El nuevo Reglamento UE 2016/679 sobre protección de datos personales: análisis y repercusiones. Especial referencia a los ficheros de solvencia patrimonial y su responsabilidad civil

Víctor Manuel Seligrat González
Abogado. Especialista en responsabilidad civil.
Doctor en Derecho Civil

Este trabajo ha sido seleccionado para su publicación por: don Francisco Gil Durán, doña María José Morillas Jarillo, don José María Segovia Cañadas, don Antonio Serrano Acitores y don Mariano Yzquierdo Tolsada.

Extracto

El tratamiento de datos personales debe realizarse asegurando todas las garantías previstas en la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre. No obstante, esta normativa ha experimentado un gran cambio a partir del 25 de mayo de 2018, momento en que entró en vigor el Reglamento de la Unión Europea 2016/679, el cual tiene eficacia directa y obliga a una modificación de la ley española a fin de alcanzar una congruencia entre ambas normativas. Estos cambios plantearán numerosas dificultades, como son las nuevas obligaciones que deben asumir, entre otros, los titulares o encargados de aquellos ficheros que recogen, administran, etc., datos de carácter tanto estrictamente económico, como aquellos otros que tienen un carácter económico más indirecto. Por ello, el objeto del trabajo, además, está enfocado en la responsabilidad civil que puede surgir en este ámbito. Especialmente, el trabajo se centrará en los denominados registros de morosos, los cuales tienen claramente un significado económico. Y, por otro lado, se abordará el estudio de los posibles daños surgidos con origen en la eventual vulneración de protección de datos realizada por los titulares de bases de datos con un carácter económico más indirecto, como es el caso del llamado «fichero de la Central de Riesgos del Banco de España» (CIRBE).

Palabras clave: protección de datos; Reglamento de la Unión Europea 2016/679; responsabilidad civil; intromisión ilegítima; ficheros de solvencia patrimonial.

Fecha de entrada: 03-05-2018 / Fecha de aceptación: 10-07-2018

Cómo citar: Seligrat González, V. M. (2019). El nuevo Reglamento UE 2016/679 sobre protección de datos personales: análisis y repercusiones. Especial referencia a los ficheros de solvencia patrimonial y su responsabilidad civil. *Revista CEFLegal*, *218*, 5-38.

The new EU Regulation 2016/679 on protection of personal data: analysis and effects. Special reference to asset solvency files and their civil liability

Víctor Manuel Seligrat González

Abstract

Processing of personal data must be done protecting all guarantees provided by Spanish Organic Law on Data Protection 15/1999, of December 13. However, this Organic Law has suffered a major change since May 25, 2018, when the European Union Regulation 2016/679 is enforceable, as a result of its direct effect. Furthermore, it implies the obligation to modify Spanish law in order to achieve congruence between both regulations. These changes will arouse several difficulties and among them are the new obligations that must assume asset solvency files with a strict economic nature as well as those with an indirect economic character. Thus, the study also focuses on civil liability that may arise in these areas. Especially, the paper analyzes the so-called records of defaulters, which clearly have an economic nature. And besides this, the study addresses eventual damages that find its source on an infringement of data protection by holders of data bases with a more indirect economic character, such as the known as «file of Risk Center of the Bank of Spain» (CIRBE).

Keywords: data protection; European Union Regulation 2016/679; civil liability; illegitimate intrusion; asset solvency files.

Citation: Seligrat González, V. M. (2019). El nuevo Reglamento UE 2016/679 sobre protección de datos personales: análisis y repercusiones. Especial referencia a los ficheros de solvencia patrimonial y su responsabilidad civil. *Revista CEFLegal*, *218*, 5-38.

Sumario

1. Introducción

El tratamiento de datos personales es un campo que desde hace años ha planteado problemas desde el inicio en su regulación, esto es, en la derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, hasta la vigente Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre. Este panorama se vuelve más complejo desde el 25 de mayo de 2018, momento en que entró en vigor el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[1] (en adelante, Reglamento UE 2016/679). Ahora bien, esta norma es más garantista para el particular que las anteriores y su importancia radica no solo en la extensión y matización de cara a la regulación de una nueva normativa sobre protección de datos donde, entre otras cuestiones, se modifican e introducen principios nuevos. También, esta norma de la Unión Europea tiene mayor repercusión que antecesoras dada su naturaleza, dado que, al ser un reglamento, goza de eficacia directa y no necesita de ningún acto de transposición, como ocurre con las directivas de la Unión Europea, de cara a su aplicación dentro de los Estados miembros. Este hecho, que debería ser una garantía de protección para el ciudadano, para el Estado legislador le puede suponer más bien una carga, ya que entre la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre y el Reglamento UE 2016/679 existen desconexiones normativas que conllevan el efecto de que pueda surgir una incongruencia entre la normativa interna española y aquella otra aprobada por el legislador de la Unión Europea, la cual, en caso de conflicto, debería prevalecer sobre la primera. Sin embargo, en el momento de redactar estas líneas, el Gobierno es consciente de esta realidad y por ello se está en tramitación el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal aprobado por el Ministerio de Justicia. Es más, el 24 de noviembre se publicó en el Boletín Oficial del Congreso de los Diputados el inicio de la tramitación de este proyecto. Ahora bien, estará por ver la responsabilidad del legislador de cara a adaptar correctamente la legislación interna de conformidad con aquella impuesta desde la Unión Europea y espero que no resulte una ocasión desaprovechada para poder implementar mejoras o actualizaciones al Reglamento UE 2016/679 y que no se limite a ser una modificación que únicamente realice remisiones a la norma de la Unión Europea o transcripciones literales.

[1] Diario Oficial de la Unión Europea, serie L número 119, de 4 de mayo.

Por otro lado, el estudio aborda uno de los grandes problemas que existía con anterioridad al 25 de mayo de 2018 y se complica aún más a partir de dicha fecha, como son los ficheros de solvencia patrimonial, pues no solo entra en juego la legislación sobre protección de datos sino que están íntimamente vinculados con el derecho fundamental del artículo 18.4 de la Constitución que reconoce que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos» y la responsabilidad que surge en caso de su vulneración. Estas dificultades se acrecientan debido a la dicotomía que existe en los ficheros de solvencia patrimonial entre aquellos que tienen un carácter estrictamente económico y otros que tiene un efecto económico más indirecto. Los primeros aluden a los llamados «registros de morosos». Este tipo de registro constituyen ficheros de datos personales cuyo fin es informar a operadores económicos, como son los bancos (aunque su utilidad no se limita a estas entidades sino también a otro tipo de empresas que conceden crédito a sus clientes o cuyas prestaciones son objeto de pagos periódicos), sobre qué potenciales clientes han incumplido obligaciones dinerarias anteriormente y, por tanto, no son merecedores de confianza en futuras contrataciones, y alertar sobre su solvencia patrimonial económica con carácter directo. Y en cuanto a los segundos, afectan, entre otras cuestiones, a posibles operaciones financieras futuras del titular de los datos (por ejemplo, solicitud de avales, fianzas, etc.), siendo el fichero de la Central de Riesgos del Banco de España (CIRBE) uno de los más relevantes. En este tipo de registros, se pueden recoger datos sobre la posible solvencia patrimonial del titular de datos aunque su finalidad no es en atención al incumplimiento de deudas dinerarias, como en los denominados «registros de morosos», sino en referencia a determinadas cargas u obligaciones que ha adquirido el titular de los datos y que pueden ser de utilidad a entidades de cara a valorar su solvencia patrimonial y los riesgos que asumen si contratan con esta persona. Por ello, ambos tipos de registros adquieren gran repercusión y la inclusión errónea de datos personales puede dar lugar a indemnizaciones, respecto de las que, como se observará en el estudio, existirán diversas opciones para fundamentar su reparación (aunque los tribunales tengan la tendencia de acudir al concepto de «intromisión ilegítima» en virtud de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen).

2. Marco normativo del derecho a la protección de datos de carácter personal previo a la entrada en vigor del Reglamento UE 2016/679

La norma sobre la que pivota la regulación del derecho a la protección de datos de carácter personal es el artículo 18.4 de la Constitución, en el cual se estipula que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Así, en desarrollo de este precepto se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento au-

tomatizado de los datos de carácter personal, actualmente derogada[2]. Por ende, la regulación vigente se encuentra en la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre[3]. Debe destacarse que lo que en un primer momento podía parecer un simple mandato al legislador en virtud del artículo 18.4 de la Constitución, encaminado a regular el uso de la informática o, incluso, interpretado como una mera garantía institucional (una regulación del uso de la informática que garantizara determinados derechos y principios), adquirió una importancia de mayor rango en función de la jurisprudencia del Tribunal Constitucional. Por tanto, el uso de la informática vino a constituir un auténtico derecho fundamental desarrollado por el Tribunal Constitucional. Esta importancia se debe, entre otras cuestiones, a que como ya señaló la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, el precepto constitucional referido tiene como fin proteger la libertad del individuo frente a las potenciales agresiones a la dignidad y a la libertad provenientes del uso ilegítimo de datos mecanizados. De este modo, desde las primeras sentencias dictadas por el Tribunal Constitucional se consideró que el artículo 18.4 de la Constitución consagra tanto un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, como también un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos. Así, como destaca la inmediatamente referida Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, se trata del derecho de control sobre los datos relativos a la propia persona insertos en un programa informático, denominado como *habeas data*. Igualmente, otras sentencias del Tribunal Constitucional han denominado este derecho como «libertad informática»[4].

Por otro lado, la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre ha sido objeto de desarrollo reglamentario, el cual se encuentra recogido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[5]. Este reglamen-

---

2 Para un análisis de esta ley, donde se anticipa problemas con difícil solución con esta normativa, como los relacionados con la informática, *vid*. Murillo de la Cueva (1993).

3 Para un estudio detallado de esta norma, *vid*. Aparicio Salom (2009), Lesmes Serrano (2008) y Vizcaíno Calderón (2001), entre otros.

4 *Vid*. SSTC 143/1994, de 9 de mayo; 11/1998, de 13 de enero; 94/1998, de 4 de mayo, o 202/1999, de 8 de noviembre, entre otras.

5 No obstante, como puede apreciarse, este desarrollo reglamentario tardó en llegar, a pesar de que la Ley Orgánica de Protección de Datos preveía la necesidad del mismo. Así, ante la necesidad de este desarrollo reglamentario, para el que se habilitaba al Gobierno en la disposición final primera, pero que se demoró ocho años, y para evitar un vacío normativo, la disposición transitoria tercera de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, con el título «subsistencia de normas preexistentes», dispuso: «Hasta tanto se lleven a efecto las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente ley».

to también ha planteado dificultades en cuanto a su interpretación e, incluso, ha sido objeto de impugnación ante el Tribunal Supremo[6] aunque la mayoría de su contenido se mantuvo.

Igualmente, a nivel internacional, los derechos derivados del tratamiento de datos de carácter personal se han regulado desde el ámbito del derecho convencional internacional sobre derechos humanos. Así, encontramos el Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Entre las características más importantes de este convenio, puede destacarse su artículo 5 donde se establece que los datos de carácter personal que fueran objeto de tratamiento automatizado deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado, exactos y si fuera necesario puestos al día; así como su artículo 8 donde se recoge como derechos de cualquier persona, entre otros, la comunicación al interesado de los datos personales que consten en el fichero en forma inteligible, y obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de, entre otros, los principios de adecuación, pertinencia, proporcionalidad y exactitud referidos en el artículo 5 del convenio[7].

No obstante lo anterior, la mayor regulación sobre el tratamiento de datos de carácter personal se debe al trabajo realizado desde la Unión Europea. En este sentido, destaca la Directiva 1995/46/CE, de 24 octubre del Parlamento Europeo y del Consejo de la Unión Europea, de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[8]. Dicha directiva supuso un gran cambio para la legislación de los Estados miembros y muestra de ello fue que, en lo que respecta a España, conllevó que la referida Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal quedara obsoleta en su contenido y fuera necesaria la aprobación de la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual sigue en gran medida las líneas de esta directiva.

3. El Reglamento UE 2016/679. Síntesis de su contenido y principales novedades

Hasta este punto, encontraríamos el marco normativo vigente hasta el 25 de mayo de 2018. Sin embargo, dada su importancia merece mención separada el cambio que se ha experimentado a raíz de la mencionada fecha, motivado por la entrada en vigor del Reglamento UE 2016/679.

---

6 Sobre dicha impugnación, *vid*. STS de 15 de julio de 2010 (rec. núm. 23/2008).

7 Para un análisis detallado de la relación entre la protección de datos y las actividades del Consejo de Europa encaminadas a este fin, *vid*. Garzón Clariana (1981, pp. 9-25).

8 Diario Oficial de la Unión Europea, serie L número 281, de 23 de noviembre.

Con prioridad a entrar en un análisis sintético y que resalte las principales novedades y repercusiones de este reglamento (pues, de lo contrario, se excedería con creces los fines y límites del presente trabajo), resulta conveniente examinar los antecedentes de esta norma de la Unión Europea. De este modo, remontándonos brevemente a sus antecedentes, el 6 de abril de 2016, la Unión Europea acordó una importante modificación de su marco de protección de datos, mediante la adopción del conjunto de reformas de la protección de datos, donde se incluye el aludido Reglamento general de protección de datos 2016/679, que sustituirá a la antes mencionada Directiva 1995/46/CE, de 24 octubre del Parlamento Europeo y del Consejo de la Unión Europea, la cual, a pesar de llevar vigente desde hace más de veinte años, supuso una revolución que redundó en beneficio de los derechos de las personas físicas, el tratamiento de sus datos personales y las garantía en cuanto a su tratamiento y circulación. Posteriormente, en enero de 2017, la Comisión de la Unión Europea propuso armonizar las normas sobre las comunicaciones electrónicas (privacidad electrónica) a las nuevas normas mundiales del Reglamento general de protección de datos 2016/679. Así las cosas, en septiembre de 2017, la Comisión Europea propuso un nuevo conjunto de normas para regular la libre circulación de datos no personales en la Unión Europea. Sin embargo, este «paquete» de propuestas ya no están incluidas dentro del contenido normativo del Reglamento UE 2016/679, pues el mismo se limita a los datos personales, mientras que esta nueva propuesta de la Comisión de la Unión Europea abarca nuevas medidas que permitirán el almacenamiento y tratamiento de datos no personales en toda la Unión a fin de impulsar la competitividad de las empresas europeas y modernizar los servicios públicos. Por tanto, incluso antes de la entrada en vigor del Reglamento UE 2016/679, la Unión Europea ya vislumbraba otras dificultades que deben ser atajadas desde el ámbito normativo. Sin embargo, su aprobación final estará por ver y dependerá del Parlamento Europeo y los Estados miembros.

Entrando ya en el contenido, novedades y repercusiones del Reglamento UE 2016/679, debe destacarse, en primer lugar, que el mismo configura el derecho a la protección de datos como un compendio de facultades, regulándose detalladamente los derechos de transparencia (artículo 12), información (artículos 13 a 14), acceso (artículo 15), rectificación (artículo 16), supresión o el llamado «derecho al olvido» (artículo 17), limitación del tratamiento (artículo 18), portabilidad de datos (artículo 20) y oposición (artículo 21), etc. Igualmente, personalmente considero que debe ensalzarse la forma elegida por el legislador de la Unión Europea a la hora de aprobar esta norma. Así, estamos ante un reglamento con eficacia directa y que no requiere de transposición por ninguno de los Estados miembros para su aplicación en toda la Unión Europea. Esta característica ya lo distancia de la anterior Directiva 1995/46, de 24 octubre, del Parlamento Europeo y del Consejo de la Unión Europea, de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la cual no tenía eficacia directa y obligaba a los Estados miembros a la transposición en su legislación interna.

Por otro lado, en cuanto al ámbito de aplicación territorial, el artículo 3.2 del Reglamento UE 2016/679 introduce una importante novedad en relación con el régimen jurídico vigente, recogido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Ca-

rácter Personal, ampliando el ámbito territorial de dicho reglamento a todo responsable o encargado no establecido en la Unión cuando las actividades relacionadas con el tratamiento consistan en la oferta de bienes o servicios a ciudadanos europeos o bien si controlan el comportamiento de los mismos, por ejemplo, haciendo perfilado de usuarios. Entre los argumentos apuntados en los considerandos del Reglamento UE 2016/679 para justificar la ampliación del ámbito territorial, está la garantía de que los ciudadanos europeos no se vean privados de su derecho fundamental a la protección de datos por el mero hecho de que el encargado o responsable resida fuera de la Unión. A efectos prácticos, debe resaltarse que este cambio legislativo conlleva repercusiones fundamentalmente respecto de las grandes empresas multinacionales tecnológicas con domicilio social en Estados Unidos, quienes hasta la entrada en vigor del Reglamento UE 2016/679 aprovechaban para alimentar sus bases de datos, ya sean redes sociales, servicios de *email* gratuito y análogos, con aquellos datos de ciudadanos de la Unión Europea, todo lo cual, acarreaba in riesgo inherente puesto que Estados Unidos no cuenta con el estándar de protección en materia de datos personales equiparable al existente en la Unión Europea[9], incluso a la vista de la ya tradicional Directiva 1995/46/CE. Por ello, desde el 25 de mayo de 2018, toda empresa radicada en cualquier parte del mundo que cumpla con los requisitos del artículo 3.2 del Reglamento UE 2016/679 estará sujeta, en los mismos términos que una empresa radicada en la Unión Europea, a las obligaciones contenidas en el referenciado reglamento. Por tanto, resulta clara la intención del legislador comunitario de establecer un marco de competencia territorial lo más amplio posible. Máxime cuando el propio reglamento, a un mes de entrar en vigor, fue objeto de una corrección de errores, que, en lo que aquí se refiere, conllevaba un efecto más allá de una simple corrección, dado que extendía aún más su aplicación territorial. De tal modo, en función de esta corrección de errores, el artículo 3, apartado 2, ha pasado de establecer que «2. El presente Reglamento se aplica al tratamiento de datos personales de interesados *que residan* en la Unión», a establecer que «2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión»[10].

Asimismo, debe destacarse el deber de transparencia que fija el Reglamento UE 2016/679 en materias tales como obtención del consentimiento, deber de información y nuevos derechos que reconoce a los ciudadanos. En cuanto al consentimiento, la obtención del mismo se articula de una manera más formal de lo que se exige con base en la regulación anterior

---

9 En relación con ello, debe destacarse la diferente concepción que existe entre Estados Unidos y la Unión Europea en cuanto al alcance, extensión, límites, etc., del derecho a la privacidad. Al efecto, *vid*. Méndez (2010, pp. 617- 645).

10 Artículo 3.2 del Reglamento UE 2016/679: «El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentre en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión».

al Reglamento. Así, hasta la plena aplicación del Reglamento UE 2016/679 (es decir, hasta el 25 de mayo de 2018) eran válidos los consentimientos obtenidos mediante la mera inacción del usuario, el uso de casillas pre-marcadas y demás subterfugios para evitar el conocimiento total por parte del titular del dato. Sin embargo, a raíz del Reglamento UE 2016/679, se exige mayor transparencia y este requisito requiere que el responsable demuestre que obtuvo el consentimiento por parte del usuario de una manera libre, mediante una acción proactiva y concreta para cada una de las finalidades del tratamiento, tal y como estipula su artículo 7. Unido a este deber de transparencia y en orden a su efectivo cumplimiento en la obtención del consentimiento, que ya deberá ser siempre expreso y negándose toda forma tácita del mismo, se refuerzan los requisitos de información. Como novedad, el responsable de la base de datos de carácter personal deberá informar sobre determinados extremos con antelación a la obtención del consentimiento, entre los que cabe destacar: los datos del delegado de protección de datos (a quien, por su importancia, se le dedicará un apartado expreso en líneas posteriores), la intención de transferir sus datos a terceros Estados, el plazo de retención de los datos, información sobre cómo ejercer los nuevos derechos que otorga el Reglamento UE 2016/679 al interesado o información relativa al derecho a presentar una reclamación ante una autoridad de control (como sería la Agencia Española de Protección de Datos de Carácter Personal).

Igualmente, es de destacar la regulación expresa de lo que hasta este momento se denominaba como «derecho al olvido», aunque no se trataba de un derecho recogido expresamente en la legislación sobre protección de datos personales ya fuera a nivel nacional o de la Unión Europea, sino que era un derecho que se había configurado gracias al desarrollo jurisprudencial de los tribunales[11]. Debe apuntarse que en el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal no se recoge este derecho como tal y con esta denominación (al menos, en el momento de redactar estas líneas). Sin embargo, el Reglamento UE 2016/679 estipula en su artículo 17 el llamado «derecho al olvido», el cual también denomina como derecho de supresión, estableciendo una serie de requisitos conforme a los cuales, a partir de su entrada en vigor, los particulares encuentran una base normativa para ejercer este derecho sin tener que recurrir a interpretaciones judiciales que, si bien deben ser valoradas, no alcanzan el nivel de seguridad jurídica de contar con una cobertura legal al respecto. Y de igual modo, resulta relevante la introducción del llamado derecho a la portabilidad de los datos, regulado en el artículo 20 del Reglamento UE 2016/679, el cual, en síntesis, conlleva que el interesado pueda solicitar al responsable todos los datos perso-

[11] Derecho que, además, encuentra su inicio jurisprudencial en el ámbito de la Unión Europea, concretamente en el conocido como «caso Google», resuelto a través de la STJUE de 13 de mayo de 2014, Caso Google Spain SL contra Agencia Española de Protección de Datos (AEPD) (TCE\2014\85). No obstante, en España también encontramos sentencias del Tribunal Supremo que reconocieron y desarrollaron este derecho en su momento. Al efecto, *vid.* STS 545/2015, de 15 de octubre (Id Cendoj: 28079119912015100034, ponente: Rafael Sarazá Jimena), la cual delimita el alcance del derecho al olvido diferenciando, al respecto, entre el ámbito de los buscadores de internet más populares de los buscadores internos con los que pueden contar páginas web como los diarios digitales.

nales que le incumban en un formato estructurado e incluso poder solicitar que transmita esos datos a otro responsable. De este modo, puede decirse que el derecho a la portabilidad de los datos dispone de una doble vertiente: por un lado, el derecho que tiene el titular a obtener una copia de sus datos personales en un formato electrónico estructurado y de uso común y; por otro lado, el derecho que tiene el interesado a transmitir los datos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.

Por último, y dado que resulta inviable abordar todas las materias contenidas en el Reglamento UE 2016/679, resaltar el régimen sancionador, donde también encontramos importantes novedades. Así, el capítulo VIII del Reglamento relativo a los «Recursos, responsabilidad y sanciones» recoge, en sus artículos del 78 al 89 uno de los cambios con más repercusión a estos efectos, de manera que el importe de las sanciones a empresas, Administraciones y otros entes se eleva de forma exponencial, llegando a alcanzar un importe equivalente al mayor entre 20 millones de euros o el 4 % de su facturación anual global.

4. La repercusión del «principio de responsabilidad proactiva» o «principio de *accountability*»

Como consecuencia de su impacto y trascendencia en el cambio del modelo de protección de datos de carácter personal realizado en virtud del Reglamento UE 2016/679, merece mención separada el llamado «principio de responsabilidad proactiva» o «principio de *accountability*» (como es conocido en el ámbito anglosajón). Con carácter meramente introductorio debe apuntarse que existe un cambio respecto de la legislación anterior al 25 de mayo de 2018, la cual puede calificarse como reactiva, en lo que se refiere a la protección de datos personales, hacia un modelo sustentado en el Reglamento UE 2016/679 que viene a exigir una responsabilidad proactiva por parte de los responsables de tratamientos de datos personales. Esta novedad constituye la respuesta que el reglamento da a la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que pivota sobre el principio de responsabilidad proactiva, lo que exige una previa valoración por el responsable o por el encargado respecto del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan. Igualmente, como se podrá comprobar *ut infra*, el principio de responsabilidad proactiva está íntimamente ligado con la nueva figura del delegado de protección de datos creada en virtud de los artículos 37 y siguientes del Reglamento UE 2016/679.

Así las cosas, el Reglamento UE 2016/679 fija el principio de la responsabilidad proactiva del responsable del tratamiento de los datos personales en la elección de proveedores con los que trabaja, de modo que sobre él pesa el deber de asegurarse que aquellos cumplen con la normativa europea de protección de datos en relación con la implantación de medidas técnicas y organizativas apropiadas, en orden a garantizar un nivel adecuado de protección en consonancia al riesgo que suponga el tratamiento de los datos personales.

Por tanto, ya no estamos ante un principio de responsabilidad reactiva, en virtud del cual se actúa una vez se detecta un fallo en la protección de datos, sino que desde el 25 de mayo de 2018 ello ya no resulta suficiente, puesto que se debe poder demostrar que el tratamiento de los datos de carácter personal resulta conforme con las disposiciones del Reglamento UE 2016/679 y, además, se ha de estar en disposición de acreditarlo ante cualquier requerimiento de las autoridades competentes en materia de protección de datos personales.

No obstante lo anterior, debe apuntarse que, aunque el Reglamento UE 2016/679 introduce este cambio en la concepción de la protección de datos a nivel europeo, el principio de responsabilidad proactiva (también conocido como «principio de *accountability*») ya se venía gestando tiempo atrás. De esta manera, este principio ya fue introducido en 1980 por la OCDE (Organización para la Cooperación y el Desarrollo Económico) en sus Códigos de Conducta o Guías de Protección de la Privacidad y Flujo Transfronterizo de Datos Personales. Igualmente, ya se configuró este principio en el año 2010 gracias al grupo de trabajo del artículo 29 de la Directiva 95/46/CE (también conocido como «GT29») a través de la opinión 3/2010 sobre el principio de la responsabilidad proactiva o «principio de *accountability*». En este informe el referido grupo de trabajo presentó una propuesta concreta para introducir el principio de responsabilidad proactiva en la normativa de protección de datos, de tal forma que los responsables del tratamiento llevaran a cabo procedimientos y medidas eficaces con el objetivo de garantizar el cumplimiento de los principios y obligaciones establecidos en la Directiva 95/46/CE, con la finalidad última de poder demostrar ante las autoridades el cumplimiento de la misma. Además, estas recomendaciones tuvieron su acogida en algunos de los Estados miembros de la Unión, como demuestra el hecho de que las mismas fueron llevadas a la práctica por la Autoridad de Control Francesa (CNIL), organismo que aprobó, en enero de 2015, una norma de cumplimiento en materia de protección de datos[12].

Por otro lado, se ha señalado anteriormente que el principio de responsabilidad proactiva también es denominado como «principio de *accountability*». Sin embargo, aludir a este último concepto puede entrañar mayores dificultades en su concepción. Ello obedece al hecho de que existe un concepto asociado con esta última denominación como es la rendición de cuentas, lo cual se utiliza como sinónimo de responsabilidad, es decir, de dar cuenta, responder por, dar cumplimiento, fundamentalmente a nivel de gestión pública. En este sentido, existen autores como Ebrahim (2010, p. 27) que entienden el concepto de rendición de cuen-

[12] La norma francesa define las reglas y las mejores prácticas que debe implantar y desarrollar una organización para garantizar una gestión respetuosa con los principios de protección de datos. La norma se divide en 25 apartados o requisitos relativos, entre otras cuestiones, a la existencia de políticas de privacidad internas y externas, el nombramiento de un responsable de protección de datos, la gestión de las incidencias y siniestros, etc. Con ello, la CNIL introdujo en su normativa de protección de datos, con prioridad al Reglamento UE 2016/679, el principio de responsabilidad proactiva, de tal forma que aquellas organizaciones que demostraran que cumplían con dicha norma de cumplimiento obtendrían un «sello de cumplimiento» del principio de responsabilidad proactiva emitido por la CNIL, garantizando el cumplimiento de la normativa francesa de protección de datos.

tas como la responsabilidad de responder por un desempeño particular ante las expectativas de distintas audiencias o partes interesadas. No obstante, en España esta diferente nomenclatura no conlleva mayores dificultades que el denominado principio de responsabilidad proactiva. Así lo demuestra Núñez García (28 de enero de 2014), quien se expresa señalando que en la práctica, y desde el punto de vista de la privacidad, la «accountability» tendría dos grandes vertientes: por un lado, la implementación de una cultura de respeto a este derecho fundamental en el seno de la organización, acompañada del establecimiento de todo tipo de garantías para preservar los principios y obligaciones que del mismo se derivan; por el otro, el compromiso de ser transparente en las actuaciones diarias, generando mecanismos que permitan calibrar y controlar hasta qué punto las garantías anteriores funcionan correctamente y poniéndolos a disposición de las autoridades en caso de que estas así lo requieran.

En definitiva, considero que no debe caerse en posibles interpretaciones que tergiversen y dificulten unos principios que pretenden alcanzar un cambio claro en materia de protección de datos y que se logre una mayor protección para el particular. Por tanto, desde mi punto de vista, el principio de responsabilidad proactiva y el también denominado «principio de *accountability*» responden a un fin último, como es que el encargado y responsable del tratamiento de datos personales adopte con prioridad todas las medidas necesarias y legalmente exigibles de cara a su protección, así como al hecho ya apuntado en 2010 por el grupo de trabajo del artículo 29 de la Directiva 95/46/CE, en cuanto al deber de poder demostrar ante las autoridades competentes el cumplimiento de la normativa sobre protección de datos de carácter personal.

5. La introducción del «delegado de protección de datos». Una figura todavía por experimentar

Como se ha indicado anteriormente, mención especial separada merece el análisis de la introducción por el Reglamento UE 2016/679 de una nueva figura en sus artículos 37 y siguientes, como es el «delegado de protección de datos», también conocido por su nomenclatura inglesa como «*data protection officer*» (DPO). Al respecto, la Comisión Europea, en su documento de trabajo sobre la evaluación de impacto relativo a la propuesta de reglamento, define al delegado de protección de datos como «una persona responsable en el seno de un responsable o un encargado del tratamiento para supervisar y monitorear de una forma independiente la aplicación interna y el respeto de las normas sobre protección de datos. El DPO puede ser tanto un empleado como un consultor externo»[13]. Sin embargo, a pesar de esta definición, incluso dentro de la Unión Europea, la configuración en toda su extensión de esta figura está todavía por desarrollar y muestra de ello es que el grupo de

[13] Comisión Europea, Commission Staff Working Paper, Impact Assessment, SEC (2012) 72 final, Brussels, 25 de enero de 2012. Recuperado de <http://eur-lex.europa.eu>.

trabajo del artículo 29 de la Directiva 95/46/CE (conocido como «GT29») decidió dedicarle una de sus primeras directrices sobre dicha norma, que sirven, entre otros objetivos, para contar con elementos interpretativos de algunos aspectos de su articulado[14].

Adentrándonos en lo estipulado por el Reglamento UE 2016/679, en primer lugar debe señalarse que se trata de una figura que resulta de obligada creación por parte de las empresas en determinados supuestos recogidos en su artículo 37. De tal modo, como previene el apartado 1 del artículo 37, el responsable y el encargado del tratamiento deberán designar un delegado de protección de datos en tres supuestos:

1. En los casos donde el tratamiento lo lleve a cabo una autoridad u organismo público[15], excepto los tribunales que actúen en ejercicio de su función judicial.
2. Si las actividades principales del responsable o del encargado consisten en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran una observación habitual y sistemática de interesados a gran escala, y, por último,
3. Siempre que las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10 del Reglamento UE 2016/679.

Sin embargo, en el resto de supuestos se trata de una figura de creación opcional aunque puede anticiparse que en empresas con cierto volumen en la gestión de datos personales resultará conveniente, e incluso necesario, en la práctica, contar con un delegado de protección de datos. Así lo dispone el apartado 4 del artículo 37 del Reglamento UE 2016/679 al estipular que:

> En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección

[14] En concreto, el 13 de diciembre de 2016, el GT29 adoptó las directrices sobre los delegados de protección de datos (Guidelines on Data Protection Officers, WP 243). Recuperado de <http://ec.europa.eu>. Igualmente, publicó un anexo con preguntas frecuentes. Consultado en: <http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf>. Para un análisis de estas directrices, *vid*. Recio Gayo (12 de enero de 2017).

[15] La introducción obligatoria de esta figura en el ámbito público debería conllevar un mayor compromiso en la protección de datos personales por los entes públicos y, especialmente, un incremento en la eficacia y el contacto con el particular, pues el delegado de protección de datos debe servir como canal de comunicación para aquellos conflictos donde esté implicado cualquier organismo público. Para un análisis de la repercusión de la legislación sobre protección de datos en el funcionamiento de las Administraciones públicas, *vid*. Troncoso Reigada (2006).

de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

Ahora bien, las legislaciones nacionales pueden ampliar el número de supuestos donde se exige la creación de un delegado de protección de datos, lo cual ocurre en el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, cuyo artículo 34 realiza una remisión expresa a los supuestos contemplados ya en el Reglamento UE 2016/679 pero, adicionalmente, enumera otra serie de supuestos donde se requiere esta figura[16], incluyendo, por ejemplo, en su apartado j), a los ficheros de solvencia patrimonial, los cuales son objeto de análisis *ut infra* junto a su responsabilidad civil.

En cuanto a las funciones del delegado de protección de datos, estas vienen enumeradas en el artículo 39 del Reglamento UE 2016/679 y entre ellas destacan: informar de las obligaciones que tienen responsables y encargados; supervisar el cumplimiento del reglamento y formar al personal de la compañía; asesorar y revisar las evaluaciones de impacto; cooperar con la autoridad de control y actuar como punto de contacto para que cualquier particular le pueda consultar cuestiones relativas a un tratamiento o frente a la

---

[16] Artículo 34 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal: *Designación de un delegado de protección de datos.*

> 1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate delas siguientes entidades:
>
> a) Los colegios profesionales y sus consejos generales, regulados por la Ley 2/1974, de 13 febrero, sobre colegios profesionales.
>
> b) Los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006, de 3 de mayo, de Educación, y las Universidades públicas y privadas.
>
> c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en la Ley 9/2014, de 9 de mayo, General de telecomunicaciones, cuando traten habitual y sistemáticamente datos personales a gran escala.
>
> d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
>
> e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
>
> f) Los establecimientos financieros de crédito regulados por Título II de la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial.
>
> g) Las entidades aseguradoras y reaseguradoras sometidas a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
>
> h) Las empresas de servicios de inversión, reguladas por el Título V del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.
>
> i) Los distribuidores y comercializadores de energía eléctrica, conforme a lo dispuesto en la Ley 24/2013, de 26 de diciembre, del sector eléctrico, y los distribuidores y comercializadores de gas natural, conforme a la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

autoridad de control. Un aspecto determinante en esta figura radica en el hecho de que expresamente se le otorga una plena independencia, la cual debe ser garantizada y respetada por la entidad para la cual trabaje, tal y como estipula el artículo 38.3 del Reglamento UE 2016/679[17]. Igualmente, en virtud del artículo 37.6 del Reglamento UE 2016/679[18], el delegado de protección de datos puede ser un profesional externo o interno a la entidad para la que trabaje.

Por otro lado, uno de los mayores problemas que puede acarrear es la formación del delegado de protección de datos. Ello, entre otras cuestiones, debido al amplio elenco de facultades que se le pueden encomendar y porque de las mismas pueden derivarse responsabilidades tanto en el ámbito administrativo sancionador como en el ámbito de la responsabilidad civil. En este sentido, el Reglamento UE 2016/679 no resulta exhaustivo y no especifica requisitos en cuanto a su formación, señalando únicamente su artículo 37.5 que:

> El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

---

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por el artículo 32 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a lo dispuesto en la Ley 3/2011, de 27 de mayo, de regulación del juego.

ñ) Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

[17] Artículo 38.3 del Reglamento UE 2016/679: «El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado».

[18] Artículo 37.6 del Reglamento UE 2016/679: «El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios».

En definitiva, la creación de la figura del delegado de protección de datos debe valorarse positivamente, pero su desarrollo en la práctica debe hacerse con cautelas, dado que es una figura que puede disponer de numerosas facultades y, por ende, adquirir grandes dosis de responsabilidad en la entidad para la que trabaje. Todo ello teniendo en consideración que no existe requisito formativo en el Reglamento UE 2016/679, de manera que sería una buena opción que, ante este silencio, el legislador español, aprovechando la tramitación del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, complementara esta laguna del reglamento. Además, debe resaltarse que el propio proyecto ya complementa alguna de las funciones del delegado de protección de datos, como es el hecho de que su artículo 65.4[19], en orden a promover la resolución amistosa de conflictos y reclamaciones de particulares, permite la posibilidad de que el delegado de protección de datos pueda resolver algunas de estas reclamaciones, a pesar de que no se limita el derecho a acudir a la autoridad competente, como sería, en el ámbito estatal, la Agencia Española de Protección de Datos de Carácter Personal[20]. Por tanto, si el legislador español introduce esta novedad, también puede aprovechar la ocasión para regular los requisitos formativos que deben exigirse a quien pretenda ejercer las funciones y responsabilidades del delegado de protección de datos.

6. Especial referencia a la responsabilidad civil en el tratamiento de ficheros de solvencia patrimonial

6.1. Ficheros con carácter estrictamente económico. Los llamados «registros de morosos»

La responsabilidad civil que puede surgir en el tratamiento de datos personales es una materia que puede dar lugar a numerosos supuestos que exceden con creces los límites y pretensiones del presente estudio. No obstante, el trabajo pretende dar un enfoque y especial análisis en uno de los casos que más repercusión puede tener en los particulares. Se trata de los ficheros de solvencia patrimonial. De tal modo, la repercusión en el parti-

[19] Artículo 65.4 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal: «Cuando las reclamaciones no se hayan formulado previamente ante el delegado de protección de datos designado por el encargado o responsable del tratamiento o ante el organismo de supervisión establecido para la aplicación de los códigos de conducta, la Agencia podrá remitírselas, antes de resolver sobre la admisión a trámite, a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica».

[20] Debe apuntarse que la Agencia Española de Protección de Datos de Carácter Personal es la principal y más conocida autoridad a estos efectos y que, como se ha señalado anteriormente, uno de las funciones clave del delegado de protección de datos es servir de enlace entre la entidad de tratamiento de datos personales y las autoridades en la materia. Sin embargo, y al margen de discusiones competenciales, han proliferado autoridades de control en materia de control de datos a nivel autonómico. Para un análisis detallado de la cuestión y el problema competencial generado, *vid*. López Román y Mora Sanguinetti (2009).

cular en cuanto al tratamiento de sus datos personales en este tipo de ficheros cobra gran importancia no solo porque estén proliferando, pues permiten obtener y almacenar datos sobre la economía de los particulares, sino también por el efecto negativo que puede generar en estos particulares, quienes vean que tras su inclusión en estos ficheros, se les niega cualquier tipo de concesión de crédito u otro tipo de negocio jurídico donde se valore su capacidad y solvencia económica.

Así las cosas, por su importancia, la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre dedica a los ficheros de solvencia patrimonial un tratamiento específico. Anteriormente a la entrada en vigor de la referida ley orgánica, el tratamiento de datos personales destinado o realizado con ocasión de la prestación de servicios de información sobre solvencia patrimonial y crédito se regulaban en el artículo 28 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[21], el cual fue objeto de desarrollo por la Instrucción 1/1995, de 1 de marzo, sobre prestación de servicios de información sobre solvencia patrimonial y crédito, y la norma cuarta de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso y rectificación, ambas dictadas por la Agencia Española de Protección de Datos. No obstante, la regulación vigente sobre la materia se encuentra en el artículo 29 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, bajo el título «prestación de servicios de información sobre solvencia patrimonial y crédito»[22]:

---

[21] Artículo 28 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal: *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

> 1. Quienes se dediquen a la prestación de servicios de información sobre solvencia patrimonial y el crédito solo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Podrán tratarse, igualmente, datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los afectados respecto de los que hayan registrado datos de carácter personal en ficheros automatizados, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.
>
> 2. Cuando el afectado lo solicite, el responsable del fichero le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección del cesionario.
>
> 3. Solo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando sean adversos, a más de seis años.

[22] Artículo 29 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre:

> 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito solo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

Ahora bien, como puede apreciarse a la luz del citado artículo, los tipos de registros que se regulan no se reducen a aquellos con carácter estrictamente económico o, más concretamente y en lo que interesa en este trabajo, a los llamados registros de morosos. Es por ello que la Sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo), de 15 de julio de 2010 (rec. núm. 23/2008) afirma, en referencia al citado artículo 29, que:

> La lectura de dichos apartados permite concluir, en una interpretación lógico-sistemática de los mismos, que el apartado 1 se está refiriendo a los ficheros positivos o de solvencia patrimonial, exigiéndose para el tratamiento de los datos su obtención de los registros y fuentes accesibles al público o de las informaciones facilitadas por el propio interesado o con su consentimiento y que el apartado 2 hace mención a los ficheros negativos o de incumplimiento, como sin dificultad se infiere, pese a la referencia al «cumplimiento o incumplimiento de las obligaciones».

De este modo, los denominados registros de morosos se encuadrarían dentro del apartado 2 del artículo 29 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre.

Sentado lo anterior, como resulta de la lectura del artículo 29.2, los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias a que alude son aquellos facilitados a las empresas que prestan servicios de información sobre incumplimiento de obligaciones dinerarias por el acreedor o por quien actúe por su cuenta o interés. Debe puntualizarse que, como regla general, no se trata de datos obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento. De este modo, tal y como aclaraba la Instrucción 1/1995 de la Agencia Española de Protección de Datos, en estos supuestos coexisten dos tipos de ficheros conectados entre sí. Primero: el propio de los acreedores, que se compone de los datos personales que son consecuencia de las relaciones económicas mantenidas con los afectados y cuya única finalidad es obtener la satisfacción de la obligación dineraria. Segundo: otro tipo de fichero, que se podría denominar común, el cual, consolidando todos los datos personales contenidos en los ficheros de los acreedores, tiene por finalidad proporcionar información sobre la solvencia de una persona determinada.

> 2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

6.2. Ficheros con carácter económico indirecto. Especial referencia al fichero de la Central de Riesgos del Banco de España

Respecto de este tipo de ficheros debe aclararse que, si bien pueden tener un carácter económico, el mismo no es tan directo como aquel que existe en los regulados a través del artículo 29.2 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre. Es decir, no estamos únicamente ante el tratamiento de datos personales relativos al cumplimiento o incumplimiento de obligaciones dinerarias. No obstante, sus datos pueden tener una relevante trascendencia económica en el interesado y también pueden, por tanto, irrogarse perjuicios al mismo por su inclusión errónea.

Dentro de este tipo de ficheros, como consecuencia de su repercusión en el tráfico económico, destacaría el llamado «fichero de la Central de Riesgos del Banco de España» (CIRBE). Este fichero y otros de naturaleza semejante encuentran su regulación en los artículo 59 y siguientes de la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero. Sin embargo, el análisis exhaustivo de lo que el artículo 59 de la Ley 44/2002 denomina como «Central de Riesgos» excede de los límites de este estudio. No obstante, en referencia al CIRBE puede decirse, de manera sintética, que, como expone la Sentencia del Tribunal Supremo 586/2017, de 2 de noviembre, estamos ante un servicio público cuya finalidad radica en recabar de las entidades de crédito y otras entidades financieras datos e informaciones sobre los riesgos de crédito derivados de contratos tales como préstamos, créditos, descuentos, emisiones de valores, contratos de garantía, compromisos relativos a instrumentos financieros, o cualquier otro tipo de negocio jurídico propio de su actividad financiera, para facilitar a las entidades declarantes datos necesarios para el ejercicio de su actividad, permitir a las autoridades competentes para la supervisión prudencial de dichas entidades el adecuado ejercicio de sus competencias de supervisión e inspección y contribuir al correcto desarrollo de las restantes funciones que el Banco de España tiene legalmente atribuidas. Con este objetivo, este tipo de entidades financieras o de crédito deben enviar con carácter periódico al CIRBE los datos sobre las operaciones de esa naturaleza que concierten y las personas que directa o indirectamente resulten obligadas en ellas. Igualmente, comunicarán los datos que reflejen una situación de incumplimiento de las obligaciones de la otra parte frente a la entidad financiera o de crédito declarante correspondiente.

Por otro lado, las entidades que han asumido las obligaciones referenciadas con el Banco de España disponen del derecho a obtener informes sobre los riesgos de las personas físicas o jurídicas registradas en el fichero de CIRBE siempre que tales personas mantengan con la entidad respectiva algún tipo de riesgo, hayan solicitado a la entidad un préstamo u otra operación de riesgo o, por último, figuren como obligadas al pago o garantes en documentos cambiarios o de crédito cuya adquisición o negociación haya sido solicitada a la entidad.

De tal modo, a la vista de lo expuesto puede concluirse que el CIRBE no es un fichero de solvencia patrimonial de los recogidos en el artículo 29.2 de la Ley Orgánica de Protección de Datos, esto es, no se configura como uno de los llamados «ficheros de morosos» o «registro de morosos»[23], pues su finalidad no es recoger datos de carácter personal relativos al incumplimiento de obligaciones dinerarias facilitados por el acreedor. Al contrario, se trata de un fichero administrativo específico destinado a informar sobre los riesgos de crédito derivados de contratos propios de la actividad financiera. Debe apuntarse que puede contener informaciones sobre la existencia de incumplimientos de obligaciones dinerarias en los casos que estas hayan podido producirse, pero no se trata de su finalidad última ni única. En consecuencia, los datos de una persona que se incluyan en el CIRBE no necesariamente deben estar vinculados con informaciones sobre incumplimientos de obligaciones dinerarias, sino que puede ser con motivo de que tal persona figure como prestataria, fiadora o avalista, tal y como ocurre en el caso resuelto en la aludida Sentencia del Tribunal Supremo 586/2017, de 2 de noviembre.

7. La dificultad de cuantificar el daño y la reciente Sentencia del Tribunal Supremo 261/2017, de 26 de abril: La escasa cuantía de la deuda incluida no es causa de reducción de responsabilidad civil

7.1. La dificultad de cuantificar el daño

Previamente a entrar a analizar los puntos más controvertidos sobre la cuantificación del daño por inclusión indebida de datos personales en registros de morosos, debe analizarse cuál es el horizonte que se nos presenta en la difícil tarea de cuantificar el daño en este tipo de casos. En esta línea debe hacerse una matización que puede parecer obvia pero es importante destacar, la cual consiste en que, a pesar de la importancia de la Agencia Española de Protección de Datos a la hora de proteger a los particulares y el correcto uso de sus datos personales, su ámbito de acción se circunscribe, entre otros, al aspecto sancionador, pero no dispone de algún tipo de función similar a la jurisdiccional que permita a este organismo resolver controversias sobre reclamación de daños y perjuicios por la errónea inclusión en ficheros de solvencia patrimonial. En otras palabras, tal y como puso de manifiesto la Sentencia de la Audiencia Nacional de 8 de marzo de 2006 (Sala 1.ª de lo Contencioso-Administrativo), la Agencia Española de Protección de Datos no es el organismo competente para decidir sobre la responsabilidad civil en que haya podido incurrir la empresa responsable del tratamiento de los datos, al igual que tampoco es competente en la resolución de estas controversias sobre daños y perjuicios

[23] Denominación, esta última, dada por la STS 284/2009, de 24 de abril.

el órgano jurisdiccional contencioso-administrativo que conozca del recurso jurisdiccional interpuesto contra cualquier resolución administrativa dictada por la Agencia Española de Protección de Datos.

Por tanto, los organismos competentes para conocer las reclamaciones de responsabilidad civil por la inclusión indebida en ficheros de morosos son los juzgados y tribunales jurisdiccionales, más concretamente, aquellos correspondientes al orden civil. Así, el orden civil será el competente para conocer aquellas controversias derivadas de aquellas inclusiones de datos en registro de solvencia patrimonial que se realicen sin respetar las exigencias legales relativas a la veracidad, exactitud, pertinencia y, en definitiva, tratamiento legal de los datos, todo lo cual implica la infracción de los derechos fundamentales del afectado. Este es el motivo por el que, como se analizará *ut infra*, serán de aplicación las reglas indemnizatorias de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Ahora bien, debe apuntarse que existe otro fundamento legal en orden a las pretensiones resarcitorias. Se trata del artículo 19 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, donde se previene la responsabilidad civil de los encargados del tratamiento de datos personales, tanto respecto de aquellos titulares de carácter privado como público[24]. Respecto de este artículo, tal y como apunta Ordóñez Solís (2011, p. 214), se puede cuestionar la procedencia en cuanto a la inclusión expresa de este tipo de derecho resarcitorio en la norma sobre protección de datos. Personalmente, creo que no debe haber duda en cuanto a su procedencia, pues no resulta ocioso incluir una referencia a la responsabilidad civil en esta norma, al margen de que pueda fundamentarse mejor las responsabilidades civiles en otro tipo de normas. Además, Aparicio Salom (2009, p. 271) señala que este tipo de cláusulas constituyen la clave de bóveda de todo el sistema español de protección de datos. Y a mayor abundamiento, en el ámbito de la Unión Europea, al antes analizado Reglamento UE 2016/679 recoge expresamente una cláusula de responsabilidad en su artículo 82.1 señalando al efecto:

> Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

---

[24] Artículo 19 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre:

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

Por tanto, todo refuerzo legal en la fundamentación de las responsabilidades civiles en el tratamiento de datos personales siempre debe tener una buena acogida pues, aunque sea en última instancia y existan normas con mejor fundamento reparador (y respecto las cuales, los tribunales sean más propensos a reconocer las demandas por daños y perjuicios), siempre resultarán de utilidad para fundar las peticiones resarcitorias de los particulares damnificados.

Así las cosas, a la vista de la interpretación del Tribunal Supremo, no se recurre ni al artículo 19 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, ni a cláusulas generales reparadoras, como el más que conocido artículo 1.902 del Código Civil[25] (o, incluso, en el ámbito de ficheros de titularidad pública, al artículo 32.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público)[26], dado que se considera más apropiado acudir al régimen especial en materia de honor, intimidad y propia imagen que contiene la Ley Orgánica 1/1982. Asimismo, ello encuentra su sentido en el hecho de que los daños generados por la vulneración en la protección de datos de particulares supondrán, en la mayoría de los casos, un quebranto del honor o intimidad, por lo que resulta lógico acudir a una norma que regula expresamente estos daños. Además, aunque siempre subsista la posibilidad de acudir al general artículo 1.902 del Código Civil y al referenciado artículo 19 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, debe recordarse el aforismo *lex specialis derogat legi generali*, lo cual reforzaría el fundamento de basar las pretensiones resarcitorias en la Ley Orgánica 1/1982.

Sentado lo anterior, resulta claro que la Ley Orgánica 1/1982 se convierte en uno de los ejes principales a la hora de cuantificar el daño en estos casos, de manera que el Tribunal Supremo ha considerado que existe una inclusión errónea de datos personales cuya indemnización debe valorarse conforme a la citada ley orgánica cuando la misma resulta indebida, por no respetarse los principios de calidad de los datos y demás requisitos exigidos por la normativa sobre ficheros de datos sobre incumplimientos de obligaciones dinerarias. Y lo más importante radica en el hecho de que, a raíz de lo anterior, se genera una intromisión ilegítima en el derecho al honor del afectado e, incluso, en un momento inicial también se consideraba vulnerado el derecho a la intimidad. Este es el caso de la Sentencia del Tribunal Supremo núm. 660/2004, de 5 de julio donde se declaró.

---

25 Artículo 1902 del Código Civil: «El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado».

26 Artículo 32.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que reproduce lo previsto en el clásico y ya derogado artículo 139.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, estipulando al efecto: «Los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos salvo en los casos de fuerza mayor o de daños que el particular tenga el deber jurídico de soportar de acuerdo con la Ley».

> En todo caso, el ataque al honor del demandante (más propiamente ataque a su intimidad personal patrimonial), lo conforma el hecho probado de la inclusión indebida en el registro de morosos, por deuda inexistente, lo que indudablemente, sobre todo tratándose de una persona no comerciante, supone desmerecimiento y descrédito en la consideración ajena (artículo 7.7.º Ley Orgánica 1/1982), pues esta clase de registros suele incluir a personas valoradas socialmente en forma negativa, o al menos con recelos y reparos, sobre todo cuando se trata de llevar a cabo relaciones contractuales con las mismas.

Sin embargo, como apunta Ortí Vallejo (1994, p. 166), el cálculo de la indemnización por daño moral es una cuestión de difícil determinación.

De este modo, la tendencia actual gira en torno a la consideración de que la inclusión indebida en registros de solvencia patrimonial genera un daño al derecho al honor del afectado, en lugar de vulnerar su derecho a la intimidad. Por tanto, la Sentencia del Tribunal Supremo núm. 212/2006, de 7 de marzo, en un supuesto de inclusión indebida en un fichero de morosos que determinó que se denegase la concesión de un préstamo, consideró que se había vulnerado el derecho al honor del afectado[27]. Y esta tendencia se consolidó en virtud de la Sentencia del Tribunal Supremo núm. 284/2009, de 24 de abril, la cual es una sentencia dictada en pleno y que sienta como doctrina jurisprudencial la consolidación respecto a que el derecho fundamental vulnerado en estos supuestos es el derecho al honor, afirmando sobre este particular:

> Esta Sala, en pleno, ha mantenido la posición de entender que la inclusión, faltando a la veracidad, por una entidad, en un registro de solvencia patrimonial –los llamados «registros de morosos»– implica un atentado al derecho del honor del interesado que ha aparecido en tal registro, erróneamente[28].

---

[27] Expresando al efecto: «No se precisa en la persona que ataca (la que comete la intromisión ilegítima) el derecho al honor, la intención –dolo o culpa– de dañar tal derecho; se trata de una responsabilidad objetiva: cuando se da la intromisión ilegítima, se presume *iuris et de iure* (art. 9.3 de la Ley Orgánica, de 5 de mayo de 1982) el perjuicio, al que corresponde la indemnización por el daño moral. La jurisprudencia ha mantenido que, si se produce un ataque al honor, no es preciso dolo o culpa en el atacante, desde las sentencias de 30 de marzo de 1988 y 16 de diciembre de 1988 hasta la más reciente de 4 de febrero de 1993 que dice, literalmente: "[...] el hecho de que el informador careciese de propósito difamatorio, al no ser precisa la existencia de una específica intención de dañar o menospreciar"».

[28] Interpretación jurisprudencial que es reiterada en la siguiente afirmación: «Esta Sala en pleno, ha resuelto como doctrina jurisprudencial que, como principio, la inclusión en un registro de morosos, erróneamente, sin que concurra veracidad, es una intromisión ilegítima en el derecho al honor, por cuanto es una imputación, la de ser moroso, que lesiona la dignidad de la persona y menoscaba su fama y atenta a su propia estimación».

Igualmente, esta sentencia es relevante dado que considera que, a la hora de que se entienda vulnerado el derecho al honor del afectado, es intrascendente que el registro que incluyó los datos vulnerando las reglas sobre protección de datos personales haya sido o no consultado por terceras personas. En consecuencia, esta interpretación lleva a concluir que no resulta preciso, en orden a que existe una intromisión ilegítima en el derecho al honor del afectado susceptible de indemnización, que haya existido una efectiva divulgación del dato.

No obstante lo anterior, debe tenerse presente que si los datos indebidamente incluidos en un fichero de morosos llegan a ser efectivamente difundidos y conocidos por terceras personas, el daño se verá agravado y, por ende, la indemnización por daños morales deberá ser superior[29]. Así, la inclusión de datos de una persona en un registro de morosos vulnerando los requisitos establecidos por la Ley Orgánica de Protección de Datos 15/1999 sería indemnizable por dos conceptos: el primero, en atención a la afectación a la dignidad en su aspecto interno o subjetivo; y el segundo, relativo al externo u objetivo, el cual tiene que ver con la consideración de las demás personas. Por tanto, es en este segundo aspecto donde la efectiva divulgación y conocimientos de terceros del dato indebidamente incluido en un fichero de solvencia patrimonial debe servir para calibrar la indemnización procedente pues, por ejemplo, no es lo mismo que solo hayan tenido conocimiento de los datos personales del perjudicado los empleados de la empresa acreedora y los de la empresa titular del registro de morosos, a que el dato haya sido comunicado a un número mayor o menor de asociados al sistema que hayan tenido acceso a dicho registro de morosos.

Por otro lado, en cuanto a la concreta cuantificación de daños y perjuicios, como se ha comprobado, deberá acudirse a las reglas establecidas en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. En este sentido, el artículo clave es el 9.3 de la referida ley orgánica, donde se establece que:

> La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido. También se valorará el beneficio que haya obtenido el causante de la lesión como consecuencia de la misma.

---

[29] Sobre esta cuestión la STS núm. 284/2009, de 24 de abril afirma: «Y es intrascendente el que el registro haya sido o no consultado por terceras personas, ya que basta la posibilidad de conocimiento por un público, sea o no restringido, y que esta falsa morosidad haya salido de la esfera interna del conocimiento de los supuestos acreedor y deudor, para pasar a ser de una proyección pública. Si, además, es conocido por terceros y ello provoca unas consecuencias económicas (como la negación de un préstamo hipotecario) o un grave perjuicio a un comerciante (como el rechazo de la línea de crédito), sería indemnizable, además del daño moral que supone la intromisión en el derecho al honor y que impone el artículo 9.3 de la mencionada Ley de 5 de mayo de 1982».

Sobre este artículo deben puntualizarse varias cuestiones, las cuales alejan las reglas indemnizatorias de aquellas otras más genéricas recogidas en el artículo 1.902 del Código Civil. En primer lugar, el artículo 9.3 establece una presunción *iuris et de iure*, es decir, que no admite prueba en contra, que conlleva el hecho de que siempre que exista intromisión ilegítima se entenderá producido un daño indemnizable. En este sentido, la Sentencia del Tribunal Supremo de 5 de junio de 2014 (rec. núm. 3303/2012) indica que dada la presunción *iuris et de iure* de existencia de perjuicio indemnizable, el hecho de que la valoración del daño moral no pueda obtenerse de una prueba objetiva no excusa ni imposibilita legalmente a los tribunales para fijar su cuantificación, manifestando que:

> A cuyo efecto ha de tenerse en cuenta y ponderar las circunstancias concurrentes en cada caso (sentencias de esta sala núm. 964/2000, de 19 de octubre, y núm. 12/2014, de 22 de enero) [y que se trata, por tanto], de una valoración estimativa, que en el caso de daños morales derivados de la vulneración de un derecho fundamental del art. 18.1 de la Constitución, ha de atender a los parámetros previstos en el art. 9.3 de la Ley Orgánica 1/1982, de acuerdo con la incidencia que en cada caso tengan las circunstancias relevantes para la aplicación de tales parámetros, utilizando criterios de prudente arbitrio.

Igualmente, la indemnización basada en el artículo 9.3 de la Ley Orgánica 1/1982 incluye criterios diversos a los tradicionales del ordenamiento jurídico español, cuyo máximo exponente es el referido artículo 1.902 del Código Civil pues, por ejemplo, a la hora de valorar el daño moral alude al grado de difusión del daño o el beneficio obtenido por el infractor. Estos son criterios que pueden conectarse con acciones diferentes, como la de enriquecimiento injusto y, especialmente, desde mi punto de vista, conlleva una especie de daños punitivos, los cuales no son admitidos por las reglas generales de responsabilidad civil españolas. De este modo, el hecho de que se incremente la indemnización sobre la base del beneficio obtenido por el infractor es un aspecto que, en principio y bajo las reglas tradicionales indemnizatorias españolas, no tiene que ver con el daño efectivo causado al perjudicado. Es decir, el daño sería el mismo con independencia de los beneficios que haya obtenido el infractor mediante dicho daño, lo cual, desde una perspectiva de la justicia conmutativa y no retributiva que existe como principio general indemnizatorio en nuestro ordenamiento jurídico, no debería ser admisible. Así, bajo estas reglas generales que entroncan el sistema indemnizatorio español, el mayor o menor provecho del infractor debería ser penalizado por las reglas a las que se somete el derecho administrativo sancionador, pero no sobre las normas relativas a responsabilidad civil. Sin embargo, el artículo 9.3 de la Ley Orgánica 1/1982 constituye una excepción a esta regla general en beneficio del perjudicado, y, desde mi punto de vista, encuentro justificada dicha excepción pues considero más justo que el posible beneficio obtenido por el infractor repercuta en positivo en la víctima en lugar de que la posible sanción administrativa acabe en las arcas del Estado.

Como se ha comprobado, existen diversos problemas y particularidades respecto al régimen general indemnizatorio español para los casos de inclusión indebida de datos personales en registros de morosos. A ello debe añadirse un aspecto novedoso, resaltado por la reciente Sentencia del Tribunal Supremo 2161/2017, de 26 de abril, el cual consiste en que la escasa cuantía por la que se incluye indebidamente el dato personal de un sujeto en un registro de morosos no es motivo suficiente como para entender que la intromisión ilegítima es de menor entidad, ni que, en consecuencia, procede minorar la cuantía indemnizatoria. En este caso, el Juzgado de Primera Instancia núm. 1 de Laviana (Sentencia núm. 117/2015, de 16 de diciembre) estimó la demanda y condenó a la empresa a lo reclamado, así como a ejecutar cuantos actos y comunicaciones fueran necesarios para excluir a la demandante del fichero, derivados de la deuda. Para el cálculo de la indemnización el juzgado atendió a la difusión e incerteza de la deuda, además de a la permanencia en el tiempo de la inclusión de los datos en el registro. Sin embargo, la indemnización concedida en primera instancia fue minorada en virtud del recurso de apelación presentado por la demanda ante la Audiencia Provincial de Oviedo (rec. núm. 190/2016, de 17 de junio), debido a que consideraba que la escasa cuantía de la deuda por la que fue indebidamente incluido el afectado en el registro de morosos era motivo suficiente (reduciéndola así a 2.000 euros).

Ahora bien, la resolución dictada en apelación fue recurrida ante el Tribunal Supremo y su Sentencia núm. 261/2017, de 26 de abril casó la Sentencia de la Audiencia Provincial de Oviedo, entendiendo que la escasa cuantía del débito por el cual se incluía a la afectada en un registro de morosos no era causa suficiente como para reducir el daño, declarando al efecto:

> No puede aceptarse (sentencia núm. 81/2015, de 18 de febrero) el argumento de que la inclusión de datos sobre una deuda de pequeña entidad en un registro de morosos no supone una intromisión ilegítima en el derecho al honor de una trascendencia considerable (y por tanto no puede dar lugar más que a una pequeña indemnización), porque claramente muestra que no responde a un problema de solvencia, sino a una actuación incorrecta del acreedor. La inclusión en registros de morosos por deudas de pequeña cuantía es correcta y congruente con la finalidad de informar sobre la insolvencia del deudor y el incumplimiento de sus obligaciones dinerarias. Y cuando tal inclusión se ha realizado, quienes consultan el registro pueden suponer legítimamente que el acreedor ha cumplido con las exigencias del principio de calidad de los datos, y no lo contrario, que es lo que hace la Audiencia, y que por tanto es cierto que el afectado ha dejado de cumplir sus obligaciones dinerarias.

Es más, incluso determinó que el hecho de que no constara que la indebida inclusión en el registro de morosos impidiera a la recurrente acceder a créditos u otros servicios financieros tampoco era motivo suficiente como entender que la intromisión ilegítima en su derecho al honor y, por ende, el daño indemnizable era de menor relevancia. Por tanto,

la Sentencia del Tribunal Supremo 261/2017, de 26 de abril considera que la reducción indemnizatoria efectuada en segunda instancia por la Audiencia Provincial era improcedente y no podía basarse en la escasa cuantía de la deuda incluida en el registro de morosos, de manera que el «daño indemnizable sufrido por la demandante se compadece más con el que cuantifica la sentencia de primera instancia que con el que fija la sentencia recurrida». Ello, además, debido a que la inclusión indebida de los datos en el registro de morosos era causa suficiente para afectar negativamente al prestigio e imagen de solvencia de la demandante, así como para impedir la obtención de financiación o la contratación de prestaciones periódicas o continuadas, a lo que debía unirse las gestiones que tuvo que realizar la afectada a fin de conseguir la cancelación de sus datos en el registro de morosos.

Por último, existe otro aspecto relevante a enfatizar en la Sentencia del Tribunal Supremo 261/2017, de 26 de abril, el cual tiene que ver con la posibilidad de revisión en sede casacional de los hechos, así como de las cuantías indemnizatorias concedidas en instancias inferiores. Sobre este aspecto, primeramente declara que la regla general es la imposibilidad de acceso a casación de este tipo de cuestiones[30]. No obstante, posteriormente manifiesta que, dado que se trata de un derecho fundamental, como es el derecho al honor, el que se ha quebrantado, la revisión a través del recurso de casación tiene un margen más amplio, manifestando sobre este particular:

> El ámbito de la revisión que es posible en casación es más amplio en este tipo de litigios que en otros que versan sobre cuestiones sin trascendencia constitucional. Cuando la resolución del recurso de casación afecta a derechos fundamentales, este tribunal no puede partir de una incondicional aceptación de las conclusiones probatorias obtenidas por las sentencias de instancia, sino que debe realizar, asumiendo una tarea de calificación jurídica, una valoración de los hechos en todos aquellos extremos relevantes para apreciar la posible infracción de los derechos fundamentales alegados (sentencias núm. 311/2013, de 8 de mayo, y núm. 312/2014, de 5 de junio, entre las más recientes).

---

30 Expresando que: «Constituye doctrina constante de esta Sala (entre las más recientes, SSTS de 9 de octubre de 2015, rec. núm. 669/2013, de 10 de febrero de 2014, rec. núm. 2298/2011, y 22 de enero de 2014, rec. núm. 1305/2011) que la fijación de la cuantía de las indemnizaciones por resarcimiento de daños morales en este tipo de procedimientos es competencia de los tribunales de instancia, cuya decisión al respecto ha de respetarse en casación salvo que "no se hubiera atenido a los criterios que establece el art. 9.3 LO 1/82" (STS de 17 de julio de 2014, rec. núm. 1588/2008, con cita de las SSTS de 21 de noviembre de 2008, en rec. núm. 1131/2006; 6 de marzo de 2013, en rec. núm. 868/2011; 24 de febrero de 2014, en rec. núm. 229/2011, y 28 de mayo de 2014, en rec. núm. 2122/2007) o en caso de error notorio, arbitrariedad o notoria desproporción (sentencias de 5 de diciembre de 2000, 31 de enero de 2001, 25 de enero de 2002, 10 de junio de 2002, 3 de febrero de 2004, 28 de marzo de 2005, 9 de junio de 2005, 21 de abril de 2005, 17 de enero de 2006, 27 de febrero de 2006, 5 de abril de 2006, 9 de junio de 2006, 13 de junio de 2006, 16 de noviembre de 2006)».

7.2. Una tendencia a evitar: Las indemnizaciones simbólicas o *nummo uno*

La antes citada Sentencia del Tribunal Supremo 261/2017, de 26 de abril, al margen de considerar que la reducción indemnizatoria efectuada en segunda instancia era improcedente y no podía basarse en la escasa cuantía de la deuda incluida en el registro de morosos, estima que la cuantía concedida en dicha instancia adolecía de otro error, como es el de su escasa cuantía (2.000 euros), lo cual lleva al tribunal a concluir que dicha indemnización resulta simbólica y, por ende, inadmisible también por este motivo. Esta problemática tiene que ver con la concesión de indemnizaciones simbólicas o *nummno uno*. Este tipo de supuesto acaecen en los casos donde, si bien se considera que existe una intromisión ilegítima en los términos del artículo 9.3 de la Ley Orgánica 1/1982, el perjuicio que debe presumirse *iuris et de iure* no es de suficiente entidad como para conceder una cuantía indemnizatoria verdadera. Con ello, se incurre en una tendencia que debe evitarse, motivada por el hecho de que algunos tribunales consideran que se ven obligados a condenar al demandado por haber incurrido en intromisión ilegítima pero, desde su punto de vista, no existe un verdadero daño indemnizable como tal. Por ello, y a fin de cumplir con la normativa, estiman la intromisión ilegítima, aunque a la hora de cuantificar la indemnización la reducen en tal extensión que la convierten en irrisoria, esto es, simbólica, la cual nada tiene que ver con una verdadera indemnización destinada a reparar un daño. Así, este tipo de prácticas estás proscritas por el Tribunal Supremo, y como expresa la referenciada Sentencia del Tribunal Supremo 261/2017, de 26 de abril:

> Una reducción tan notoria como la llevada a cabo por la sentencia recurrida, en circunstancias como las descritas, ha de calificarse de indemnización simbólica, disuasoria para impetrar la tutela de derechos que son fundamentales para la persona.

Por tanto, desde mi punto de vista, y sobre la posición mantenida actualmente por el Tribunal Supremo en tiempos más recientes, la concesión de indemnizaciones simbólicas o *nummo uno* impide la correcta tutela de derechos fundamentales, como son el honor, la intimidad y la propia imagen. En esta línea encontramos supuestos donde se conceden indemnizaciones claramente irrisorias. Así resulta sorprendente el criterio antes seguido (y que, afortunadamente, parece ya desterrado) por el Tribunal Supremo en su Sentencia 1302/1989, de 23 de febrero de 1989 (Id. CENDOJ: 28079110011989100433), donde la cuantía indemnizatoria por la difamación sufrida por un médico por una carta injuriosa publicada en un diario se establece en una peseta[31]. Debe matizarse que este tipo de indemnizaciones son habituales en el

[31] Esta sentencia, al mismo tiempo, es una muestra de cómo se confunde la poca divulgación y la falta de lucro derivado con la información con el hecho de que no se vulnere el ámbito del daño moral del derecho al honor. En este sentido, se afirma que «es de tener en cuenta que es constante y reiterada la doctrina mantenida por esta Sala, siempre que se respeten los parámetros legales en orden al hecho, la de que: "el *quantum* de la indemnización es una cuestión de hecho, atribuible por su naturaleza al juzgador, pues el daño moral se valora atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente

mundo anglosajón, pero complican aún más la valoración en el derecho español respecto de los daños a los derechos fundamentales del artículo 18.1 de la Constitución, pues conllevan que de manera velada se eliminen los fines reparadores de la protección de tales derechos y se rebajen las acciones en garantía de los mismos a un simple reconocimiento declarativo de su existencia. Por ello, comparto la postura de Martín Casals (1990, p. 1.264), quien afirma que «si no hay indemnización es porque no hay daño en sentido jurídico del que se deba responder; si hay daño, y no puede ser reparado en forma específica, deberá haber una indemnización», de manera que «la indemnización simbólica o *nummo uno* no es propiamente una indemnización». No obstante, y afortunadamente, el propio Tribunal Supremo, en fechas más recientes, se ha manifestado en contra de la concesión de este tipo de indemnizaciones. Así, la Sentencia del Tribunal Supremo de 17 de octubre de 1996 (rec. núm. 2973/1993), en un supuesto donde el demandante reclamaba una peseta por considerarse difamado afirma que:

> Esta Sala tiene declarado que su misión no es la de dar satisfacción moral, sino la de resolver problemas jurídicos con entidad real, por lo que debe proscribirse toda condena simbólica.

E, igualmente, el Tribunal Constitucional ha declarado inadmisibles este tipo de condenas indemnizatorias de carácter simbólico[32].

Por ende, aunque los derechos al honor, intimidad y propia imagen tengan un contenido extrapatrimonial, también existe una vertiente patrimonial, que es la que trata de garantizar el artículo 9.3 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, por lo que si se vulnera alguno de estos derechos y pretende satisfacerse dicha vertiente patrimonial, así como alcanzar una reparación del daño, debe evitarse la concesión de indemnizaciones meramente simbólicas. Ello, porque si bien es cierto que la reparación ideal para los daños morales causados al derecho al honor,

---

producida, la determinación de cuyos factores han de quedar al prudente y buen criterio de los tribunales de instancia", siendo exponentes de la indicada doctrina, entre otras, las sentencias de 11 de abril y 1 de diciembre de 1987, y 19 de febrero, 22 de junio, 18 y 19 de julio de 1988, y en cuenta, también, que la indemnización se valorará atendiendo a los presupuestos de las circunstancias del caso, gravedad de la lesión efectivamente producida y beneficio que haya obtenido el causante de la lesión como consecuencia de la misma. El análisis del hecho de autos es revelador de que el causante directo de la intromisión ilegítima, el señor C. C., no obtuvo ningún beneficio derivado de ella, siendo muy dudoso que percibiera alguno significativo la empresa editorial, ya que la sección de "cartas" en que se publicó el documento carecía de relieve e importancia comparada con las restantes del periódico; y, por otro lado, como bien dice el juez de primer grado, no se produjo "menoscabo del prestigio y reputación profesional del actor", toda vez que era de público conocimiento la postura favorable al aborto por parte del mismo y la realización de tal operación, ello sin contar que aquel, con sus manifestaciones en medios de difusión, venía a provocar, en cierta manera, las reacciones contrarias, además, no ha resultado acreditada la concurrencia en el caso concreto de circunstancias especiales que determinen una valoración del daño moral, y de aquí que el razonamiento del juez de fijar por tal concepto "una cantidad meramente simbólica" resulte ajustado a derecho, todo lo cual viene a determinar el rechazo del segundo motivo, ante la inexistencia de la infracción que lo configura».

[32] *Vid*. SSTC 12/1994, de 17 de enero y 186/2001, de 17 de septiembre.

intimidad o propia imagen sería una restitución *in natur*a (es decir, volver al estado anterior en que la intromisión ilegítima y el daño se produjeron), esta opción es irrealizable, por lo que la reparación del daño tendrá que venir necesariamente a través de una restitución equivalente, lo cual supondrá conceder una cuantía indemnizatoria. Y si esta cuantía indemnizatoria resulta irrisoria o simbólica se estará degradando y minusvalorando la protección que debe otorgarse a estos derechos fundamentales reconocidos en el artículo 18.1 de la Constitución.

8. La mera inclusión en el CIRBE sin que exista morosidad no supone vulneración del derecho al honor. A raíz de la Sentencia del Tribunal Supremo 586/2017, de 2 de noviembre

A la vista de lo anteriormente expuesto y analizado, los ficheros con un carácter económico indirecto (como es el caso del CIRBE) deben diferenciarse de aquellos que sí tienen estrictamente este carácter económico, como son los registros de morosos. Por tanto, en los supuestos de inclusión de datos personales en los primeros, los criterios a seguir en orden a determinar si existe una vulneración del derecho al honor del titular de los daños deben valorarse en atención a otras pautas.

De este modo, como concluye la Sentencia del Tribunal Supremo 568/2017, de 2 de noviembre, la simple inclusión en el CIRBE de los datos relativos a la existencia de una deuda o de una garantía, sin que exista una situación de morosidad, no implica atentado contra el derecho al honor susceptible de ser indemnizado. En consecuencia, como indica el Tribunal Supremo, para entender producido un atentado contra el honor por la inclusión indebida de los daños personales del afectado en el CIRBE, se exige «que de las menciones contenidas en el fichero del CIRBE se desprenda que el afectado es un moroso, y que tales menciones no respondan a la realidad». Sin embargo, a raíz de los hechos objeto de enjuiciamiento en la Sentencia del Tribunal Supremo 568/2017, de 2 de noviembre, las menciones contenidas en el CIRBE únicamente indicaban que los demandantes estaban afectos por un riesgo indirecto al aparecer como avalistas. Por tanto, no podía deducirse situación de morosidad derivada de esta inclusión de datos personales y tampoco producida intromisión ilegítima en el derecho al honor de los titulares de los datos.

Ahora bien, como se ha dicho, debe tenerse en cuenta que el CIRBE no recoge únicamente datos personales de los que pueda extraerse una situación de morosidad, sino también otros datos relacionados con la solvencia y los riesgos financieros como, por ejemplo, las circunstancias de que el titular de los datos figure como avalista, fiador, etc. Y en este sentido, debe puntualizarse que tales datos no están exentos de control judicial, por lo que pueden conllevar una intromisión ilegítima en el derecho al honor si tales datos no son ciertos. E, incluso, no solo puede verse afectado un derecho fundamental como es el derecho al honor, sino que también puede producirse un daño merecedor de resarcimiento a pesar de que su vulneración no tenga rango constitucional, si de la inclusión de un dato de manera indebida se causan perjuicios, como

pueden ser eventuales denegaciones de créditos o financiaciones por entidades que actúen sobre la base de la información a que han tenido acceso a través del CIRBE. Esta situación es atisbada por la Sentencia del Tribunal Supremo 568/2017, de 2 de noviembre, al afirmar que:

> La inclusión indebida, por no ser cierta o no ser exacta, de los datos personales de una persona física en el CIRBE puede suponer la vulneración de su derecho al honor, pero también de otros derechos distintos del derecho al honor, de naturaleza constitucional o infraconstitucional, o puede causar al afectado daños de naturaleza extracontractual, como pudiera ser el daño patrimonial consistente en la denegación de financiación por un exceso de riesgo que no era real.

En definitiva, los datos personales que se recojan indebidamente en el CIRBE y sin cumplir con las exigencias de la normativa sobre protección de datos pueden dan lugar a indemnización por intromisión ilegítima en el derecho al honor si de los mismos se desprende una situación de morosidad al amparo del artículo 9.3 de la Ley Orgánica 1/1982, de 5 de mayo. Sin embargo, también pueden producirse daños que no afecten necesariamente al derecho al honor si como consecuencia de la inclusión indebida de datos en el CIRBE, se irrogan perjuicios al titular de los mismos. Perjuicios tales como posibles denegaciones de créditos, financiaciones, etc., efectuadas en atención a los datos incluidos erróneamente, los cuales, a fin de alcanzar una *restitutio in integrum* podrán fundarse conforme a otras reglas de responsabilidad civil, como serían las generales contenidas en los artículos 1.902 y siguientes del Código Civil o, incluso, conforme a los antes citados artículos sobre responsabilidad civil incluidos en la legislación sobre protección de datos, como son el artículo 19 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre o, a partir del 25 de mayo de 2018, el artículo 82.1 del Reglamento UE 2016/679.

9. Conclusiones

1. El Reglamento UE 2016/679 supone un claro avance en los derechos y garantías de los particulares en lo relativo al tratamiento de sus datos personales y, en consecuencia, derivará en una protección más eficaz del derecho fundamental a la intimidad. Además, el referenciado reglamento va un paso más allá en lo que venía siendo la voluntad del legislador de la Unión Europea, pues a diferencia de la regulación anterior, esto es, la Directiva 1995/46/CE, tiene una eficacia directa en todos los Estados miembros y no necesita ningún acto de transposición para su aplicación, como así ocurre con las directivas de la Unión Europea.

2. No obstante lo anterior, el Reglamento UE 2016/679 exige que las legislaciones nacionales se acomoden a su regulación en orden a que no existan incongruencias normativas. Por ello, en España, desde su publicación el 24 de noviembre en el Boletín Oficial del Congreso de los Diputados, se tramita el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal con la finalidad de adaptar la ley española a las modificaciones introducidas por el Reglamento UE 2016/679. Sin embargo, el Reglamento UE 2016/679 no limita que

las modificaciones legislativas nacionales introduzcan mayores protecciones que las contenidas en aquel. En consecuencia, la tramitación parlamentaria del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal debe constituir, al mismo tiempo, una oportunidad para poder mejorar y aclarar aquellas cuestiones donde el Reglamento UE 2016/679 puede resultar escueto o plantear dudas sobre los límites, excepciones, etc., en su aplicación.

3. El denominado principio de responsabilidad proactiva supone un cambio en la concepción de protección de datos de carácter personal llevada a cabo por el Reglamento UE 2016/679. En virtud de este principio, los responsables del tratamiento de datos dejarán de actuar a la vista de una posible vulneración en la protección de datos, en lo que se venía conociendo hasta ahora como «responsabilidad reactiva», y tendrán que tomar todas las medidas necesarias encaminadas a la protección de las personas cuyos datos administren, gestionen, almacenen, etc., y lo que es más importante, deberán estar en disposición de acreditar estas medidas ante las autoridades competentes.

4. La introducción de la figura del delegado de protección de datos es una destacada novedad del Reglamento UE 2016/679. Resultan importantes las funciones que este profesional puede adquirir, pero se debe ser precavido, pues puede estar sujeto a altas responsabilidades, de manera que las empresas aprovechen la ocasión para intentar exonerarse de su responsabilidad trasladándola toda a dicho delegado de protección de datos. Todo ello al margen de la cualificación que se exigirá a este profesional, pues el Reglamento UE 2016/679 no solo permite que el delegado de protección de datos se instaure con personal interno o externo, sino que guarda silencio en lo referente a la formación requerida para poder ejercer sus funciones.

5. En cuanto a la responsabilidad de los encargados del tratamiento de ficheros de solvencia patrimonial, cabe concluir que la inclusión errónea de datos personales es uno de los casos que más perjuicios pueden generar a los particulares, especialmente por el hecho de que les supone una gran traba de cara a obtener créditos o poder realizar otro tipo de operaciones financieras. Por ello, como se analiza en el estudio y al amparo de la interpretación de Tribunal Supremo, la escasa cuantía por la que se incluye erróneamente a una persona en los llamados registros de morosos no implica que el daño que deba ser resarcido resulte menor por este hecho. En esta línea, la fundamentación para obtener una indemnización puede encontrar cobertura en distintos preceptos del ordenamiento jurídico, aunque los tribunales prefieren acogerse al concepto de «intromisión ilegítima» de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

6. Finalmente, en otro tipo de ficheros de solvencia patrimonial con un contenido económico que puede denominarse «indirecto» (como el caso del CIRBE), también se pueden generar daños a los particulares por la inclusión errónea de sus datos personales. Sin embargo, de la mera inclusión en este tipo de ficheros de solvencia patrimonial no se irrogará un daño si no puede desprenderse con ello que se imputa una situación de morosidad al afectado. No obstante, el Tribunal Supremo deja abierta la posibilidad de que exista una vulneración al derecho al honor si este tipo de casos, a pesar de no equivaler a una declaración de morosidad, supone para el particular un obstáculo de cara a realizar determinadas operaciones financieras, como determinados negocios jurídicos de garantía (aval, fianza, etc.).

Referencias bibliográficas

Aparicio Salom, J. (2009). *Estudio sobre la Ley Orgánica de protección de datos de carácter personal*. Navarra: Aranzadi.

Ebrahim, A. (2010). The many faces of nonprofit accountability. *Harvard Business School Working Paper*.

Garzón Clariana, G. (1981). La protección de los datos personales y la función normativa del Consejo de Europa. *Revista de Instituciones Europeas*, *8*(1).

Lesmes Serrano, C. (Coord.). (2008). *La Ley de protección de datos. Análisis y comentario de su jurisprudencia*. Valladolid: Lex Nova.

López Román, E. y Mora Sanguinetti, J. S. (2009). Un análisis de la estructura institucional de protección de datos en España. *InDret*, *2/2009*.

Lucas Murillo de la Cueva, P. (1993). Informática y protección de datos personales. En *Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter persona*. Madrid: Centro de Estudios Constitucionales.

Martín Casals, M. (1990). Notas sobre la indemnización del daño moral en las acciones por difamación de la LO 1/1982. En Asociación de Profesores de Derecho Civil, *Centenario del Código Civil*, t. II. Madrid: Centro de Estudios Ramón Areces.

Méndez, M. (2010). Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States. *Publius: The Journal of Federalism*, *40*(4).

Núñez García, J. L. (28 de enero de 2014). La accountability, ¿herramienta sancionadora? Asociación Profesional Española de Privacidad (APEP). Recuperado de <http://www.apep.es>.

Ordóñez Solís, D. (2011). *Privacidad y protección judicial de datos personales* Barcelona: Bosch.

Ortí Vallejo, A. (1994). *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*. Granada: Comares.

Recio Gayo, M. (12 de enero de 2017). Directrices del GT29 sobre el delegado de protección de datos: figura clave para la responsabilidad («accountability»). *Diario La Ley*, *2*, sección Legal Management.

Troncoso Reigada, A. (Dir.). (2006). Estudios sobre Administraciones públicas y protección de datos personales. En *I Encuentro entre Agencias Autonómicas de Protección de Datos Personales*. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid.

Vizcaíno Calderón, M. (2001). *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas.