enlaces a sus datos personales no aparezcan entre los resultados.

Es especialmente interesante la opinión formulada a raíz de esta sentencia por el profesor Orza Linares, sobre la caracterización del derecho al olvido: *"el derecho al olvido no es un mecanismo de "borrado automático". Solo procederá cuando se justifique la necesidad de dicho borrado*

[95] ORZA LINARES, Ramón M. El "derecho al olvido" contra la muerte de la privacidad… cit. Pág. 22.

conforme a los criterios de la normativa sobre protección de datos. No se trata, por tanto, de imponer al prestador de servicios una obligación general de supervisar los datos que trasmitan o almacenen".[96]

De esta se deriva la siguiente conclusión: el interesado solo podrá solicitar el ejercicio de su derecho al olvido y consiguiente eliminación de datos personales de internet siempre que se cumplan una serie de criterios regulados, no teniendo el buscador obligación alguna de supervisar los datos que almacene o a que dirija el motor de búsqueda (tarea que, dado el actual volumen de datos contenidos en la red, sería imposible de realizar en su totalidad).

9.7.2 La jurisprudencia del Tribunal Supremo.

En el ámbito nacional, también comenzó a hacerse hincapié en el derecho al olvido a partir de dicha sentencia.

En primer lugar, la sentencia de la Sala de lo Contencioso – Administrativo del Tribunal Supremo 1381/2016, de 13 de junio de 2016, declara también la importancia de la protección del derecho al olvido, el cual ha reconocido expresamente, y manifiesta, del mismo modo, la responsabilidad que al respecto tendrán los motores de búsqueda:

> *"Es manifiesto, por lo tanto, que es al responsable del tratamiento al que, según la ley, deben exigirse e imponerse las obligaciones derivadas del ejercicio del derecho al olvido y al que corresponde la adopción de las medidas oportunas para su cumplimiento".*[97]
>
> "*Cabe añadir que la conclusión alcanzada se confirma con la actuación de Google Inc, que a la vista de la sentencia del TJUE de 13 de mayo de 2014, ha decidido crear un Consejo Asesor integrado por asesores expertos en regulación europea y presidido por el Presidente de dicha sociedad, cuyo objeto es cumplir con el denominado "derecho al olvido" en Internet que se reconoce en la citada sentencia*". [98]

[96] ORZA LINARES, Ramón M. El "derecho al olvido" contra la muerte de la privacidad… cit. Pág. 23.
[97] Sentencia del Tribunal Supremo, Sala de lo Contencioso, Madrid. 13-06-2016. ROJ: 2722/2016. STS Nº Recurso: 641/2015. Fundamento de derecho sexto. Ponente: Octavio Juan Herrero Pina.

[98] Sentencia del Tribunal Supremo, Sala de lo Contencioso, Madrid.13-06-2016. ROJ: STS 2722/2016. Nº Recurso: 641/2015. Fundamento de derecho noveno. Ponente: Octavio Juan Herrero Pina.

Se encuentra también, en el ámbito del Tribunal Supremo, la sentencia de 21 de julio de 2016 y asimismo referente al derecho al olvido.

En esta, el Tribunal manifiesta lo siguiente:

> "*[…] el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, […] precisa notablemente otras obligaciones, siempre referidas al responsable del tratamiento, […] siendo significativa, a los efectos de este proceso, la previsión contenida en el art. 17, que se refiere expresamente al "Derecho de supresión (derecho al olvido)" y con esta concreta denominación establece que "el interesado tendrá 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 ...", precepto que se complementa con el art. 58, según el cual, entre los poderes de la autoridad de control, se incluye el de ordenar al responsable o encargado del tratamiento que atiendan las solicitudes del ejercicio de los derechos del interesado (art. 58.2 c) y, en concreto, ordenar la supresión de los datos con arreglo al art. 17 y la notificación de las medidas adoptadas por el responsable en los términos del número 2 de dicho art. 17 (art. 58.2.g), medidas que, como señala el considerando 66, se imponen al responsable del tratamiento que haya hecho público los datos, precisamente para reforzar el derecho al olvido. Es igualmente significativo que la decisión de la autoridad de control, aun notificada al establecimiento principal o único establecimiento del responsable en el territorio de un Estado miembro, se adopta en relación con el responsable del tratamiento, que es quien a su vez debe adoptar las medidas necesarias para garantizar el cumplimiento de la decisión. […] Es manifiesto, por lo tanto, que es al responsable del tratamiento al que, según la ley, deben exigirse e imponerse las obligaciones derivadas del ejercicio del derecho al olvido y al que corresponde la adopción de las medidas oportunas para su cumplimiento*". [99]

Por lo tanto, de ambas resoluciones puede deducirse que el Tribunal Supremo sigue la senda marcada por la jurisprudencia europea, dotando al derecho al olvido de una gran

[99] Sentencia del Tribunal Supremo, Sala de lo Contencioso, Madrid, sección 6. 21-07-2016. ROJ: STS 3721/2016. Nº Recurso: 2866/2015. Fundamento de Derecho sexto. Ponente: Octavio Juan Herrero Pina.

trascendencia y haciendo prevalecer el derecho a la protección de datos y el derecho a la intimidad, en muchas ocasiones, sobre el derecho a la libre comunicación de información veraz.

Otra prueba más reciente de la importancia del derecho al olvido, es la resolución de 7 de febrero de 2018 de la Sala de lo Contencioso del Tribunal Supremo[100], en la que muestra el cambio de perspectiva hacia la preponderancia de la protección de datos de carácter personal, influenciada, sin duda, por la vigencia del Reglamento General de Protección de Datos.

Esta resolución manifiesta la relevancia del derecho al olvido y los casos en que puede ser operativo en varios de sus fragmentos:

"*Partiendo, así, de la jurisprudencia constitucional y comunitaria que interpreta la normativa aplicable, la Sala concluye que […] debe prevalecer el derecho a la protección de los datos personales. Entiende, en este sentido, que, aun siendo evidente el interés público de la noticia y el interés legítimo de los internautas a su acceso, […] la información difundida […] carece de una de las notas que deber concurrir en el legítimo derecho a la libertad de información: su veracidad*". (Hecho Segundo).

Y continúa, algo más adelante (en el Hecho Cuarto):

> "[…] *La ausencia de exactitud de la información facilitada en los enlaces ofrecidos por el buscador de Google y su carácter lesivo para la privacidad, consideración social y profesional del reclamante determinan la prevalencia del derecho a la protección de datos de carácter personal del reclamante. El tratamiento de los datos personales del denunciante realizado por Google sin su consentimiento no encuentra amparo en el legítimo derecho a la libertad de información, al no tener constancia de su veracidad*".
>
> *"[…] Tras la oportuna ponderación de los derechos en conflicto, la Sala declara la prevalencia del derecho a la protección de los datos de carácter personal (derecho al olvido) del reclamante ante la AEPD. […] Es cierto que la Sala de lo Contencioso-Administrativo ha dictado ya diversas sentencias en materia de protección de datos de carácter personal y de derecho*

[100] Auto del Tribunal Supremo, Sala de lo Contencioso, Madrid, sección 1. 07-02-2018. ROJ: ATS 732/2018. Nº Recurso: 5579/2017. Ponente: José María del Riego Valledor.

al olvido […] y que no resulta preciso un pronunciamiento general sobre la necesaria labor de ponderación que corresponde al órgano judicial cuando, en ejercicio del derecho al olvido por parte de un particular, entran en conflicto los derechos a la libertad de expresión y/o información […] y el derecho a la protección de datos de carácter personal en relación con el artículo 18. 4 CE. Sin embargo, la determinación de si en esa labor de ponderación - atendiendo a los principios de calidad y pertinencia de los datos- la veracidad de la información que exige el artículo 20. 1 d) CE debe interpretarse como la necesaria exactitud de los datos contenidos en los enlaces a los que remite el motor de búsqueda y si, de ser sí, la constatación de la ausencia de veracidad puede fundamentar la solicitud de cancelación de los datos personales ante el gestor del motor de búsqueda como responsable de su tratamiento, es una cuestión sobre la que no se ha pronunciado esta Sala Tercera y que trasciende del caso objeto del proceso". [101]

Esta resolución, además, implica la existencia de un problema al que debería ponerse pronta solución: debe formarse jurisprudencia aclaratoria de si, "*en la labor de ponderación del derecho a la información y del derecho a la protección de datos de carácter personal (desde la perspectiva del derecho al olvido) cuando ambos entran en conflicto, el requisito de veracidad de la información que exige el artículo 20. 1 d) CE debe entenderse como exactitud de la información contenida en los enlaces a que remite el motor de búsqueda y, en ese caso, si su ausencia puede fundamentar válidamente una solicitud de cancelación de datos personales ante el gestor del motor de búsqueda como responsable del tratamiento de dichos datos personales".* [102]

Por otra parte, en el caso de la AEPD, el caso de Mario Costeja no fue su primer acercamiento al derecho al olvido. La Agencia ha tratado de lograr ambos fines, delimitación y definición del derecho al olvido, a través de sus resoluciones que, en este ámbito, se adelantan incluso a esta "Sentencia Google", ya que se remontan al año 2007.

---

[101] Auto del Tribunal Supremo, Sala de lo Contencioso, Madrid, sección 1. 07-02-2018. ROJ: ATS 732/2018. Nº Recurso: 5579/2017. Razonamiento Jurídico segundo. Ponente: José María del Riego Valledor.

[102] Auto del Tribunal Supremo, Sala de lo Contencioso, Madrid, sección 1. 07-02-2018. ROJ: ATS 732/2018. Nº Recurso: 5579/2017. Razonamiento Jurídico segundo. Ponente: José María del Riego Valledor.

Ahora bien, en el año 2007, la AEPD consideraba que las publicaciones veraces eran correctas y que no era competente para valorar las posibles colisiones con otros derechos fundamentales, y que las hemerotecas no eran bases de datos susceptibles de tratamiento, quedando fuera del ámbito protector de la normativa de protección de datos. Argumentaba que estas hemerotecas no publicaban ningún dato personal por sí mismas. También, respecto de los buscadores, manifestó que la información no se contenía en ellos, sino en las páginas a las que dirigen a partir de la búsqueda, siendo los responsables de estas páginas los responsables del tratamiento de los datos.

Sin embargo, respecto de los buscadores de internet, la AEPD cambió de criterio en sus resoluciones en torno al año 2009. Será a partir de entonces cuando la Agencia señale que *"la libertad de información no impone que los datos personales del reclamante figuren en los índices que utiliza Google para facilitar al usuario el acceso a determinadas páginas, ni tampoco preceptúa que figuren en las páginas que Google conserva temporalmente en memoria caché"*. [103]

Lo que esto quiere decir es que la AEPD pasó a considerar a Google, y también a cualquier otro motor de búsqueda, encargado de evitar que ciertos datos de carácter personal puedan recuperarse mediante la búsqueda. Fundamentó esto la AEPD en la existencia del derecho de oposición frente a la libertad de información.

Además, en lo relativo a las hemerotecas de prensa, en la Resolución de 26 de enero de 2009, determinó que dichos medios de comunicación debían ponderar si su actuación, al publicar ciertos datos sobre una persona, conciliaba o no el derecho a la libertad de información y la protección de datos de carácter personal de dicha persona.

A raíz de esta resolución, lo que habrán de tener en cuenta a la hora de publicar – y mantener, posteriormente, en las hemerotecas – son aquellas informaciones que permitan identificar y dotar de relevancia pública a la persona; deberán tomar medidas para evitar dicha identificación a través de la supresión del nombre e, incluso, de las iniciales y prescindiendo de cualquier referencia que pudiera llegar a permitir la determinación de la identidad de la persona; y deberán tener en cuenta, finalmente, acerca de la inconveniencia de mantener permanentemente el acceso a una serie de datos contenidos en noticias cuya relevancia actual haya o pueda haber desaparecido, puesto que de estas noticias puede derivarse una vulneración del derecho a la intimidad, a la privacidad y a la protección de datos.

[103] ORZA LINARES, Ramón M. El "derecho al olvido" contra la muerte de la privacidad… cit. Pág. 17.

La Agencia, desde el año 2009, ha mantenido esta línea de responsabilidad en sus resoluciones, tal y como muestra con su participación en el caso de la "Sentencia Google", considerando que ante informaciones públicas y legítimas carentes ya de relevancia, los interesados podrán ejercer este derecho al olvido frente a los motores de búsqueda y oponerse al tratamiento de sus datos que estos realizan.

Cabe señalar una importante consecuencia que se deriva de todas estas resoluciones, y es que los algunos motores de búsqueda han creado páginas web a disposición de los ciudadanos europeos. A través de ellas, podrían acceder a una serie de formularios para solicitar la supresión de sus datos de carácter personal.

Este sistema, puesto a disposición de los interesados y los potenciales usuarios del buscador, permitiría conseguir que no apareciesen datos personales vinculados al nombre entre los resultados de la búsqueda.

El único elemento que se interpondrá entre el afectado y la consecución de su propósito será la evaluación que, de dicha solicitud, deberá realizar el mencionado Consejo Asesor de Google [104] (mencionado en la sentencia 1381/2016 del Tribunal Supremo).

9.8. Procedimiento para su ejercicio.

Vista la gran trascendencia que actualmente tiene el derecho al olvido, es necesario conocer, de manera muy sucinta, el procedimiento establecido para el ejercicio de este derecho, que queda determinado tras la entrada en vigor del Reglamento Europeo de Protección de Datos.

Este procedimiento puede deducirse de la mencionada sentencia del Tribunal Supremo 1381/2016, de 13 de junio de 2016, que permite resumir de manera sencilla los pasos a seguir a la hora de hacer valer el derecho de supresión o derecho al olvido.

Así, en primer lugar, el interesado deberá reclamar o comunicar su deseo de supresión de sus datos de carácter personal del fichero en que se encuentren recogidos. Deberá comunicarlo al responsable del tratamiento del fichero, mediante el ejercicio del derecho de supresión.

Recibida o no una respuesta por parte del responsable, el interesado podrá después formular una reclamación ante la AEPD, quien deberá dictar una resolución en el plazo

[104] Consejo de expertos al que Google consulta para recibir ayuda sobre cómo aplicar la sentencia del "caso Google" y el derecho al olvido en todos los casos posteriores que se susciten.

máximo de seis meses. Además, contra esta resolución, el afectado podrá interponer el correspondiente recurso contencioso – administrativo.

Así, llegado el interesado a la vía jurisdiccional, el proceso contencioso – administrativo continuará hasta su terminación por cualquiera de las formas previstas en la ley. En caso de terminar con una sentencia, será recurrible en amparo y susceptible de llegar al TJUE.

10. CONCLUSIONES.

I. El derecho a la protección de datos es un derecho de carácter fundamental ya desde su reconocimiento, debido a su estrecha relación con el derecho a la intimidad y su encuadre en el art. 18 CE, y un derecho necesitado de una especial protección por su importancia.

II. El concepto de "dato de carácter personal" es un concepto muy amplio, pero está desactualizado y deberían incluirse en él tanto el número de teléfono móvil (debido a las redes sociales que se valen del mismo), como la dirección IP.

III. La determinación del Reglamento Europeo por ampliar la protección de los datos personales de los menores es admirable, pero debería establecer medidas concretas para hacer efectiva dicha protección, especialmente en el ámbito de las redes sociales, y no solo limitarse a indicar ciertas pautas.

IV. Respecto a la transparencia, no debería primar en todo caso sobre la protección de datos, sino que debería realizarse una estricta ponderación casuística con base en criterios que también deberían ser exhaustivamente plasmados en la normativa.

V. La figura del Delegado de Protección de Datos resulta innecesaria, debido a que la protección y control de la protección de los datos de carácter personal ya la ha venido desarrollando de forma satisfactoria la AEPD.

VI. El apercibimiento resulta, igualmente, poco útil, puesto que es dudoso que un simple aviso de posible sanción para aquellas entidades que tratan un gran volumen de datos y cometen infracciones asiduamente, vaya a ser disuasorio de su actividad.

VII. En el mismo sentido, y atendiendo a los datos de infracciones aportados por las Memorias de la AEPD, las sanciones deberían incrementar su dureza, debido a que a las grandes entidades les es preferible, con frecuencia, pagar las cuantías por las que son sancionadas, y continuar con dichas infracciones, ya que sus beneficios siguen siendo considerables a raíz del tráfico de datos por el que se las sanciona, y esto se contrapone al art. 29.2 de la Ley 40/2015, de Régimen Jurídico del Sector Público, que establece que

"el establecimiento de sanciones pecuniarias deberá prever que la comisión de las infracciones tipificadas no resulte más beneficioso para el infractor que el cumplimiento de las normas infringidas."

VIII. Finalmente, ya que el Reglamento Europeo no determina con detalle los aspectos del derecho al olvido, la legislación española (en especial el Proyecto de Ley) debería ahondar más en esta cuestión, concretarlo y determinar sus aspectos de modo más preciso, no simplemente mencionándolo, para suplir esta falta de información y caracteres del derecho.

IX. En definitiva, la importancia de los datos de carácter personal en la actualidad hace necesaria la existencia de un régimen jurídico protector completo, específico y concreto, que permita el disfrute de este derecho fundamental en consonancia con el resto de derechos reconocidos, y que deberá desarrollarse acorde al avance tecnológico actual, para asegurar una efectiva protección de nuestros datos.

REFERENCIAS BIBLIOGRÁFICAS.

Albaladejo García, Manuel – *Derecho Civil. Introducción y Parte General. Vol. II*. Bosh, 1977.

Andreu Martínez, María Belén – *La protección de datos personales de los menores de edad.* Aranzadi, 2013.

Conde Ortiz, Concepción – *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad.* Dykinson, 2005.

Galán Muñoz, Alfonso – *La protección de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación.* Tirant Lo Blanch, 2014.

Garriga Domínguez, Ana – *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua.* Dykinson, 2016.

Gil González, Elena – *Big data, privacidad y protección de datos.* Agencia Estatal Boletín Oficial del Estado, 2016.

Hernández López, José Miguel – *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional.* Aranzadi, 2013.

Kundera, Milan – *La inmortalidad.* RBA Editores, S.A., 1992.

López Álvarez, Luis Felipe – *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento Europeo.* Lefebvre-El Derecho, S.A., 2016.

Marzal Raga, Consuelo de los Reyes – *el apercibimiento: una nueva sanción en materia de protección de datos de carácter personal.* Tirant Lo Blanch, 2015.

Simón Castellano, Pere – *El régimen constitucional del derecho al olvido en internet.* Huygens editorial, 2011.

Troncoso Reigada, Antonio – *La protección de datos personales: en busca del equilibrio.* Tirant Lo Blanch, 2011.

Varios autores (coordinado por Aparicio Vaquero, Juan Pablo; Batuecas Caletrío, Alfredo) – *Algunos desafíos en la protección de datos personales.* Editorial Comares, Granada, 2018.

Varios autores (dirigido por Piñar Mañas, José Luis) – *Transparencia, acceso a la información y protección de datos.* REUS, S.A. 2014.

Varios autores (dirigido por Troncoso Reigada, Antonio) – *Comentario a la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno.* Aranzadi, 2017.

Varios autores (dirigido por Troncoso Reigada, Antonio) – *Comentario a la Ley Orgánica de Protección de Datos de Carácter personal.* Aranzadi, 2010.

ARTÍCULOS.

Davara Fernández de Marcos, Laura – "Las 10 + 1 Claves del Proyecto de Ley Orgánica de Protección de Datos", *Diario La Ley, Sección Ciberderecho.* 2017.

Guasch Portas, Vicente y Soler Fuensanta, José Ramón – "El interés legítimo en la protección de datos". *Revista de Derecho UNED.* Nº. 16, 2015.

Minero Alejandre, Gemma – "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario Jurídico y Económico Escurialense*, 2017.

Ortega Expósito, Gema María. - "Transparencia versus Protección de Datos II: Conclusiones*", Lefebvre - El derecho,* 2016.

Orza Linares, Ramón M. – "El derecho al olvido contra la muerte de la privacidad". *Revista de la Escuela Jacobea de Posgrado.* Nº 12, 2017.

WEBGRAFÍA.

www.abc.es

www.aepd.es

www.boe.es

www.cribeo.lavanguardia.com

www.dej.rae.es

www.derechoshumanos.net

www.eldiario.es

www.elespanol.com

www.elpais.com

www.elperiodico.com/es/

www.europapress.es

www.lavanguardia.com

www.lavozdegalicia.es

www.poderjudicial.es

www.tribunalconstitucional.es