7 comunitania

REVISTA INTERNACIONAL DE TRABAJO SOCIAL Y CIENCIAS SOCIALES
INTERNATIONAL JOURNAL OF SOCIAL WORK AND SOCIAL SCIENCES

ENERO / 2014

ISSN: 2173-0512 / www.comunitania.com

YOLANDA AGUDO | FRANCISCO JAVIER GARCÍA | LAURA PONCE DE LEÓN | SILVIA VÁZQUEZ
BLANCA GUADALUPE CID DE LEÓN | JOSEFINA PIMENTEL | Mª CARMEN PLANA | JAVIER SIERRA | LUIS MANUEL RODRÍGUEZ

El derecho fundamental a la protección de datos personales y los ficheros privados: el interés legítimo en el tratamiento de datos[1]

The fundamental right of personal and private files protection: the legitimate interest in the data processing

Mª Carmen Plana Arnaldos*

* Universidad de Murcia. mcarmenp@um.es

Abstrac:

This paper aims to describe the evolution of the concept of data protection as a fundamental right in spanish law and in european law. There is specially analyzed the regulation of private information files, in particular files relating to the creditworthiness and fulfilment or non-fulfilment of pecuniary obligations. In this particular case, one of the outstanding characteristic is the possibility of processing personal information without consent, working on the principle that a legitimate interest, that justifies it, exists. Nevertheless, only to appeal for a legitimate interest is not enough, it is necessary to strike a balance between the legitimate interest of whom is going to process personal information and rights of individuals to privacy, to determinate wich one should prevail considering the circumstances.

Keywords: Personal data protection. Files relating to the creditworthiness and fulfilment or non-fulfilment of pecuniary obligations. Consent. Legitimate interest.

Resumen:

Este trabajo pretende dar una visión de la concepción actual de la protección de datos como derecho fundamental, tanto en el ordenamiento jurídico español, como en el europeo. En especial, se analiza la regulación de los ficheros de datos de carácter privado, en concreto los ficheros de solvencia patrimonial y cumplimiento e incumplimiento de obligaciones dinerarias. En estos casos, una de las especialidades más destacadas es la posibilidad de tratar datos de la persona sin su consentimiento, sobre la base de la existencia de un interés legítimo que lo justifica y permite. Con todo, la mera invocación de un inte-

[1] Este trabajo se enmarca dentro del proyecto de investigación del Ministerio de Ciencia e Innovación español: "Los desafíos jurídicos de Internet para la protección de los datos personales: hacia un marco normativo de tercera generación" (ref. DER2009-09157).

rés legítimo no es suficiente para legitimar el tratamiento de datos sin el consentimiento del afectado, será necesario realizar en cada caso concreto una ponderación entre el interés legítimo de quien va a tratar los datos y los derechos fundamentales de los ciudadanos afectados, con el fin de determinar cuál prevalece atendiendo a las circunstancias concurrentes.

Palabras clave: Protección de datos personales. Ficheros de solvencia patrimonial y cumplimiento e incumplimiento de obligaciones dinerarias. Consentimiento. Interés legítimo.

Article info:

Received: 16/10/2012 / Received in revised form: 07/03/2013
Accepted: 01/04/2014 / Published online: 30/01/2014
DOI: http://dx.doi.org/10.5944/comunitania.7.4

1. El reconocimiento del derecho a la protección de datos en el ordenamiento español y en la Unión Europea

El derecho a la protección de los datos personales se reconoce y garantiza en la actualidad en los distintos países del entorno jurídico europeo, incluido nuestro país. Esta circunstancia es fruto de una larga evolución reflejada en la doctrina y legislación de los distintos países y también en las normas del Derecho de la Unión Europea.

Así, por lo que se refiere a nuestro país (vid. sobre el concepto de derecho fundamental a la protección de datos y su consolidación: Lucas Murillo 1990 y 2002; Martínez 2004 y 2007), la concepción de la protección de datos personales como derecho fundamental ha sido establecida por el Tribunal Constitucional en diversas sentencias, que han desembocado en el reconocimiento de un derecho fundamental y autónomo a la protección de datos personales que se incluye en el artículo 18.4 de la Constitución Española. La primera de estas sentencias (254/1993) recoge el derecho a la que denomina "libertad informática", de manera poco definida y con perfiles que no resultan demasiado claros (vid. Villaverde 1994); se trata solo del punto de partida de un camino que se va a desarrollar teniendo en cuenta los nuevos perfiles y contenido de un amplio derecho a la privacidad y en la misma línea establecida por la que es comúnmente admitida como la primera sentencia en la materia: la sentencia del Tribunal Constitucional alemán en relación a la Ley del Censo, según la cual el derecho general del individuo a la privacidad supone la atribución de la capacidad de decidir, en el ejercicio de su autodeterminación, que datos quiere revelar sobre sí mismo (sobre esta sentencia vid. Heredero 1983**)**. Esta corriente va a desembocar en nuestro ordenamiento jurídico, en la conocida sentencia del Tribunal Constitucional 292/2000, en el reconocimiento del derecho fundamental a la protección de datos, con perfiles ya claros y delimitados (vid. Lucas Murillo 2003; Garriga 2009). En esta resolución el Alto Tribunal asume la interpretación según la cual el artículo 18.4 de la CE incorpora un derecho fundamental autónomo que hay que

diferenciar del derecho a la intimidad (en el Fundamento jurídico quinto de esta sentencia el Tribunal entiende que *"Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos, cuya concreta regulación debe establecer la ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente que también su objeto y contenido difieran"*).

La concepción del derecho a la protección de datos establecida por el Tribunal Constitucional, a pesar de ser objeto de crítica por diversos sectores doctrinales, se ha reflejado en la legislación en la materia, especialmente en la vigente LOPD (Ley Orgánica 15/1999 de 13 de diciembre de Protección de los Datos de Carácter Personal) y en el Reglamento de desarrollo de la Ley, aprobado por Real decreto 1720/2007 de 21 de diciembre (RLOPD).

Junto al desarrollo de la legislación y doctrina interna en materia de protección de datos, la situación actual ha de tener en cuenta los trabajos que se han desarrollado en este ámbito en la Unión Europea, que han incidido decisivamente en nuestra legislación. En este sentido, el artículo II-68 de la Constitución Europea, pese a no haber llegado a buen fin, da una clara idea de la concepción de este derecho (*"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se trataran de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto en la ley. Toda persona tiene derecha a acceder a los datos recogidos que le conciernan y obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente"*).

Por lo que se refiere al derecho positivo, la Directiva 95/46, de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, constituye el marco de referencia general, en el ámbito de la Unión Europea, con relación a la protección de datos y, por tanto, el parámetro al que deben ajustarse las legislaciones de los distintos Estados miembros de la Unión.

Esta norma de referencia, junto a diversas normas complementarias (Directiva 97/66, de 15 de diciembre de 1976, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, la Directiva 2002/58, de 12 de julio de 2002, relativa al tratamiento de los datos personales y la

protección de la intimidad en el sector de las comunicaciones electrónicas y la Directiva 2006/24 sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones) ha sido desde su promulgación hasta hoy el marco de referencia al que se han acomodado las diversas legislaciones en la materia de los Estados miembro. Sin embargo, se plantea actualmente una reforma general en materia de protección de la privacidad y más concretamente una reforma en las normas reguladoras de la protección de los datos personales.

Esta reforma se plantea como un nuevo marco regulador llamado "de tercera generación", que supere las carencias observadas en la regulación actual. A estos efectos, resulta útil señalar que se han distinguido diversas etapas o generaciones de la protección de la privacidad: en la "1ª generación" el concepto de privacidad es meramente negativo, el derecho de exclusión de los demás del ámbito de lo privado (derecho a la intimidad...). La "2ª generación", la actual, está determinada por los avances sociales, tecnológicos e informáticos y el cambio en los modos de relación. Y por fin, la "3ª generación", se caracteriza por el desarrollo de las TICs (Tecnologías de la Información), que suponen cambios en las relaciones sociales, en el comportamiento individual y demandan nueva regulación, ya que los esquemas y principios actuales no son adecuados para resolver las nuevas necesidades.

En este nuevo marco regulador, se incluye la reforma de la protección de los datos personales. En particular, uno de los pilares de la reforma es el reforzamiento de los derechos del titular de los datos, lo que se pretende conseguir a través de diversas vías, en especial, se entiende como esencial la nueva regulación del consentimiento, ya que resulta ser en última instancia éste el elemento decisivo para legitimar el tratamiento de datos personales; dicho de modo sencillo: al margen del cumplimento de otros requisitos específicos y que pueden variar en cada caso, el tratamiento de datos personales con consentimiento del titular es lícito, y no lo es si no media este consentimiento. La regulación actual exige un consentimiento inequívoco del titular de los datos para el tratamiento. El problema es que se ha interpretado de maneras diversas lo que es el consentimiento inequívoco en las diversas legislaciones: unas veces es consentimiento expreso, otras se admite el consentimiento tácito e incluso se admite el silencio como declaración de voluntad (art. 14 RLOPD).

El Parlamento Europeo insiste en que el consentimiento ha de ser *explícito* y, desde luego, no puede considerarse explícito el silencio. Realmente el silencio podría considerarse como declaración de voluntad cuando una norma obliga a actuar y no se hace, o cuando de las circunstancias, el uso y la buena fe se puede deducir la existencia de este deber de actuar. No obstante, otorgar valor positivo al silencio debe hacerse con mucha cautela cuando está en juego un derecho fundamental como es la protección de datos personales. Llama la atención que en ámbitos como el derecho de consumo, en los que no está en juego un derecho funda-

mental, pero las circunstancias son muy similares a las de la materia que tratamos (asimetría contractual, ventaja informativa institucional, vulnerabilidad de una de las partes, considerada como más débil…) se prohíbe otorgar valor positivo al silencio (entre otros textos normativos: Texto Refundido de la Ley de Defensa de Consumidores y Usuarios: TRLGDCU, Ley de Comercialización a distancia de servicios financieros…).

Por otra parte, en el entorno en línea se plantean problemas específicos en relación a cuando debe considerarse que existe consentimiento, por ejemplo, si los parámetros del navegador del internauta expresan su consentimiento.

Partiendo de las consideraciones expuestas, en este trabajo nos proponemos dar una breve visión sobre cómo han de ser aplicados actualmente los principios y normas de protección de datos a un tipo específico de tratamiento de datos personales que son los ficheros privados, y más concretamente, en el caso de los ficheros privados que tratan datos de cumplimiento e incumplimiento de obligaciones dinerarias, los conocidos como "ficheros de morosos" (vid. una perspectiva general sobre la regulación de los ficheros privados desde la consideración de la protección de datos como derecho fundamental, en Delgado 2009).

2. El derecho a la protección de datos personales y los ficheros privados

El tratamiento de datos personales con fines de publicidad, o con la finalidad de conocer la solvencia del particular, llevados a cabo por empresas titulares de "ficheros privados" es una práctica común en la sociedad actual, no exenta, sin embargo, tanto de críticas, especialmente por su funcionamiento, como de riesgos, ya que los intereses económicos en juego hacen necesario un estricto control para evitar que se vulneren los derechos de los particulares (vid. el comentario al artículo 30 de la LOPD en Martínez 2009; Aparicio 2009; Troncoso 2010).

La existencia de estos ficheros está amparada en nuestra legislación. La Ley española de protección de datos (LOPD) hace una referencia específica a diversos ficheros de titularidad privada que, por sus características (procedencia y naturaleza de los datos, relevancia social y económica de los mismos...) merecen una regulación especial. En este sentido, además de los ficheros sobre publicidad, el art. 29 de la citada Ley regula el régimen especial para el tratamiento de datos relativos a solvencia patrimonial y crédito.

Resulta de especial interés el caso de los llamados ficheros de solvencia patrimonial y crédito, ya que en este caso el principio fundamental del consentimiento, esencial para la legitimidad del tratamiento de datos personales, se excepciona, sobre la base, según vamos a ver, de la existencia de un "interés legítimo" que se convierte en elemento legitimador sustituyendo al citado consentimiento.

2.1. Ficheros de solvencia patrimonial: concepto y funcionamiento

El art. 29 de la LOPD regula el régimen especial para el tratamiento de datos relativos a solvencia patrimonial y crédito. Hasta fechas relativamente recientes, el escaso régimen jurídico establecido en la Ley se completaba con la Instrucción 1/1995 de 1 de marzo de la Agencia Española de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito y la Instrucción 1/1998 de 19 de enero relativa al ejercicio de los derechos de acceso, rectificación y cancelación (cuya Norma cuarta se refiere específicamente a estos ficheros). Actualmente, el artículo 29 se completa con las previsiones sobre ficheros de solvencia patrimonial contenidas en el Reglamento de desarrollo de la LOPD (El título IV, bajo la rúbrica "Disposiciones aplicables a determinados ficheros de titularidad privada" establece el régimen aplicable a los que comúnmente se conocen como ficheros especiales o simplemente ficheros privados: los "Ficheros de información sobre solvencia patrimonial y crédito", capítulo I, y los ficheros para publicidad, capítulo II "Tratamientos para actividades de publicidad y prospección comercial". Los artículos 37 a 44 se refieren específicamente a los "Ficheros de información sobre solvencia patrimonial y crédito").

Podríamos definir los ficheros a los que nos referimos, a falta de un concepto legal, como aquellos ficheros que tienen como finalidad dar a conocer datos relativos a la solvencia patrimonial y al grado de cumplimiento o incumplimiento de las obligaciones dinerarias de los sujetos incluidos.

Sobre la base de reconocer el interés legítimo que subyace en el tratamiento de estos datos, la LOPD reconoce la posibilidad de crear ficheros de solvencia patrimonial en los que se incluyen datos económicos del sujeto sin su consentimiento. Partiendo de esta base, la regulación de estos ficheros privados se funda en dos principios: de un lado, se excepcionan para los ficheros de solvencia patrimonial y las entidades prestadoras de este servicio algunos de los principios generales que inspiran la legislación de protección de datos, especialmente la necesidad de consentimiento del sujeto para ser incluidos los datos en el fichero (principio de consentimiento informado). Y por otro lado, para asegurar los derechos de los incluidos y garantizar la seguridad jurídica y el respeto a los principios inspiradores de la legislación sobre protección de datos personales, se establecen una serie de requisitos especiales para la creación de estos ficheros (especialmente en cuanto a las fuentes de información), y que deben cumplir las entidades prestadoras de este servicio (comunicación de la inclusión, de las informaciones suministradas sobre el contenido del fichero...) y también se regula la baja en los mencionados ficheros (que en la práctica plantea graves problemas).

Debemos señalar que coexiste con estos ficheros privados un fichero sobre datos económicos de los particulares y empresas dependiente del Banco de España, la Central de Riesgos del Banco de España: CIRBE (El régimen jurídico de la CIRBE está

básicamente en la Ley 44/2002 de 22 de noviembre de medidas de reforma del sistema financiero y en Circulares del Banco de España, en especial la 3/1995 de 25 septiembre y las posteriores de modificación parcial. La normativa aplicable se puede consultar en la página web del Banco de España (www.bed.es)). La naturaleza pública de tal fichero lo excluye del ámbito de aplicación del art. 29 LOPD, quedando sometido a su propio régimen jurídico, aunque ciertamente tanto la finalidad como el funcionamiento de la CIRBE resultan similar a la de los ficheros de solvencia patrimonial (La Ley 44/2002 de Reforma del Sistema Financiero, establece en su artículo 69, en el marco de la regulación de la CIRBE, que "la actividad de facilitar a las entidades de crédito los datos necesarios para el ejercicio de su actividad crediticia podrá ser también realizada por otras entidades de naturaleza privada cuya actividad se ajustará, en todo caso, al régimen previsto en la LOPD"). Según la información institucional sobre este servicio, la Central de Información de Riesgos del Banco de España tiene como principal objetivo facilitar a las entidades declarantes (entidades de crédito y otros) los datos necesarios para el mejor análisis de sus riesgos de crédito. Asimismo, la CIRBE permite al Banco de España obtener datos globales sobre los créditos concedidos por las entidades, con lo que facilita el adecuado ejercicio de sus competencias de supervisión bancaria.

Cualquier Entidad declarante a la CIRBE recibe mensualmente la información agregada de todo el sistema del riesgo de las personas físicas y jurídicas declarados por ella (titulares), y puede acceder a una información similar de los titulares para los que no haya declarado riesgos a la CIRBE, siempre, en este último caso, que éstos le hayan solicitado una operación de riesgo o figuren como obligados al pago o garantes en documentos cambiarios o de crédito cuya adquisición o negociación le haya sido solicitada a la entidad.

Asimismo, cualquier titular, persona física o jurídica, podrá solicitar los datos declarados en la CIRBE a su nombre, para lo cual deberá identificarse fehacientemente". Este esquema de funcionamiento resulta muy parecido al de los ficheros privados, pero no se incluye en el ámbito de aplicación de la LOPD y por tanto no es objeto de nuestro estudio. Centrándonos en los ficheros privados, conforme al régimen establecido en la LOPD, hay que diferenciar dos tipos de ficheros, a los que se refiere el artículo 29:

a) Los que contienen datos sobre solvencia patrimonial y crédito de naturaleza positiva, es decir, información sobre las posibilidades económicas y financieras de una persona. Sólo podrán obtenerse los datos de estos ficheros: de fuentes accesibles al público; de informaciones facilitadas por el afectado; de cesiones consentidas por el afectado. Es decir, el tratamiento de estos datos requiere bien el consentimiento del afectado, regla general de la legislación sobre protección de datos personales, o bien la habilitación legal, que se esté ante un supuesto en que la norma permite el tratamiento sin consentimiento (información proveniente de fuentes accesibles al público y Registros).

b) Los que contienen información sobre cumplimiento o incumplimiento de obligaciones dinerarias. En este caso, sólo podrán obtenerse los datos personales del acreedor o quien actúe por su cuenta o interés, con la obligación de éste de notificarlo al afectado.

Realmente, los denominados "ficheros de morosos" son los que recogen este segundo tipo de datos y son los que se han constituido en el práctica más habitual, convirtiéndose además, en un elemento de gran importancia en el tráfico jurídico-patrimonial (vid. Casado 2004; Ferrando 2009).

En este segundo supuesto hay que tener en cuenta que, en el ámbito de la información sobre cumplimiento e incumplimiento de obligaciones es necesario distinguir entre dos tipos de ficheros, lo que responde a una realidad de la que ya se hizo eco, en lo que al Derecho español se refiere, la Instrucción de 1/1995, antes citada, según la cual "la realidad demuestra que coexisten perfectamente engarzados dos tipos de ficheros: uno el propio del acreedor, que se nutre de datos personales que son consecuencia de las relaciones económicas mantenidas con el afectado, cuya única finalidad es obtener la satisfacción de la obligación dineraria, y otro, un fichero que se podría denominar común que, consolidando todos los datos personales contenidos en aquellos otros ficheros, tiene por finalidad proporcionar información sobre la solvencia de una persona determinada y cuyo responsable, al no ser el acreedor, no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en aquellos".

Estamos por tanto ante dos tipos de ficheros: el del acreedor, del que provienen los datos y el fichero que acumula estos datos y presta el servicio de información. Este último es un fichero cuyo titular es una entidad prestadora de servicios de información y crédito al que acuden las empresas afiliadas en busca de esta información. Al fichero común podrán aportar datos el acreedor, es decir, el titular del derecho de crédito que ha quedado lesionado por el incumplimiento y quien actúa "por cuenta o interés del acreedor". En esta segunda referencia podríamos admitir a aquella persona que actúa en representación (directa o indirecta) del acreedor y quien actúa en interés del acreedor, como ocurre en el caso de la entidad bancaria encargada de gestionar el cobro que resulta fallido, o también los casos en que los datos son facilitados por una entidad encargada de recuperar la deuda.

Las entidades titulares de los ficheros prestan sus servicios en un ámbito de actividad económica, agrupando a diversas empresas pertenecientes a este sector (seguros, bancos y entidades de crédito o financieras etc.); estas empresas se asocian o afilian creando el fichero común cuya titularidad se atribuye a una entidad que realmente es la prestadora del servicio de información sobre solvencia patrimonial y crédito.

Se pueden distinguir dos fases en el desarrollo de su actividad: recogida de los datos suministrados por los afiliados e información a requerimiento de alguno de

los afiliados o asociados. Los afiliados (también denominados asociados o entidades suscriptoras; en definitiva, los demandantes del servicio) proporcionan datos relativos a sus clientes, como acreedores que son, siempre cumpliendo los requisitos exigidos: que se trate de deudores cuya deuda sea cierta, vencida, exigible, impagada, cuyo pago haya sido previamente requerido y no satisfecho, que no haya interpuesto reclamación y que no hayan transcurrido más de seis años desde que debió hacerse el pago (requisitos para la inclusión en el fichero, que se analizaran posteriormente). Estos son los datos de los que se nutre el fichero, cuyo contenido, en definitiva, será el resultado de la puesta en común de los datos que tienen las distintas empresas asociadas. Al mismo tiempo, los afiliados demandan información sobre la situación económica de determinada persona y proporcionársela constituye el verdadero objeto de la labor de la entidad prestadora del servicio. La relación entre el afiliado y la entidad prestadora se rige por un convenio suscrito entre ambos, en virtud del cual el afiliado se adhiere al fichero, comprometiéndose a proporcionar los datos sobre sus deudores, y el responsable del fichero común se obliga a facilitar la información que posea sobre la persona objeto de consulta. La posición jurídica de estos sujetos y el papel que cada uno desarrolla en el ámbito de la creación y mantenimiento de los ficheros de solvencia patrimonial, así como, fundamentalmente, el ámbito de decisión que a cada uno de ellos corresponde, sobre todo en lo que se refiere a la inclusión de los datos en el fichero, es fundamental para analizar la responsabilidad que cada uno de ellos ha de asumir, especialmente en los casos de inclusión de datos erróneos que probablemente sean los que plantean mayores problemas.

2.2. Requisitos de inclusión de datos y derechos de los afectados

Como hemos señalado, es necesario que se cumplan ciertos requisitos para que el acreedor pueda comunicar los datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias para que sean incluidos en el fichero común. Estos requisitos se encuentran enumerados básicamente en el art. 38 del RLOPD (antes en La Instrucción 1/1995, Norma primera, bajo el título *Calidad de los datos objeto de tratamiento*).

Con carácter general, el citado precepto establece que "solo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado…". Este límite, aunque impreciso, supone el veto a la mención de circunstancias personales o que no sean estrictamente relevantes (por ejemplo estado civil del deudor…). Según el artículo 38 RLOPD, los requisitos concretos para la inclusión de datos son (vid. la interpretación del precepto en los Comentarios al Reglamento de Palomar 2008; Martínez 2009):

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada (en este punto, la STS de julio de 2010 anuló la referencia que este

precepto hacía la necesidad de que no se hubiera entablado respecto a la deuda reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los comisionados para la defensa del cliente de servicios financieros, aprobado por Real decreto 303/2004 de 20 de febrero).

b) Que no hayan transcurrido 6 años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquella fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación. Con relación a este requisito se pueden plantear dudas en los casos en que se trate de una deuda con pluralidad de deudores y en el caso de que exista un fiador o avalista. Si acudimos a las reglas generales de obligaciones y contratos, en caso de que se trate de deudores solidarios, cada uno responde de la totalidad de la deuda, por lo que antes de incluir a cualquiera de ellos en el fichero, el acreedor deberá requerir el pago a todos ellos. Si son deudores mancomunados, es suficiente con que se requiera a cada uno por la parte de la deuda de que responde, de forma que si el requerido incumple, puede ser incluido en el fichero por la parte que le corresponde de la deuda. Por último, si hay un fiador o avalista de la deuda, habrá que requerir el cumplimiento a éste antes de incluir en el fichero al deudor principal (sobre el requerimiento previo de pago vid. Ramos 2008).

No podrán incluirse datos en el fichero cuando exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores. Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero. Una precisión similar ya se establecía en la Instrucción de 1995, según la cual el responsable del fichero común debería proceder a la cancelación cautelar del dato cuando el deudor aporte un principio de prueba documental suficiente que desvirtúe alguno de los requisitos de inclusión exigidos (por ej. justificante de pago...). El acreedor o quien actúe por su cuenta o interés estará obligado a conservar documentación suficiente que acredite el cumplimiento de los requisitos establecidos y de la información previa a la inclusión (art. 38.3 RLOPD).

Los datos incluidos en los ficheros no sólo deben cumplir los requisitos para su acceso antes mencionados, sino que deben respetar el principio general de calidad de los datos. Este principio, recogido en el art. 6 de la Directiva 95/46 y en el art. 4 de la LOPD supone que los datos objeto de recogida y tratamiento han de ser adecuados, pertinentes, no excesivos en relación con la finalidad para la que se recogieron, así como exactos y puestos al día, de forma que respondan de manera veraz a la situación actual del afectado, debiendo cancelarse o rectificarse si resultan inexactos o incompletos. En este mismo sentido, en relación a los ficheros de moro-

sos el art. 41 del RLOPD establece que "Solo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto..." El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma. La exigencia legal de que la situación reflejada en el fichero se la "actual" hace necesario que la actualización del fichero sea permanente, debiendo el acreedor comunicar al responsable del fichero común el dato inexistente o inexacto en el mínimo tiempo posible (la Instrucción antes citada establecía como plazo máximo el de una semana, que también se aplica al fichero del acreedor, y parece que, al no regular nada el Reglamento, esta previsión se puede seguir aplicando).

El incumplimiento de estas obligaciones constituye una infracción sancionable en vía administrativa. En este sentido, tanto la AEPD (Agencia Española de Protección de Datos) como los Tribunales se han mostrado especialmente exigentes con relación a la actualización de estos registros, dada la trascendencia que el figurar en ellos puede tener para el sujeto afectado.

Según el artículo 29.4 LOPD los datos registrados, cuando sean adversos, no se podrán referir a más de seis años. Este es por tanto el plazo máximo de permanencia de los datos en el fichero, siempre, además, que tales datos respondan a la realidad. Hay que distinguir además entre datos adversos, a los que se les aplica el límite temporal de 6 años y los datos que no lo sean (si es que figura alguno en un registro de las características de los que tratamos) a los que se aplican las reglas generales. Las dudas se han planteado con relación a cual debe considerarse el "dies a quo" para el cómputo de este plazo: la fecha de la anotación de la deuda, la última actualización o el vencimiento de la obligación. A juicio de la Audiencia Nacional (entre otras sentencia de 3 de marzo de 2000) el cómputo se debe iniciar el día del vencimiento de la obligación impagada.

Principalmente como contrapartida a la excepción del consentimiento del afectado para ser incluido en el fichero, la Ley le reconoce una serie de derechos (que al mismo tiempo se configuran como obligaciones del acreedor y el titular del fichero común) que le permiten conocer y corregir los datos incluidos en el fichero, así como oponerse a su inclusión o cancelar la misma.

En primer lugar, entre tales derechos del titular-obligación del acreedor o titular del fichero común, está el derecho de información previa a la inclusión.

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento previo de pago, que de no producirse el pago en el termino previsto para ello y cumplirse los requisitos previstos en el art. 38 del RLOPD, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento e incumplimiento de obligaciones dinerarias.

La obligación principal del titular del fichero, cumplidos los requisitos de inclusión, es la notificación de la inclusión. Como sabemos, la inclusión en el fichero no requiere el previo consentimiento del afectado, lo que supone una excepción al principio fundamental que rige con carácter general en materia de protección de datos personales. Como contrapartida a esta restricción de los derechos del afectado, se establecen una serie de cautelas, sustituyéndose la necesidad de consentimiento por el requisito de la notificación posterior de la inclusión al afectado. Conforme al art. 29.2 LOPD, se notificará a los interesados respecto a los que haya registrados datos de carácter personal en ficheros, en el plazo de 30 días desde el registro. En concreto, se notificará una referencia de los datos personales que han sido incluidos, informándole asimismo del derecho que le asiste a recabar la información de la totalidad de los mismos (el art. 40.1 del Reglamento establece lo mismo). Tal previsión legal se completa con lo establecido en el artículo 40 del Reglamento. En el apartado 2 se establece que "*se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores"*.

La notificación deberá efectuarse a través de un medio fiable, auditable, e independiente de la entidad notificante, que le permita acreditar la efectiva realización de los envíos. Esta exigencia normativa responde a las necesidades que la práctica había puesto de manifiesto antes de la regulación reglamentaria, ya que en muchas ocasiones se discutía sobre la prueba de la notificación, pretendiendo la entidad titular del fichero acreditar la notificación con la certificación de su emisión, que se guardaba en un fichero de notificaciones de la propia entidad. Parece que podemos concluir que las certificaciones provenientes de los ficheros de notificaciones no son suficientes para considerar acreditado el cumplimiento de la obligación de notificación, aunque pueden ser tenidas en cuenta, junto a otras formas de prueba, para acreditar el cumplimiento.

No se entenderán suficientes las devoluciones en las que simplemente el destinatario haya rehusado recibir el envío.

Por último, según el Reglamento, si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección se corresponde con la establecida contractualmente y no procederá al tratamiento de los datos sin comprobar este dato. El problema que se plantea es cómo se prueba que se ha realizado esta gestión y, sobre todo, a quien incumbe tal prueba.

La notificación cumple la función principal de comunicar al afectado su inclusión en el fichero, dada la trascendencia que ello puede tener para sus derechos (negativa a contratar de ciertas empresas, denegación de operaciones de crédito etc.). Pero al mismo tiempo, también es un requisito que garantiza al sujeto la posibilidad de ejercitar los derechos de rectificación y cancelación que la Ley le reconoce, además de poder oponerse a la inclusión en el fichero.

Tanto la AEPD, como los Tribunales son sumamente exigentes al comprobar que se ha producido la notificación de la inclusión en el fichero, ya que no se trata de un simple requisito formal, sino del pilar básico que garantiza los derechos de los afectados.

Por último, nuestra legislación garantiza los derechos del titular de los datos para el acceso, rectificación y cancelación de los datos, cuyo ejercicio tanto frente al acreedor como frente al titular de los datos es regulado detalladamente en el RLOPD (vid. los comentarios al Reglamento de Palomar 2008; Martínez 2009; Zabia 2008).

2.3. Responsabilidad por inclusión errónea de datos en ficheros de incumplimiento de obligaciones dinerarias

Una de las cuestiones fundamentales que se plantean con relación a los ficheros a los que nos venimos refiriendo, tanto los de solvencia patrimonial como los de cumplimiento e incumplimiento de obligaciones dinerarias, es la responsabilidad a que da lugar el incumplimiento de los requisitos establecidos en la legislación de protección de datos y especialmente la responsabilidad por la inclusión de datos erróneos en el fichero o la no actualización del mismo (vid. Casado 2003).

Si observamos tanto las resoluciones de la AEPD (en procedimientos sancionadores) como las resoluciones judiciales, es fácil concluir que la mayor parte de las reclamaciones se centran en la inclusión errónea de datos en los ficheros o el mantenimiento en estos de datos que no responden a la realidad (vid. Grimalt 1995). Concretamente, la AEPD ha señalado como supuestos llamativos, por el volumen que suponen, las reclamaciones que se dirigen contra empresas de telefonía; los motivos de la reclamación son principalmente errores en los procesos de facturación, solicitudes de baja de servicio no cursadas, prolongándose la situación de alta, no proceder a la cancelación de la deuda tras el pago de la misma, atribución de la deuda de un cliente a otra persona al incluir en ficheros comunes de incumplimiento de obligaciones dinerarias datos identificativos erróneos y altas fraudulentas.

La cuestión se complica especialmente, habida cuenta que el error o infracción puede provenir de dos sujetos distintos: el acreedor o quien actúa por su cuenta e interés y el encargado del fichero. Es necesario determinar quien debe entenderse responsable de que los datos incluidos en el fichero común sean correctos y de que la información que se conserva esté actualizada (sobre el supuesto concreto del Registro de aceptaciones impagadas, el conocido RAI, vid. Tellez 1999).

Tanto la AEPD como los Tribunales se han esforzado en determinar cuál es el ámbito de responsabilidad de cada uno de los sujetos intervinientes, basándose para ello tanto en las obligaciones que la ley atribuye a cada uno como, especialmente, en el

poder de decisión que tiene cada cual; así, podríamos decir, como principio general, que no se puede hacer responsable a un sujeto de aquello en lo que no tiene poder de decisión. Con carácter general, se han venido utilizando criterios que parten de ciertas premisas.

El acreedor (o quien actúa en su nombre o interés) es responsable (por el incumplimiento de las obligaciones que la ley le impone, según hemos visto) de la veracidad y exactitud de la información que se incorpora al fichero común (debiendo responder por tanto de la concurrencia de todos los requisitos de inclusión), de la rectificación y actualización de estos datos y por último de la cancelación de los mismos, bien porque sean erróneos o por el transcurso del plazo máximo de permanencia establecido en la LOPD.

El titular del fichero está obligado fundamentalmente a notificar al afectado la inclusión en el fichero y garantizar el ejercicio de los derechos de acceso, rectificación y cancelación, así como tratar con celeridad los datos que le son suministrados y de comunicar los nombres y direcciones de los terceros que han consultado la información del interesado, y, en su caso, las valoraciones y apreciaciones que se hayan vertido. Por tanto, responde estrictamente en este ámbito, del incumplimiento de las obligaciones que le son exigibles y, en definitiva, dentro del ámbito de decisión que la ley le permite.

El titular del fichero común no dispone de los datos relativos a la solvencia y crédito incluidos en el fichero, ni tiene otra posibilidad de conocerlos y contrastarlos que el propio acreedor, que es quien se los suministra; por tanto, será este último el responsable de la calidad de los datos y a quien corresponde comprobar su exactitud y actualización. Parece razonable no exigir a un sujeto algo que está más allá de su propia esfera de control; así, en tanto el titular del fichero común actúa de mero agente canalizador de los datos, tampoco responde de su exactitud; será la fuente de donde provienen esos datos, el acreedor, quien deberá asegurar la exactitud y veracidad de los mismos, así como el encargado de su actualización. El acreedor es el único que puede realizar cualquier acto de disposición sobre el dato incluido en el fichero y por tanto es el que se considera responsable a efectos de la LOPD (art. 3 d). El titular del fichero realiza los actos que le autoriza el contrato o convenio firmado con el acreedor que regula el funcionamiento del fichero.

El art. 43 del Reglamento establece la responsabilidad del acreedor o quien actúa por su cuenta o interés, por la inexistencia o inexactitud de los datos facilitados para su inclusión en el fichero.

La entidad titular del fichero común responde de los errores que se hayan podido producir dentro de su esfera de decisión y competencia. Por ello, si el error se ha producido al introducir los datos comunicados correctamente, entonces responde el titular del fichero y lo mismo ocurre en caso de incumplimiento de cualquiera de los

deberes que le incumben, como la notificación de la inclusión (entre otras, sentencias de 9 de mayo de 2003 y 24 de enero de 2003) y facilitar el derecho de acceso informando sobre quien ha incluido los datos en el fichero y remitir al acreedor las solicitudes de cancelación o rectificación presentadas por los interesados, a efectos de que éste compruebe si la información es correcta y en caso contrario ordene su rectificación. Si el acreedor no respondiera en el plazo legalmente previsto de 10 días, deberá cancelar cautelarmente los datos hasta que el acreedor decida sobre su mantenimiento o modificación.

Con todo, hay que tener en cuenta que la responsabilidad a que nos venimos refiriendo se rige por las reglas generales de nuestro ordenamiento jurídico y por tanto, no habiéndose establecido expresamente, no se trata de un caso de responsabilidad objetiva, sino que habrá que juzgar si el sujeto ha actuado con culpa o dolo (vid. Grimalt 1999 y 2011). A este respecto, hemos de destacar que la jurisprudencia es sumamente rigurosa al enjuiciar la diligencia aplicable, exigiéndose a la entidad un "control riguroso": según podemos leer en la sentencia de la Audiencia Nacional de 22 de junio de 2005, que cita las resoluciones anteriores en la materia.

La afirmación tajante de los Tribunales españoles sobre la posibilidad de que la infracción se produzca por simple falta de diligencia, siendo además muy rigurosos al apreciar la existencia de la misma, es muy importante, sobre todo si tenemos en cuenta que la propia AEPD ha puesto de manifiesto que uno de los argumentos utilizado por las entidades sancionadas para oponerse a tal sanción es la falta de culpabilidad, al haberse producido la inclusión del dato inexacto o incorrecto en el fichero por errores informáticos o de procedimiento (por ejemplo la sentencia de la AN de 18 de enero de 2006, en la que el acreedor alega un error informático, defensa muy común).

Además, hay que tener en cuenta que, aunque resulta sumamente útil el régimen sancionador de la LOPD, sobre todo por el control de la AEPD, el informante estará sometido a responsabilidad por aplicación de las reglas generales (responsabilidad contractual, por incumplimiento de las obligaciones legales y, en su caso, responsabilidad extracontractual). Estos sujetos responden por la infracción de las obligaciones que la ley le impone y están sometidos a la responsabilidad administrativa que la Ley establece, pero también son responsable según las reglas de incumplimiento contractual (1101 ss del Código civil), de modo que aunque no estuvieran previsto el régimen sancionador de la Ley, habría igualmente lugar a responsabilidad y tal conclusión, a nuestro juicio, será también aplicable a aquellas infracciones o conductas dañosas que, incumpliendo las previsiones legales, no estuvieran previstas en la ley expresamente y además, las conductas lesivas de los derechos de los afectados que no supongan un específico incumplimiento de las previsiones legales, si las hubiera, darían lugar a responsabilidad extracontractual. Más aún, los remedios generales articulados en nuestro ordenamiento jurídico pueden ser sumamente útiles para lograr la reparación del daño y, al mismo tiempo, conseguir el funcionamiento

correcto de los ficheros; en este sentido, recientemente el tribunal Supremo ha reconocido la existencia de intromisión en el derecho al honor de un sujeto por haber sido incluido erróneamente en un fichero de morosos y declara la correspondiente indemnización por la lesión del derecho al honor, aplicando la Ley Orgánica de Protección del Derecho al Honor, intimidad personal y familiar y propia imagen del año 1982 (sentencia de 24 de abril de 2009) (vid. sobre este tema Macias 2010 y su crítica a la STS de 31 de marzo de 2010 sobre inexistencia de intromisión en el derecho al honor a pesar de la publicación de la condición de moroso). Resulta llamativo que, partiendo del carácter autónomo del derecho a la protección de datos personales, a la postre los Tribunales estén tutelando, de algún modo, este derecho a través de la tutela del derecho al honor y a la intimidad.

3. El "interés legítimo" como legitimador del tratamiento de datos personales

El reconocimiento legal de la existencia de este tipo de ficheros sobre solvencia patrimonial, tanto en nuestro ordenamiento jurídico como en todo el entorno jurídico de la Unión Europea, se funda en admitir que existe un "interés legítimo" que justifica el tratamiento de estos datos y, por ende, tales ficheros.

El reconocimiento de un "interés legítimo" en el tratamiento de estos datos es el elemento legitimador que ha de concurrir. Así deriva de la Directiva 95/46, que no se refiere específicamente a estos ficheros, pero permite que las distintas legislaciones regulen su existencia y características, al amparo del art. 7 f del texto comunitario ("Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva").

Parece comúnmente admitido que existe un interés legítimo en el conocimiento de los datos que afectan a la solvencia y situación económica de los particulares cuando se establece o se pretende establecer una relación económica con una empresa, especialmente si el interesado en tal información ha de asumir, como consecuencia de la relación, un riesgo derivado de la concesión de crédito o de la realización de una inversión. Podríamos concretar este interés legítimo en aspectos como: evaluar el riesgo, prevenir el fraude y evitar la morosidad. Al mismo tiempo el interés en la existencia de tales ficheros es un interés general, en tanto sirven como instrumento al servicio de la agilidad y seguridad de las transacciones comerciales, por ejemplo, facilitando el acceso rápido al crédito (crédito al consumo) sobre la base de la existencia de ciertas garantías básicas para el prestamista.

No cabe duda de la importancia socio-económica de cualquiera de los datos sobre solvencia y crédito susceptibles de ser incluidos en estos ficheros. Lo cierto es que la actividad económica y el comercio actual exigen, por parte de las empresas, lo que podríamos denominar un "control de riesgos": para contratar con determinada persona se ha impuesto la exigencia de saber cuál es la situación económica y patrimonial del contratante, especialmente si la operación económica conlleva algún tipo de financiación. A esta finalidad responden los ficheros de solvencia patrimonial y crédito (vid. sobre estas consideraciones Ferrando 2009).

Precisamente en aras de la seguridad del tráfico mercantil y de la agilidad negocial sacrifica el legislador determinados principios y derechos que rigen con carácter general en materia de protección de datos; así, por ejemplo, resulta llamativo el proceder empresarial que la práctica ha impuesto y que es comúnmente admitido, ya que la decisión empresarial sobre determinada operación o cierto cliente (contratar o no, dar o no crédito, etc.) se basa en la información que obtienen de los ficheros de solvencia patrimonial, cuando por regla general (art. 13 de la LOPD) "Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad"; a pesar de este principio general, se permite la existencia de los ficheros de solvencia patrimonial, destinados, precisamente, a proporcionar un perfil económico de un sujeto, aunque con el límite de que sólo podrán constar en estos ficheros datos de naturaleza positiva. Por un lado, el reconocimiento expreso en el art. 29 de los ficheros de solvencia patrimonial parece excluirlos del ámbito de aplicación del art. 13, pues, como se ha dicho, su propia naturaleza supone la creación de un perfil económico del sujeto en el que se basan las empresas y, en cualquier caso, aun defendiendo la aplicación en estos supuestos del principio general, el problema sería probar, en cada caso, que la decisión se basa exclusivamente en los datos aportados por el fichero.

En la doctrina se ha justificado la actividad que desarrollan las empresas que prestan el servicio de información sobre el crédito de las personas, entendiendo que, la disposición de información relativa la morosidad de las personas (y podríamos añadir que en general sobre su situación económica) contribuye eficazmente a la adopción de decisiones respecto a la operación de que se trate, favoreciendo la seguridad del tráfico jurídico.

En definitiva, la existencia de un interés legítimo en el tratamiento de los datos económicos de los particulares permite su tratamiento sin consentimiento, y, en consecuencia, avala la existencia de los denominados "ficheros de morosos". Esta es precisamente la doctrina que deriva de una reciente sentencia del TJUE, (Tribunal de Justicia de la Unión Europea) de 24 de noviembre de 2011, que resuelve la cuestión prejudicial planteada por el Tribunal Supremo español respecto a la compatibilidad del artículo 10.2 del RLOPD con el artículo 7 f) de la Directiva 95/46/CE (asuntos acu-

mulados C-468/2010 y C-469/2010. Vid., la resolución en http://bit.ly/rpklHP). Esta resolución ha dado lugar a titulares e informaciones periodísticas que pueden resultar llamativas ("Las empresas podrán comercializar datos personales sin pedir permiso". "El Tribunal de la Unión Europea avala los ficheros de morosos"…) y que parecen sugerir que el TJUE avala el tratamiento de los datos económicos de los particulares sin consentimiento y, al parecer, sin límites; desde luego, no es así. Probablemente estos titulares son fruto del desconocimiento de la regulación de la materia, y al mismo tiempo reflejan que la cuestión de fondo fue planteada por la Asociación Nacional de Establecimientos Financieros de Crédito (Asnef) y la Federación de Comercio Electrónico y Marketing Directo (Fecemd), que han transmitido la resolución como un "éxito" de sus planteamientos. Con todo, aun admitiendo tal circunstancia, el concepto de interés legítimo sigue siendo, antes de la resolución y ahora, y a la vista de la Directiva, elemento legitimador ineludible: cuando no exista tal interés legítimo no podrán tratarse datos sin consentimiento del titular.

Ahora bien, en relación a la consulta concreta que se le hace, el Tribunal de la UE considera que la regulación española se ha extralimitado al imponer requisitos adicionales a los que establece la Directiva, ya que el texto europeo establece una armonización completa y no de mínimos. La LOPD ha incurrido en un error al incorporar el artículo 7 f) de la Directiva a nuestro ordenamiento, ya que no contempla el "interés legítimo" como una fuente independiente legitimadora del tratamiento de datos, exigiendo que los datos figuren en fuentes accesibles al público. De igual modo, el Reglamento que desarrolla la LOPD incurre en el mismo error.

Si tenemos en cuenta las consideraciones que hemos venido exponiendo, la sentencia del TJUE no resulta ni sorprendente ni novedosa, solo vuelve a afirmar que, como reconoce la Directiva, la existencia de un interés legítimo permite el tratamiento de datos personales sin el consentimiento de su titular, nada nuevo. La verdadera cuestión, tanto antes como después de la citada sentencia, es determinar cuando existe el interés legítimo.

Conviene recordar además, que según establece el citado artículo 7 f) de la Directiva, y ha recordado el TJUE en la resolución antes citada, el interés legítimo es una causa de legitimación del tratamiento de datos personales, siempre que *no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección…* . Así pues, el tratamiento de datos sin consentimiento del titular solo podrá hacerse cuando existe un interés legítimo y, además, no haya de prevalecer la protección de un derecho o libertad fundamental del individuo. Como establece expresamente la resolución del TJUE: *"38. Dicho artículo 7, letra f), establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado"*.

En definitiva, como precisa el TJUE, un "interés legítimo" no es cualquier interés, será necesario tener en cuenta en cada caso concreto la ponderación de los derechos y libertades de los afectados. En opinión del Tribunal, según pone de relieve Martínez (2012) lo que no encaja con las previsiones de la Directiva es una norma que no permita esa ponderación y cierre completamente cualquier aplicación del principio de interés legítimo en todos y cada uno de los casos ("*49 Habida cuenta de estas consideraciones, procede responder a la primera cuestión que el artículo 7, letra f), de la Directiva 95/46 debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en las fuentes"*).

La doctrina establecida por el TJUE en la sentencia citada ha tenido como consecuencia el pronunciamiento de nuestro Tribunal Supremo para adaptar nuestra legislación. Como es sabido, al resolver una cuestión prejudicial la decisión del TJUE no tiene efecto directo en cuanto a la validez de la norma interna, siendo por tanto la jurisdicción nacional la que tenga qua asumir la decisión y establecer las consecuencias oportunas, declarando, en su caso, la nulidad de la norma. Esto es precisamente lo que ha hecho nuestro Tribunal Supremo en la sentencia de 8 de febrero de 2012, que anula el artículo 10.2.b del RLOPD.

Frente a diversas noticias periodísticas y opiniones que parecían querer ver en estas resoluciones una nueva concepción del derecho a la protección de datos, más permisiva con relación a la excepción del consentimiento, la AEPD fue categórica al considerar que la mera invocación de un interés legítimo no puede considerarse suficiente para legitimar el tratamiento de datos personales sin el consentimiento del afectado, será necesario realizar en cada caso concreto una ponderación entre el interés legítimo de quien va a tratar los datos y los derechos fundamentales de los ciudadanos afectados, con el fin de determinar cuál prevalece atendiendo a las circunstancias concurrentes.

Por otra parte, la aplicación del principio de interés legítimo no excluye, sino que exige la aplicación del conjunto de lo dispuesto por la legislación vigente (tal como puso de relieve la Asociación de Profesionales Españoles de la Privacidad, APEP, en un comunicado acerca de la sentencia).

En especial, se debe resaltar que el mero interés comercial no se puede considerar, por si mismo, interés legítimo; será necesario, tal como se ha señalado, un ejercicio de ponderación de las circunstancias del caso concreto y los derechos en juego. Sin olvidar que, al ser la protección de datos un derecho fundamental, las excepciones al consentimiento habrán de ser consideradas de modo restrictivo.

BIBLIOGRAFIA

Aparicio, J. ed. 2009. *Estudio sobre la LODP.* Cizur Menor (Navarra): Aranzadi.

Casado, O. 2004. "Régimen especial para la actividad de solvencia patrimonial y crédito" en *La protección de datos en la gestión de empresas*. Coordinado por Marzo, A. y Ramos F.M. Monografía de la *Revista Aranzadi de Derecho y Nuevas Tecnologías* 2: 189-209.

Casado O. 2003. «Los ficheros de solvencia patrimonial y crédito». *Alfa-Redi. Revista de Derecho Informático* 57: 1681-1726.

Delgado, J. 2009. "Tratamiento de los ficheros públicos y privados en la LO 15/99 de protección de datos de carácter personal: una visión crítica desde la perspectiva del Derecho Constitucional". Pp 289-312 en *La administración electrónica y la protección de datos*. Coord. Bello, S. y Caro, A.I.

Ferrando, Mª L. 2009. "Denegación de crédito al consumidor y protección de datos personales" *Revista Aranzadi de Derecho y Nuevas Tecnologías* 21: 65-76.

Garriga, A. 2009. *Tratamiento de datos personales y derechos fundamentales.* Madrid. Dykinson.

Grimalt, P. 1999. *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada. Comares.

Grimalt, P. 1995. "El tratamiento automatizado de datos sobre solvencia patrimonial obtenidos de resoluciones judiciales (Comentario a la STS, sala 3ª, de 3 de marzo de 1995)". *Derecho Privado y constitución* 6: 219-226.

Grimalt, P. 2011. "Responsabilidad civil por contenidos en la red: LSSICE y Ley de Prensa y responsabilidad civil por hecho ajeno". Pp 269-279 en *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías,* editado por Cotino, L. Valencia. PUV Publicacions de la Universitat de Valéncia.

Heredero, M. 1983. "La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983". *Documentación Administrativa* 198:139-159.

López, E. y Mora, J. 2009. "Un análisis de la estructura institucional de protección de datos en España: un análisis jurídico y económico de la incidencia de las autoridades de control españolas en la garantía del derecho fundamental de autodeterminación informativa". *Indret. Revista para el Análisis del Derecho* 2: 2-35.

Lucas Murillo, P. 2003. "La primera jurisprudencia sobre el derecho a la autodeterminación informativa." *Datospersonales. Org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* 1: 1-25.

Lucas Murillo, P. 1990. *El derecho a la autodeterminación informativa.* Madrid. Tecnos.

Lucas Murillo, P. 2002. "Las vicisitudes del derecho de la protección de datos personales". Pp. 509-538 en *Estudios en homenaje al profesor Francisco Rubio Llorente,* vol I , edit. por Congreso de los Diputados. Madrid.

Macias, A. 2010. "Inexistencia de intromisión en el derecho al honor a pesar de la publicación de la condición de moroso: análisis de la sentencia del TS de 31 de marzo de 2010" *Actualidad Civil* 14: 1699-1702.

Martinez, R. 2004. *Una aproximación crítica a la autodeterminación informativa.* Madrid. APDCM, Madrid. Civitas.

Martínez, R. 2007. "El derecho fundamental a la protección de datos: perspectivas" *Revista de Internet, Derecho y Política. Universitat Oberta de Catalunya*. Monográfico "III Congreso Internet, Derecho y Politica. Nuevas perspectivas" 5: 47-61.

Martínez, R. 2009. *Protección de datos. Comentario al Reglamento de Desarrollo de la LOPD.* Valencia. Tirant lo Blanch.

Martínez, R. 2012. "Interés legítimo y protección de datos personales en la sentencia de 8 de febrero de 2012 del TS" *elderecho.com* 20 de febrero de 2012.

Palomar, A. y González-Espejo, J. 2008. *Comentario al Reglamento de desarrollo de la LO 15/1999, de 13 de diciembre, de protección de datos de caracter personal (aprobado por RD 1720/2007, de 21 de diciembre).* Madrid. Civitas.

Ramos, A. 2008. "El requerimiento previo a la inclusión de los datos personales en los ficheros de solvencia patrimonial y crédito." *Datos personales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* 35.

Tellez, A. 1999. «La responsabilidad de las entidades de crédito por la inclusión errónea de morosos en el registro de aceptaciones impagadas». *La Ley* 5: 1885-1893.

Troncoso, A. 2010. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Madrid. Civitas.

Villaverde, I. 1994. "Protección de datos personales, derecho a ser informado y autodeterminación informativa. A propósito de la STC254/1993". *Revista Española de Derecho Constitucional* 41:187-224.

Zabia. J. 2008. *Protección de datos. Comentarios al Reglamento.* Valladolid. Editorial Lex Nova.

comunitania
REVISTA INTERNACIONAL DE TRABAJO SOCIAL Y CIENCIAS SOCIALES
INTERNATIONAL JOURNAL OF SOCIAL WORK AND SOCIAL SCIENCES

ARTICULOS/ARTICLES

La participación de las mujeres en las Fuerzas Armadas españolas: de la incorporación a la integración / Women's participation in the Spanish Armed Forces: from incorporation to integration
Yolanda Agudo Arroyo ..... Págs 9-27

Estudio comparativo del consumo de sustancias psicoactivas en adolescentes españoles y europeos / Comparative study of psychoactive substances in Spanish and European adolescents
Francisco Javier García Castilla y Laura Ponce de León Romero ..... Págs 29-49

La práctica del Trabajo Social en salud desde la perspectiva de los modelos de intervención / The practice of Social workers in health care from the perspective of intervention models
Silvia Vázquez González, Blanca Guadalupe Cid de León Bujanos y Josefina Pimentel Martínez .. Págs 51-67

El derecho fundamental a la protección de datos personales y los ficheros privados: el interés legítimo en el tratamiento de datos / The fundamental right of personal and private files protection: the legitimate interest in the data processing
Mª Carmen Plana Arnaldos ..... Págs 69-89

Regulación electoral de los sondeos a pie de urna en España: asignaturas pendientes y obsolescencia ante las nuevas formas de comunicación / Electoral regulation of exit polls in Spain: unfinished topics and obsolescence in the face of new forms of communication
Javier Sierra Rodríguez ..... Págs 91-118

Evolución de la incidencia y preferencia de recursos por parte de los usuarios Dependientes desde 2007 hasta 2013 / Evolution of the incidence and preference of resources by Dependent users from 2007 to 2013
Luis Manuel Rodríguez Otero ..... Págs 119-146

RESEÑAS/REVIEWS

Francisco Gorjón Gómez y Antonio López Peláez (coords.). Estado del arte de la mediación / State of the art of mediation *(por Juan Carlos De Peralta Ortega)* ..... Págs 147-150

Rubén Darío Torres Kumbrián. Comunidades y Mujeres Musulmanas: Diagnósticos sectoriales y premisas epistemológicas y hermenéuticas islámicas reformistas para el Trabajo Social Comunitario / Communities and Muslim Women: Sectorial diagnostics and epistemological, hermeneutics reformist and islamic premises for Community Social Work
(por Laura Martínez Murgui) ..... Págs 151-154

Rubén Darío Torres Kumbrián. Trabajo Social con Comunidades y Mujeres Musulmanas: Premisas de la Intervención para la Plena Pertenencia Social / Social Work with Communities and Muslim Women: Intervention Assumptions for Full Social Membership
(por Eloy Vírseda Sanz) ..... Págs 155-157

editorial UNIVERSITAS
UNED FACULTAD DE DERECHO Departamento Trabajo Social
ISSN: 2173-0512