Universidad de Alcalá

TÍTULO DEL TRABAJO

El tratamiento de datos personales en los registros de incumplimiento de obligaciones dinerarias: los registros de morosos como medio “extraordinario” de cobro

The treatment of personal data in the records of non-compliance with monetary obligations: the debtors lists as an "extraordinary" means of collection

Máster Universitario en

Acceso a la Profesión de Abogado

Autor: D. SERGIO LINARES GARCIA

Tutora: Dra. MÓNICA ARENAS RAMIRO

Alcalá de Henares, 10 de Febrero de 2017

INDICE

RESUMEN

Los ficheros de morosos son un mecanismo cuya única función legal es ofrecer información sobre la solvencia económica de los titulares de los datos inscritos en los mismos. Sin embargo, en la práctica, no es extraño encontrase el uso de los mismos como un medio extraordinario de cobro. Así pues, dicho uso inadecuado puede causar una vulneración al derecho a la protección de datos del deudor, además de vulnerar otros derechos como, por ejemplo, el derecho al honor.

El presente trabajo se dividirá en dos grandes bloques para luego finalizar con unas conclusiones en las cuales se intentará proponer posibles soluciones al uso incorrecto de dichos ficheros. El primero de los bloques versará sobre la situación actual del derecho a la protección de datos y los diversos medios que existen para tutelarlo, mientras que el segundo de los bloques tratará sobre los problemas prácticos que dicho uso puede llegar a causar, centrarnos en el caso de los ficheros de morosos.

PALABRAS CLAVE: registro de morosos, protección de datos, principios de tratamiento, datos de carácter personal, acreedor, deudor.

ABSTRACT

The debtors lists are a mechanism, whose only legal function is to offer information on the economic solvency of the headlines of the data inscribed in the same. However, in the practice, is not odd found the use of the same like a half extraordinary of collection. Like this then, this unsuitable use can cause a violation to the right to the data protection of the debtor, in addition to vulnerary other rights as, for example, the right to the honor

The present work will divide in two big blocks for afterwards finalize with some conclusions in which it will try propose possible solutions to the wrong use of these files. The first of the blocks treated on the current situation of the right to the data protection and the diverse means that exist for tutelary it, whereas the second of the blocks treated on the practical problems that said use can cause, focus on the case of the debtors lists.

KEYWORDS: The debtors lists, protection of data, principles of treatment, personal data, creditor, debtor

I. Introducción.

Nuestro día a día nos lleva inevitablemente a la celebración de múltiples contratos de la naturaleza más dispares para llevar a cabo nuestra vida diaria, pero ¿qué pasaría si en alguno de esos contratos ocurriera un imprevisto que nos impidiera cumplir con nuestra parte del contrato? Asimismo, aunque celebramos contratos de forma cotidiana son pocas las ocasiones en que nos paramos a pensar las consecuencias que nos acarrearía el incumplimiento de las obligaciones pactadas y de las múltiples formas que existen para reclamar su cumplimiento o, en su defecto, el resarcimiento del daño producido por el incumplimiento de la obligación.

En el presente trabajo se va a analizar el uso incorrecto de los registros de morosos como una forma de reclamar el cumplimiento de obligaciones dinerarias, cuyos efectos, en la gran mayoría de las situaciones, resultan ser mucho más perjudiciales para el derecho a la protección de datos del deudor que cualquier otro medio de cobro. Por esta razón, se hará una exposición del actual sistema de tutela del derecho a la protección de datos para después centrarnos en los problemas prácticos que dichos registros pueden provocar con respecto a éste derecho.

II. Marco Jurídico del Derecho de Protección de Datos.

1. Regulación Jurídica.

La regulación jurídica del derecho a la protección de datos se ha ido consolidando tanto en el ámbito internacional como nacional a partir de la segunda mitad del siglo XIX.

1.1. Internacional.

En el ámbito internacional podemos encontrar, aunque no de forma expresa, recogido el derecho a la protección de datos en varias normas internacionales, tales como: la Declaración Universal de los Derechos del Hombre[1] (artículo 12), el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 4 de noviembre de 1950[2] (artículo 8) o el Pacto Internacional de Derechos Civiles y

[1] Declaración Universal de los Derechos del Hombre. Aprobado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948.
[2] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950 (BOE 10 de Octubre de 1979, núm. 243).

Políticos, 19 de diciembre de 1966[3] (artículos 17 y 19). En estas normas se protege la vida privada, en la que se entiende englobado el derecho a la protección de datos Además, debemos recordar el primer instrumento internacional vinculante y especifico sobre el derecho de protección de datos, el Convenio 108 del Consejo de Europa, 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.[4], que regula el tratamiento de datos personales.

1.2. Europea.

El marco jurídico del derecho de protección de datos en el ámbito europeo se sustenta en la actualidad en el artículo 16 Tratado de Funcionamiento de la Unión Europea[5] y en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[6], donde si se regula de forma expresa el derecho. Este derecho a la vez se traslada a los Estados miembros por medio de la trasposición de diversas Directivas, siendo la más importante la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.[7]

No obstante, la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[8] (Reglamento Europeo, en adelante) deroga la Directiva 95/46/C y supone una nueva forma de entender el derecho de protección de datos, al regirse dicho derecho por una norma directamente aplicable en todo el territorio de la Unión Europea. Aunque no será

[3] Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York, el 19 de diciembre de 1966. Instrumento de Ratificación de España de 13 de abril de 1977 (BOE 30 de Abril de 1977, núm. 103).
[4] Convenio 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, hecho en Estrasburgo, el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984 (BOE de 15 Noviembre 1985, núm. 274).
[5] Versión consolidada del Tratado de Funcionamiento de la Unión Europea, de 26 de Octubre de 2012 (Diario Oficial de la Unión Europea, de 26 de Octubre de 2012, núm. C 326).
[6] Carta de los Derechos Fundamentales de la Unión Europea, de 7 de mayo de 2016 (Diario Oficial la Unión Europea de 7 Mayo de 2016, núm. C 202/389).
[7] Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial de la Unión Europea, de 23 Noviembre 1995, núm. L 281).
[8] Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Diario Oficial de la Unión Europea, de 4 Mayo de 2016, núm. 119).

aplicable hasta el 25 de mayo de 2018 ni tampoco será de tan directa aplicación como cabria esperar de un Reglamento, pues se sustenta en gran parte en las especificaciones establecidas por los Estados miembros para completar el marco del derecho a la protección de datos. [9] Así pues, por un lado, seguirá vigente la Directiva 95/46/C hasta mayo de 2018; y por otro, las respectivas normas ya creadas quedan a la espera de un más que posible cambio para adaptarlas al Reglamento.

1.3. Española.

Dentro del ordenamiento jurídico español el derecho a la protección de datos encuentra su fundamento en el artículo 18.4 de la Constitución Española[10] (CE, en adelante), como un derecho fundamental, y es desarrollado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[11] (LOPD, en adelante) y por 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[12] (RLOPD, en adelante). Además de estas normas, en esta materia debemos tener en cuenta la normativa específica a aplicar según el caso concreto, como por ejemplo: la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, reguladora de la Central de Información de Riesgos del Banco de España; o también conocida como CIBER [13] , que se aplicará, por ejemplo, en el caso de incumplimientos de obligaciones con entidades declarantes pues las mismas están obligadas a declarar dichos incumplimientos. [14]

---

[9] Téngase en cuenta en este sentido los Considerando: 8, 10, 19, 41, 53, 119, 121, 128 a 131, 141, 153 y artículos 35, 51 a 53, 58. del Reglamento Europeo, pues en todos ellos se hace referencia o la necesidad de completar la normativa por parte del Estado o la de seguir las normas ya dispuestas para una materia concreta.

[10] Constitución Española, 1978 (BOE de 29 de Diciembre de1978, núm. 31).

[11] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE de 14 de diciembre de 1999, núm. 298).

[12] 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 (BOE de 19 Enero de 2008, núm. 17); y también téngase en cuenta la además la existencia de la Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de informaci6n sobre solvencia patrimonial y crédito (BOE 4 Marzo 1995, núm. 54) cuyo articulado se encuentra en su mayoría recogida en RLOPD motivo por el cual solo va a ser mencionado en este trabajo cuando corresponda.

[13] Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero (BOE de 23 de Noviembre de 2002, núm. 281).

[14] Entidades declarantes: las expresamente recogidas en el artículo 60.1 de la Ley 44/2002, de 22 de noviembre, entendidas como*: el Banco de España, las entidades de crédito españolas, las sucursales en España de las entidades de crédito extranjeras, el fondo de garantía de depósitos, las sociedades de garantía recíproca y de reafianzamiento, los establecimientos financieros de crédito y aquellas otras entidades que determine el Ministerio de Economía y Competitividad a propuesta del Banco de España*.

2. Principios del tratamiento de datos.

Los principios del tratamiento de datos son principios fundamentales que deben seguirse cuando se tratan datos de carácter personal para asegurar el respeto del derecho de protección de datos y evitar así posibles vulneraciones del mismo derivadas del tratamiento de los datos de carácter personal. Además están presentes a lo largo de todo el marco jurídico del derecho a la protección de datos, estableciendo derechos y obligaciones para todos los intervinientes.

En el presente trabajo se tratarán los principios de información, consentimiento, calidad y finalidad, para después, en apartados posteriores, centrarnos en la problemática que puede surgir de la puesta en práctica de dichos principios.

En lo referente al principio de información se encuentra recogido en el artículo 5 LOPD y consiste en el derecho del interesado a ser informado previamente por todo aquel que utilice sus datos de carácter personal sobre el tratamiento de estos (uso, destino, modificación.etc…), además de los derechos y acciones de los que pueda disponer según el caso en cuestión. Ya que, de no disponer de toda la información necesaria para conocer la situación de sus datos personales, el ejercicio del derecho de protección de datos sería inviable, al no poder concretar ni la persona responsable de la vulneración ni las acciones a ejercer en defensa del mismo.

Lo concerniente al principio del consentimiento se encuentra recogido en el artículo 6 LOPD y trata sobre uno de los elementos más importantes del derecho de protección de datos presente en todo el marco jurídico de protección de datos tanto en ámbito nacional como internacional, y cuya ausencia conlleva la vulneración del derecho de protección de datos. Así pues para que el consentimiento sea valido debe ser recogido conforme a los requisitos establecidos en la ley, que puede resumirse, en "*libre, inequívoca, específica e informada*" y a veces escrito, cuando así lo exija la ley.[15]

[15] Artículos 3.h), 6 y 7 LOPD.

Aunque el consentimiento es un elemento fundamental necesario en todo tratamiento de datos personales, pueden existir supuestos en los que se exima del mismo y que vienen establecidos únicamente por la ley como, por ejemplo, lo dispuesto en el artículo 29.2 LOPD referido a los registros de información sobre solvencia patrimonial, objeto de este trabajo.

En lo que respecta a los principios de finalidad y de calidad, los mismos se encuentran estrechamente relacionados y ambos se recogen en el artículo 4 LOPD. Es más, el principio de finalidad viene como consecuencia del principio de calidad y versa sobre el motivo que fundamenta y justifica el tratamiento de los datos. Motivo que debe estar amparado por el consentimiento y, por lo tanto, ser conocido y consentido por el titular de los datos. Esta finalidad, además, debe ser determinada, explicita y legitima.

Por su parte el principio de calidad hace referencia a las características que deben tener los datos personales para que su tratamiento sea válido y no vulnere el derecho a la protección de datos. Con tal fin el principio de calidad establece que los datos de los tratamientos deben ser adecuados, pertinentes y no excesivos, además de exactos y actualizados entre otros.

En el caso del objeto de este trabajo, los registros de morosos, deben hacer referencia a una deuda *"cierta, vencida, exigible, que haya resultado impagada"* además de no tener una antigüedad de 6 años desde la fecha en que fue exigible,[16] y su finalidad es la de, por un lado, asegurar que los datos inscritos sean pertinente para determinar la solvencia económica del titular de los datos y, por el otro, evitar las posibles vulneraciones al derecho a la protección de datos de los titulares de los datos inscritos.

3. Derechos de los titulares de los datos.

Los derechos de los titulares de los datos son el acceso, la rectificación, la cancelación y la oposición y también son conocidos como ARCO. Son la primera manifestación del derecho de protección de datos encaminados a devolver el poder de control sobre sus propios datos a las personas titulares de los mismos.[17]

[16] Artículo 38 RLOPD.

[17] STC 292/2000 de 30 de noviembre, FJ 7º, en el sentido que son derechos reconocidos en dicha sentencia y su ejercicio resulta obligatorio para poder recabar el amparo de los órganos judiciales.

Tal como se deduce por lo expuesto por el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, "*el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales"*[18].

El ejercicio de estas facultades frente al responsable del tratamiento es una condición *"sine qua non"* para poder recurrir al amparo de la Agencia Española de Protección de Datos (AEPD, en adelante) para después poder recurrir a de los órganos judiciales del ámbito contencioso-administrativo, una vez se deniegue el ejercicio de uno de ellos o el interesado no esté satisfecho con la respuesta ofrecida. Cabe mencionar en este punto que su interposición no es necesaria para recurrir al amparo de los órganos judiciales del ámbito civil.[19]

El régimen jurídico de estos derechos se encuentra recogido en la LOPD artículos 13 a 19, 23, 24 y en el RLOPD artículos 23 a 36, 44, 50 y 51. Asimismo, también hay que hacer referencia a la normativa específica que pueda llegar a aplicarse a cada caso concreto como, por ejemplo, en relación con nuestro trabajo, los artículos 64 y 65 de la Ley 44/2002, de 22 de noviembre, para cuando se ejerciten ante el ya citado CIRBE.[20]

Así pues, como el derecho fundamental a la protección de datos es un derecho cuyo único titular son las personas físicas, los derechos ARCO tienen un carácter eminentemente personalísimo, hecho que se hace más patente cuando los artículos 23.1

[18] STC 292/2000 de 30 de noviembre, FJ 6º, último párrafo.
[19] Véase Álvarez Hernando, Javier / Cazurro Barahona, Víctor, *"Practicum Protección de Datos 2015", Aranzadi, Pamplona*, 2014, p. 236.
[20] Ibídem, p. 224.

y 24 RLOPD remarcan tal carácter[21]. Esta característica es importante de resaltar porque de la misma no solo va influir que los derechos ARCO sean válidamente ejercidos, sino que, además, dependiendo del caso podría llegar a producirse una vulneración del derecho de protección de datos si fuesen ejercidos sin los debidos requisitos.

El ejercicio de los derechos ARCO, en consecuencia, consiste en otorgar facultades de control sobre los propios datos del interesado a dicho interesado, tal como se desprende del articulado antes mencionado y de lo expuesto por la Sentencia de la Audiencia Nacional de 19 de marzo de 2014, en su Fundamento de Derecho Segundo (trascrito a continuación): *"...del derecho de acceso, reconocido en el artículo 15 de la LOPD, resulta evidente que tan solo alcanza a los datos personales del titular de aquel derecho o a los de aquellas personas cuya representación ostentase, sin que quepa aceptar que incluye el derecho a acceder a datos de carácter personal de otras personas, pues ello comportaría la vulneración de su derecho fundamental a la protección de datos, consagrado en el artículo 18.4 de la CE".* [22]

Por lo tanto, el hecho de facilitar algún dato en base al ejercicio de alguno de estos derechos (sin la debida comprobación de la identidad del interesado), y facilitar el acceso a la información por quien no es titular de los datos, podría suponer una vulneración del derecho a la protección de datos. En concreto una vulneración de los artículos 10 y 11 LOPD (esto es, del derecho de secreto y la cesión de datos sin consentimiento), consideradas como infracciones graves en los artículo 44.3,d) y k) LOPD, que conllevan una multa de entre 40.001 a 300.000 € según dispone el artículo 45.2 de la ley anteriormente mencionada si el infractor forma parte del sector privado, que suele ser la regla general.[23]

[21] Véanse la STC 292/2000 de 30 de noviembre que no hace mención al derecho de protección como derecho de personas jurídicas, sino que durante toda su explicación lo hace como derecho de las personas físicas; y SAN de 19 de marzo de 2014, FJ. 2º, en donde se expone la doctrina sobre el carácter personal de este derecho.

[22] Véase SAN de 19 de marzo de 2014, FJ. 2º quinto párrafo antes del final; y también Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 208.

[23] Recordamos en este punto que las sanciones por infracciones cometidas por el sector público se rigen por el régimen sancionador de la Administración Pública y no conlleva penas pecuniarias.

Otra cuestión relevante sobre los derechos ARCO, a destacar a raíz de lo anterior, es su profunda relación con el derecho de información previa, un derecho cardinal del sistema de protección de datos recogido en el artículo 5 de la LOPD[24]. Este derecho/principio obliga al responsable o al encargado (en el caso de que dé respuesta bajo nombre y por encargo del responsable) a responder las peticiones sobre datos, estén o no estén los datos del interesado en su fichero, use o no los conductos que haya o no dispuesto, e incluso en el caso de que la petición del interesado resulte ser incompleta o defectuosa está obligado a solicitar del interesado la subsanación de tales defectos. [25]

En lo concerniente a la forma en que debe llevarse a cabo tal solicitud, el marco normativo del derecho de protección de datos (artículos 23 y 24 RLOPD) no exige un excesivo formalismo, pero el RLOPD sí establece en su artículo 25.1, de forma precisa, el contenido de dicha solicitud:

- Nombre y apellidos del interesado
- Fotocopia de su Documento Nacional de Identidad u otro documento equivalente
- Documentación que acredite la representación, en caso de haberla
- Cualquier otro documento que acredite su identidad de forma electrónica o no, legalmente aceptado
- Petición en que se concreta la solicitud
- Dirección a efectos de notificaciones
- Fecha y firma del solicitante
- Documentos acreditativos de la petición que formula, en su caso

Cuestión obligada, resulta, una vez llegado a este punto, tratar sobre los plazos que dispone el responsable o el encargado del tratamiento de los datos para contestar a la solicitud del interesado. Dichos plazos, por regla general, son idénticos para todos los derechos ARCO excepto, en determinadas ocasiones, como es el caso del derecho de acceso, que cuenta con plazos específicos para su estimación y que su futura solicitud haya sido o no estimada. El plazo general, común para todos los derechos ARCO (incluso en el de Acceso en lo que respeta a la ejecución del mismo), es de 10 días a contar desde la recepción por parte del responsable o del encargado de la solicitud hecha por el interesado. Recepción que ha de ser probada junto con el envío por parte del

[24] Véase Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 205.
[25] Ibídem, pp. 212 a 214; y también art. 24.5 RLOPD.

interesado mientras, que la contestación ha de ser probada por el responsable o encargado. [26] No obstante, como ha quedado dicho, en el derecho de acceso, el responsable o encargado tienen un plazo de un mes para contestar al interesado, aunque luego la ejecución se puede dar en los 10 días siguientes, tal como hemos dicho.

Como último punto en común de los derechos ARCO es necesario mencionar que los derechos ARCO, como la gran mayoría de los derechos, no son absolutos y pueden llegar a ser limitados o denegados, tal como dice el RLOPD en su artículo 25.7, por "razones *de seguridad pública en los casos y con el alcance previsto en las Leyes*. Por ello existen muchas leyes que establecen criterios añadidos al procedimiento base para el ejercicio de los derechos ARCO y que habría que tener en cuenta.[27]

Sin ánimo de detenernos en detalle en cada una de estas facultades y sus características, para el trabajo aquí desarrollado, si que tenemos que destacar algunos detalles más.

Así por, ejemplo, en cuanto a la denegación de los derechos ARCO los motivos para poder denegar su ejercicio se encuentran recogidos en el artículo 23 de la LOPD:

- En función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Siendo el único autorizado para esgrimir este motivo las Fuerzas y Cuerpos de Seguridad en referencia a sus respectivos ficheros dentro de sus atribuciones y siempre con el posterior control de la administración de justicia (articulo 22.3 LOPD).
- Cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado está siendo objeto de una actuación inspectora. Para dicho motivo, como resulta evidente de su lectura, solo está capacitado la Hacienda Pública y además se puede comprobar una cierta ambigüedad, al no establecer ningún criterio objetivo para identificar cuando es un "*obstáculo"* el ejercitar un derecho ARCO. Dejando a la

[26] Véase: SAN de 3 de diciembre de 2013, FJ.2 últimos párrafos.
[27] Véase al respecto: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 205 y 206; y en general los procesos específicos en él recogidos.

Hacienda Pública un amplio margen para la denegación de estos derechos sin necesidad de dar una explicación o argumentos claro del porqué. [28]

Aquí conviene mencionar que el derecho de acceso además de tener las causas típicas de denegación de los derechos ARCO, también tiene dos causas de denegación específicas recogidas en el artículo 30 RLOPD. En concreto dichas causas son las siguientes:

1. Cuando el interesado ejercite el derecho de acceso sin haber esperado el plazo de un año y sin contar con un interés legitimo que autorice la interposición. Dicho de otro modo el interesado ejercitó un derecho de acceso que fue aceptado o denegado y posteriormente sin haber esperado el plazo de un año y sin tener interés legítimo que justifique dicha actuación interpone por segunda vez el derecho de acceso.
2. Cuando una ley o una norma de Derecho comunitario de aplicación directa lo permita o cuando las mismas impidan al responsable del fichero la revelación de esos datos personales.

Al igual que con el derecho de acceso el derecho de cancelación cuenta con la causa genérica para su denegación recogida en el artículo 33.2 RLOPD, pero además cuenta con otra causa recogida en el artículo 33.1 de la misma norma, consistente en la posibilidad de denegar la cancelación cuando aún no haya pasado el plazo de bloqueo establecido por la norma aplicable al caso, o bien la relación contractual que justificó el tratamiento de los datos así lo requiera. En este sentido, se hace necesario tratar, para el tema que también nos ocupa, el principio de conservación de datos, recogido tanto en el articulo 4.5 LOPD como en el articulo 41 RLOPD, y que versan sobre la obligación de conservar los datos de carácter personal por parte del responsable del tratamiento por el tiempo estrictamente necesario para conseguir el fin, para el cual fueron recopilados o, en su defecto, para responder sobre las posibles vulneraciones derivadas de su tratamiento.

Asimismo, dentro del presente trabajo, el derecho de cancelación (y, por ende, el bloqueo) adquieren una gran importancia pues representan no sólo el poder de control que tienen los titulares de los datos sobre sus propios datos, sino que, demás, son un

[28] Ibídem: p. 206.

elemento clave para el respeto del principio de conservación y la tutela del derecho a la protección de datos.[29]

Para acabar, en relación a los derechos de los titulares es necesario hacer una referencia al caso específico del CIBER recogido en los artículos 64 y 65 de la Ley 44/2002, de 22 de noviembre, los cuales establecen, por un lado, un plazo de conservación de datos de 10 años (artículo 64 de la Ley 44/2002, de 22 de noviembre) y, por el otro, dos tipos diferentes de procesos de tutela de los derechos ARCO dependiendo de si los datos inscritos en el CIBER fueron hechos de forma voluntaria o obligatoria (artículo 65 de la Ley 44/2002, de 22 de noviembre).[30] Así pues, los procesos en que los datos fueron inscritos de forma voluntaria el ejercicio de los derechos ARCO no distará mucho del proceso normal, mientras que en el caso de que los datos fueran inscritos de forma obligatoria el ejercicio de los derechos ARCO se verá alterado, puesto que en ésta situación el plazo de contestación es de 15 días y el responsable del CIBER sólo actúa de intermediario entre el titular de los datos y las entidades declarantes que inscribieron los datos.

4. Obligaciones de los responsables de los datos.

Las obligaciones de los responsables de los datos son velar por el cumplimiento de los derechos de los titulares de los datos (los derechos ARCO, entre otros) y asegurase que los datos sean tratados de acuerdo con los principios del tratamiento. De entre estas obligaciones es conveniente resaltar la obligación de inscripción del fichero, responder a las solicitudes del ejercicio de los derechos ARCO y las medidas de seguridad para proteger los datos.

En lo que respecta a la obligación de inscripción de ficheros es una regla general para todo responsable de los datos proceder con la inscripción en el Registro General de la AEPD. Esta obligación rige para todo responsable del fichero excepto para los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, entendidas éstas como las relativos al marco

[29]Téngase en cuenta que sobre este tema se tratara más en profundidad dentro del apartado III.3.2 *"En relación con el derecho de los titulares especial mención al derecho al honor"* por su profunda relación con la figura del bloqueo.

[30] Téngase en cuenta a este respecto que el ejercicio del derecho de oposición está explícitamente excluido del ámbito del CIBER, tal como, manifiesta el artículo 59.3 de la Ley 44/2002, de 22 de noviembre.

de la vida privada o familiar de los particulares, los amparados bajo normas de protección de datos de materias clasificas; los relacionados con terrorismo o delincuencia organizada (siempre, y cuando, informen de su existencia, características y finalidad a la AEPD). Con la aprobación del nuevo Reglamento Europeo la continuidad de este requisito es incierta, pues no está recogido expresamente en el Reglamento Europeo, que pretende reducir los trámites administrativos. [31]

El proceso se encuentra regulado en los artículos 52, 53 y 130 a 135 del RLOPD y se inicia, como regla general, mediante una notificación dirigida al Registro General de la AEPD, previa a la creación del fichero, excepto si es un fichero de "*titularidad pública"* en cuyo caso la notificación es posterior a la publicación en el BOE de la disposición que lo habilite. [32]

El modelo y contenido de lo que debe incluirse en la notificación es proporcionado por la AEPD, que, en todo caso, tiene todos los datos referidos tanto al responsable del fichero como el tipo de datos y procesos por él utilizados. Una vez recibida la notificación la AEPD contará con un plazo de un mes para dictar y notificar resolución acordando o denegando la inscripción. Si no responde en ese plazo se entenderá como un silencio positivo.

Por otro lado, en relación con la contestación al ejercicio de los derechos ARCO, ya hemos indicado en el apartado anterior las obligaciones del responsable (o, en su caso, del encargado que trabaje por su cuenta). A ello nos remitimos.

Finalmente, en lo concerniente a las medidas de seguridad, éstas se encuentran reguladas en los artículos 9 LOPD y 79 a 114 RLOPD y establecen una obligación de resultado, pero no necesariamente absoluta.[33]

---

[31] Téngase en cuenta a este respecto que el Reglamento (UE) 2016/679 intenta consolidar el derecho de protección de datos a nivel europeo y el hecho de que algunas Agencias cuenten con el mecanismo de la inscripción y otras no puede ir en contra de este fin. Por esta razón, es muy posible que la obligación de inscripción acabe desapareciendo con el Reglamento.

[32] Véanse al respecto los artículos 20.1 y 21 LOPD. Además la definición recogida en el artículo 5.1.m) RLOPD, que puede resumirse en: fichero creado por entidades o administraciones publicas bajo el ejercicio de sus funciones y para satisfacer las mismas. Por último, téngase en cuenta que pueden existir ficheros privados pertenecientes a Administraciones Publicas.

[33] Véase al respecto Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 266 y ss., en concreto los fragmentos de las SAN de 25 de febrero de 2010 y SAN de 29 de noviembre de 2013 recogidas en dicho capitulo.

Las medidas de seguridad se dividen en 3 niveles (básico, medio y alto) dependiendo de la naturaleza de los datos tratados en el fichero, siendo éstas acumulativas en el paso de un nivel a otro. Así pues, los ficheros de nivel básico son todos aquellos que traten sobre datos de carácter personal, tal como establece el artículo 81.1 RLOPD. Los ficheros de nivel medio son todos aquellos que se encuentren recogidos en el artículo 81.2 RLOPD, tales como los relativos a la comisión de infracciones administrativas o penales, los de prestación de servicios de información sobre solvencia patrimonial y crédito, los de las Administraciones tributarias en relación con el ejercicio de su potestad tributaria, los de las entidades financieras para finalidades relacionadas con la prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social en relación con el ejercicio de sus competencias, los de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, y aquéllos que contengan un conjunto de datos de carácter personal que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Para acabar con la clasificación, los ficheros de nivel alto, tal como dispone el artículo 81.3 RLOPD, son aquellos que contengan o refieran información relativa a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, datos recabados para fines policiales sin consentimiento de las personas afectadas o datos derivados de actos de violencia de género.

Por consiguiente, en el caso que nos ocupa sobre los registros de morosos, el nivel de las medidas que deben adoptar, tanto responsable como encargados, es un nivel medio al que además se une las medidas de nivel bajo presentes en todos los ficheros.[34] Por consiguiente, en el presente apartado de medidas de seguridad no se tratarán las medidas de nivel alto (por no ser aplicables, como regla general, a los ficheros impagos).

Las medidas de nivel básico se encuentran reguladas en los artículos 89 a 94 RLOPD, y recogen una serie de requisitos mínimos:[35]

- Definir con claridad tanto funciones como las obligaciones del personal, en especial de aquellos que tengan que manejar datos de carácter personal, estableciendo además perfiles de usuarios concretados que permitan el acceso a datos de carácter

[34] Artículo 81.2.b) RLOPD.
[35] Véase al respecto Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 287 y ss., en cuanto a las medidas de seguridad y también en ese mismo libro, pp. 317 y ss. referido a las incidencias, en concreto el esquema explicativo de las incidencias.

personal únicamente en la medida de lo necesario para el cumplimiento de sus funciones.

- Crear un *fichero de incidencias* en donde se recoja como contenido mínimo: tipo de incidencia, momento de producción o detección, persona que lo notifica, a quién se notifica, efectos provocados por la incidencia y las medidas aplicadas para corregirla.
- Verificar el acceso a los datos personales por medio de los perfiles y asegurarse de su efectiva gestión al mismo tiempo que se establecen los sistemas necesarios para asegurar la correcta identificación de usuario y perfil. Todo bajo la supervisión de una persona expresamente autorizada para gestionar y modificar los perfiles.
- Asegurarse de la correcta gestión de los documentos con datos personales, independientemente de su formato, controlando tanto su tratamiento a nivel interno (salidas, entradas de datos.etc.) como su posterior destrucción cuando ya no sean necesarios.
- Establecer un proceso para la recuperación de datos o la elaboración de copias de seguridad de forma periódica, para favorecer la recuperación de los datos en caso de incidencias o pérdidas.

Las medidas de nivel medio se encuentran reguladas en los artículos 95 a 100 RLOPD y, salvo algunas excepciones como la obligación de designar responsable de seguridad o la obligación de someterse cada dos años a una auditoria, no son más que pautas para reforzar las medidas básicas. En concreto dichas medidas establecen:[36]

- La obligación de designar a un responsable de seguridad para coordinar y controlar la correcta aplicación de las medidas de seguridad, sin que en ningún caso dicha designación exonere al responsable del fichero de su responsabilidad en cuanto al tratamiento de los datos personales.
- Pasar una auditoría bienal cuyo informe sobre el estado de la protección de datos en el fichero será analizado por el responsable de seguridad para que pueda dar sus conclusiones al responsable del fichero y éste decida las medidas adoptar en consecuencia. Además, los informes serán conservados por el plazo de dos años para ser puesto a disposición de la AEPD, si ésta los solicitase.

[36] Ibídem: p. 286, en referencia al responsable de seguridad y pp. 323 a 335 en relación con la auditoria, con especial atención al listado de preguntas propuesto por la AEPD recogido en las pp. 326 a 334.

- La creación de un sistema de registro tanto de entrada como de salida de soportes o documentos, que permita conocer los datos relacionados con la entrada o salida (tipo de soporte, interviniente, fecha, hora, destinatario. etc.…).
- La creación de medidas o procesos que eviten los intentos de acceso no permitidos de forma reiterada a los sistemas informáticos además de restringir el acceso físico a aquellos equipos con información personal.
- Dentro del registro de incidencias consignar, además de los datos establecidos en las medidas básicas, los datos referidos al proceso utilizado para la recuperación, la persona que lo ejecutó, los datos restaurados y, si los hubiera, aquellos datos que tuvieron que guardarse en otro formato.
- La solicitud previa al responsable del fichero para proceder a un proceso de recuperación de datos.

Todas estas medidas de seguridad son recogidas en un documento de uso interno conocido como *"documento de seguridad"*, elaborado por el responsable del fichero o tratamiento. Sobre este documento el marco jurídico de protección de datos deja una gran libertad a la hora de elaborarlo. Sólo se dedica a imponer una serie de contenidos mínimos recogidos en el artículo 88 RLOPD, referidos tanto a la estructura del fichero como a las medidas de seguridad antes mencionadas, además de algún otro proceso que el responsable o el encargado hayan elaborado para asegurar la protección de los datos personales.

5. Garantías del Derecho.

El derecho a la protección de datos personales como todos los derechos fundamentales cuenta con la tutela de los órganos jurisdiccionales, además de la ofrecida por la Agencia Española de Protección de Datos.

En referencia a la tutela ofrecida por los órganos jurisdiccionales se encuentra presente en todos los ámbitos jurisdiccionales, aunque en el presente trabajo nos vamos a centrar en el ámbito contencioso-administrativo y el ámbito civil por entender que son los más relacionados con el objeto del trabajo.

La protección ofrecida por el ámbito administrativo y en el contencioso-administrativo es la más relevante por ser la más directamente relacionada con la tutela ejercida por la

AEPD, y por ende de su potestad sancionadora[37]. Dicha tutela es ejercida por la Audiencia Nacional al ser la competente para conocer de las resoluciones de la AEPD. Contra la resolución de la Audiencia Nacional, como es lógico, se podrá recurrir ante el Tribunal Supremo cuando las condiciones del caso lo permitan.

En cuanto a la protección en el ámbito civil se puede considerar que es complementaria de la anterior, en tanto que se reclaman daños y perjuicios por el mal uso o uso ilícito de los datos. No obstante, esta es una cuestión en la que se profundizara más adelanté en el trabajo.

En lo que respecta a la AEPD es la principal garante del derecho a la protección de datos en España, con la correspondiente supervisión por parte de los órganos judiciales. Por medio de Informes jurídicos y los procedimientos recogidos en el Titulo IX del RLOPD, que se plasman en sus resoluciones al tutelar el derecho, la AEPD garantiza el derecho de protección de datos.

No obstante, a pesar del amplio abanico de mecanismos con los que cuenta la AEPD para tutelar el derecho a la protección de datos, en el presente trabajo nos vamos a centrar en su potestad sancionadora y en otros mecanismos que podrían mejorar su cumplimiento como son los llamados Códigos Tipo. [38]

El procedimiento de defensa del derecho a la protección de datos en cuanto a la denegación del ejercicio de los derechos ARCO se encuentra recogido en los artículos 117 y siguientes RLOPD, y tiene como finalidad la tutela de dichas facultades, por medio del siguiente procedimiento:

1. Se inicia con la denuncia por parte del interesado donde expone con claridad el contenido de la misma y los preceptos que considera vulnerados porque el responsable del tratamiento no ha dado respuesta al ejercicio del derecho correspondiente.

[37] Tenga sé en cuenta, además, en este punto, la potestad de la AEPD para el inmovilizado de ficheros, recogida en el artículo 121 RLOPD.

[38] Véase al respecto, artículos 32 LOPD y artículos 71 a 78 y 145 a 152 RLOPD, en cuanto a la regulación de los códigos tipos y también; téngase en cuenta, además, que con la aprobación del Reglamento Europeo 2016/679 la AEPD tendrá que reformular sus funciones y, por tanto, sus mecanismos de tutela del derecho de protección de datos, debido al cambio sustancial que dicho Reglamento representa.

2. La AEPD da traslado de la denuncia al responsable del fichero para que formule alegaciones en el plazo de 15 días.
3. La AEPD resuelve una vez pasado dicho plazo, con o sin respuesta por parte del responsable, en base a informes previos, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y, nuevamente, del responsable del fichero.
4. Si la resolución resulta estimatoria, el responsable tiene un plazo de 10 días para ejecutar el derecho tutelado dando cuenta por escrito a la AEPD. En caso de que no se hubiera hecho resolución expresa y motivada, en el plazo de 6 meses se entenderá estimada por silencio positivo.

Así pues, en principio, y como regla general, la resolución de este proceso no conlleva ninguna sanción ni tampoco conlleva el inicio de un procedimiento sancionador. Únicamente declara si ha sido o no vulnerado un derecho ARCO y obliga a quien lo haya vulnerado a dar una respuesta correcta sobre dicho derecho.[39]

La potestad sancionadora se recoge en los artículos 48 y 49 LOPD y 120 a 129 RLOPD y es quizás una de las facultades más importantes, y efectivas, con las que cuenta la AEPD para defender el derecho a la protección de datos, mediante la imposición de cuantiosas multas que oscilan entre los 900 € como mínimo y los 600.000 € como máximo (que podrán llegar en un futuro, a raíz de la aprobación del Reglamento, a la cantidad de 20.000.000 € o un tanto por cierto en el caso de empresas, cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía).

En lo relativo al procedimiento sancionador sigue las bases del procedimiento común recogido en la Ley 39/2015[40], pero con las especialidades impuesta por los artículos 120 y siguientes RLOPD. Así pues las especialidades impuestas por esos artículos son las siguientes:

[39] Sobre este respecto véase: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 491, en concreto cuándo especifica que es la AEPD quien decide cuando se inicia un proceso sancionador y no las peticiones de los interesados.
[40] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE núm. 236, 2 de Octubre de 2015).

- En caso de iniciar actuaciones previas, éstas no podrán superar los doces meses de duración bajo pena de caducidad.
- El acuerdo de inicio deberá contener como mínimo los requisitos del artículo 127 RLOPD, esto es, la identificación de los presuntos responsables; descripción sucinta de los hechos imputados, posible calificación y sanción no vinculante; órgano competente; posibilidad de reconocer los hechos y derechos del responsable, entre otros más.
- El plazo para resolver este proceso sancionador, bajo pena de caducidad, es de 3 meses prorrogable otros 3 meses como máximo, pues el artículo 48 LOPD deja las especificaciones del proceso sancionador al RLOPD, que a su vez en su artículo 128 remite a la norma que regule el procedimiento administrativo. En este caso en cuestión dicha norma es la Ley 39/2015, en donde establece en su artículo 21.2 la obligación de responder en el plazo de 3 meses y en su artículo 23 la posibilidad de prorrogarlo otros tres meses.

Finalmente, existe un tipo de medidas a través de las cuales se favorece la protección del derecho a la protección de datos. Estas medias son los llamados "código tipos".

Los códigos tipos se encuentran regulados en los artículos 32 LOPD y 71 a 78 y 145 a 152 RLOPD y son normas creadas por los responsables del tratamiento tanto públicos como privados de un determinado sector, con el objeto de facilitar y asegurar el cumplimento de la normativa de protección de datos en el sector o ámbito del responsable o responsables de tratamiento que lo promuevan. Estos son mecanismos de autorregulación, dejando en manos de los responsables del tratamiento los medios encaminados a su cumplimiento.

Así pues, la elaboración de los códigos tipo es relativamente rápida (pues su proceso no puede superar los 6 meses), tiene carácter voluntario y en ningún caso podrá sustituir o contradecir a la normativa vigente al respecto. [41]

[41] Véase al respecto, Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 444 y ss.

Para acabar, es conveniente resaltar la influencia que tiene la AEPD en el proceso de elaboración de los códigos tipos, pues puede llegar a imponer su criterio en dichos códigos y parar el proceso de elaboración por medio de diversos requerimientos.[42]

Creemos que los códigos tipos pueden ser un buen mecanismo de garantía del derecho porque permiten establecer criterios adicionales, o concretar los ya existentes, sin la necesidad de tener que pasar por un arduo proceso legislativo para introducir o cambiar criterios. Además, por un lado, permite la creación de normas basadas en la práctica de del ámbito donde deben ser aplicadas (pues los responsables del tratamiento que las elaboran son conocedores de la práctica de su ámbito y, por ende, de las dificultades del mismo) y, por el otro, permite adaptar la normativa a las características concretas del ámbito donde debe ser aplicada.

Asimismo, dichos códigos tipos podrían mejorar el funcionamiento de los ficheros, estableciendo criterios y medidas que impusieran o reforzaran un correcto control previo de los datos antes de inscribirlos, que versaran tanto sobre las características de los datos como sobre el procedimiento a seguir para inscribir.

Con respecto a los criterios que los códigos tipos podrían establecer, estos podrían ser unos ejemplos:

- El establecimiento de una cuantía mínima para inscribir una deuda, pues, como ya se ha comprobado a lo largo del trabajo, los acreedores suelen utilizar esta práctica para ahorrarse los gastos que conllevaría reclamar judicialmente las cantidades menores. Por lo tanto, imponiendo un mínimo se eliminarían esta clase de inscripciones.

- La imposibilidad de inscribir deudas procedentes de obligaciones accesorias cuando la principal siga vigente y se continúe haciendo frente a sus pagos de forma periódica, al menos, que la cantidad adeudada de la accesoria sea superior a la principal. Con ello se intenta evitar, al igual que lo anterior, que los acreedores intenten usar los registros como medio para ahorrarse los gastos judiciales, además

[42] Ídem.

de dar una información más fiable sobre la vida contractual de la obligación, pues carece de sentido inscribir deudas de obligaciones accesorias cuando la obligación principal sigue estando al corriente de pago y sin incidencias (a aparte de que inscribir una obligación accesoria seria, se quiera o no, condenar todo el negocio jurídico al desprestigio del incumplimiento[43]).

- La imposibilidad de inscribir deudas, las cuales, o distorsionen la cuantía adeudada por el incumplimiento de la obligación, o su fundamento diste mucho del objeto perseguido por el fichero, como, por ejemplo, las cláusulas penales, cuya cuantía distorsiona la cantidad verdaderamente incumplida y su fundamento se sustenta en castigar el incumplimiento.

- En el caso de obligaciones de tracto sucesivo o continuado, sólo se podrían inscribir a partir de un determinado incumplimiento (preferiblemente entre el 3º y el 4º), pues inscribir el primero no aporta gran información sobre el negocio jurídico.

Por otro lado, en relación con las medidas a implantar para un correcto funcionamiento de este tipo de ficheros en cuanto al proceso de inscripción y el ejercicio de los derechos ARCO, éstas podrían ser unos ejemplos:

- Establecer un procedimiento claro para el ejercicio de los derechos ARCO y la comunicación entre el titular y el responsable o, al menos, las bases y las opciones disponibles para llevarlos a cabo.

- Requerir la documentación necesaria que demuestre el cumplimento de los requisitos legales para poder inscribir los datos, o, como mínimo, el requerimiento de pago. El resto de requisitos, se quiera o no, hacen referencia a la existencia o no de la deuda y los únicos competentes para conocer y decidir sobre tal cuestión son los órganos judiciales.

[43] Téngase en cuenta, que tal como está establecido actualmente el registro de moroso, no se hacen distinción entre incumplimientos, por esa razón, el inscribir un incumplimiento de una obligación accesoria (quizás hasta ajena al fin buscado por la relación contractual) sería igual que inscribir el incumplimiento de la obligación principal.

- Establecer un periodo cautelar, antes de publicar los datos inscritos, que empezaría cuando el acreedor proporcionare los datos y acabare pasado un mes desde que el titular de los datos fue notificado por el registro y éste no contestó (o se tuvo constancia de su rechazo)

    - En caso de contestación por parte del titular se decidiría de acuerdo a las pruebas aportadas por ambos.

    - En caso de no contestar el titular en el plazo de un mes desde que se le comunico, o se tuvo constancia de su rechazo, se publicarían los datos.

- Durante todo el periodo cautelar previo a la publicación, los datos estarían bloqueados.

- Una vez inscritos los datos no sólo informar a los titulares de los datos de los mínimos legales exigidos, sino que, además, se les proporcione información sobre lo que significa que sus datos estén inscritos en un registro de morosos y las posibles repercusiones que ello puede provocar.

- Informar a aquellas personas que visualizaron los datos, de la cancelación de los mismos. Cuando dicha cancelación, no venga, o bien por haber sido pagada la obligación, o bien por haber pasado el tiempo máximo de conservación de los datos.

Asimismo, con el establecimiento de todos estos criterios se deberían parar o, al menos, reducir situaciones tales como la ocurrida en la Sentencia de Tribunal Supremo del 6 de marzo del 2013, en donde el incumplimiento de una obligación accesoria (con una más que dudosa vinculación con la principal) produjo un desprestigio igual al que hubiera causado el incumplimiento de la obligación principal.

III. Un problema concreto: los registro de incumplimiento de obligaciones dinerarias: los ficheros de morosos.

Antes de empezar a tratar sobre los registros de incumplimiento de obligaciones dinerarias debemos mencionar que la LOPD recoge dos tipos diferentes de ficheros que suelen ir de la mano o juntos casi siempre en su artículo 29, los ficheros sobre solvencia patrimonial y crédito, y los ficheros de cumplimiento o incumplimiento de obligaciones dinerarias, también llamados; registros de morosos.[44]

Así pues, el presente trabajo tiene como objeto los ficheros de cumplimiento o incumplimiento de obligaciones dinerarias (registro de morosos, en adelante), por lo tanto, en lo referente a los ficheros de solvencia patrimonial y crédito no se va a hacer más que una leve referencia a los mismos.

Los ficheros de solvencia patrimonial y crédito proporcionan información positiva sobre la capacidad económica del titular de los datos, es decir, hacen referencia a la capacidad económica del titular de los datos en función de su solvencia patrimonial y no por medio de obligaciones incumplidas. Así mismo, este tipo de ficheros pueden obtener la información de registros, fuentes accesibles al público[45], del titular de los datos o con su consentimiento.[46]

En la práctica los ficheros de solvencia patrimonial y crédito suelen pertenecer a empresas especializadas, cuya actividad consiste en ofrecer información patrimonial sobre empresas o particulares y están presentes en todos los ámbitos, aunque es en el ámbito bancario donde tienen mayor presencia. La inscripción en éste tipo de ficheros

[44] Véanse al respecto: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 521, y también; Informe Jurídico 0237/2009, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 1.

[45] Fuente de acceso público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación y más concretamente, única y exclusiva, aquellos que marca la ley de forma expresa en los artículos 3.j) LOPD y 7 RLOPD. Estos son censo promocional; regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, guías de servicios de comunicaciones electrónicas; en los términos previstos por su normativa específica, listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre título; profesión; actividad; grado académico; dirección e indicación de su pertenencia al grupo, diarios y boletines oficiales y los medios de comunicación.

[46] Véanse: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p.521 y también; Informe Jurídico 0237/2009, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 1.

cuando se hace con esa finalidad y de forma voluntaria por las personas jurídicas o físicas involucradas no conlleva ningún descrédito, es más, dichos ficheros son utilizados por los titulares de los datos para dar a conocer su solvencia económica a terceros y así facilitar la celebración de relaciones contractuales, como, por ejemplo, un arrendamiento o un crédito.

En este tipo de ficheros los datos de carácter personal que no procedan ni de los registros ni de las fuentes accesibles al público deben contar obligatoriamente con el consentimiento del titular de los datos.[47] Máxime, cuando suele ser el propio titular, quien proporciona los datos para dar la apariencia de solvencia y facilitar así posibles concesiones de crédito.[48]

1. Concepto.

Centrándonos en los registros de morosos, éstos se encuentran regulados en los artículos 29.2 LOPD y 37.3 a 44 RLOPD y, al igual que sucede con los ficheros de solvencia patrimonial y crédito, no cuentan con una definición concreta establecida por el marco jurídico de protección de datos, sino que extraeremos su definición por medio de los preceptos que los regulan.

Así pues, con base a los artículos que regulan los registros de morosos podemos decir que éstos son ficheros de titularidad privada que se nutren con la información proporcionada por acreedores, o por quien actuó en su cuenta o interés, sobre el incumplimiento o cumplimiento de obligaciones dinerarias, producidos por los titulares de los datos, y cuyo único fin es enjuiciar la solvencia económica de los titulares de los datos.[49]

En la práctica estos ficheros suelen depender de un conjunto de empresas (entidades bancarias, empresas de prestación de servicios telefónicos, suministradora de energía, etc.) con sus propios ficheros de clientes (o clientes deudores, para ser más exactos),

[47] Véase: Informe Jurídico 0144/2012, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 1 y 2.
[48] Véase: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p.521
[49] Téngase en cuenta sobre este respecto que, aunque, pueden llegar a existir ficheros de moroso de titularidad pública como sucede en el caso de Francia y Portugal, en el caso de España los preceptos que regulan dichos ficheros lo hacen en referencia al ámbito privado. y véase además; Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 524.

que se asocian entre sí, para proporcionar información sobre el incumplimiento de sus clientes a un único fichero independiente conocido como *"fichero común"* o registro de morosos perteneciente, al igual que los ficheros de solvencia patrimonial y crédito, a empresas especializadas en ofrecer servicios de información sobre el patrimonio y la capacidad económica de empresas o particulares. La idea es que a través de dicho fichero, una empresa pueda disponer de los datos sobre los incumplimientos de obligaciones que hayan sido inscritos por otras empresas que puedan tener el mismo deudor u otros.[50]

Lo que se produce en la práctica es que las empresas que tienen clientes morosos, ceden los datos de los mismos a otra empresa que se encargan de gestionar sus recobros y que ofrece información financiera sobre los mismos.

Por consiguiente, los registros de morosos dan publicidad de los incumplimientos de los titulares de los datos, sin su consentimiento, con base únicamente en los datos ofrecidos por los acreedores (los iníciales responsables de los tratamientos de los datos personales de los deudores). Presuponen así, y provocan que el titular de los datos tenga una apariencia de incumplidor, lo que le imposibilitará el acceso a créditos futuros y advierte a todo aquel que lo consulte de tal hecho.

En consecuencia, podemos deducir que los registros de morosos son un mecanismo para comprobar la solvencia económica de los titulares, basada únicamente en una información negativa de los titulares de los datos (el incumplimiento de las obligaciones), proporcionada de forma unilateral por los acreedores de estos (sin el consentimiento del titular y sin posibilidad de contrastarlo con otra fuente). Y que, además, tiene el añadido de evitar el acceso al crédito por parte del titular de los datos, aparte de disuadir a terceros a entablar relaciones contractuales con los mismos, debido al incumplimiento inscrito de la obligación dineraria.

[50] Véase: Hualde Manso, María Teresa, "Ficheros de morosos, nulidad del Reglamento de Protección de Datos y derecho al honor". *Aranzadi civil-mercantil. Revista doctrinal*, Nº. 8 (diciembre), 2013, pp. 50 y ss.

2. Sujetos intervinientes.

2.1. Titulares de los datos.

Los titulares de los datos son aquellas personas a las que se refieren los datos de carácter personal o, dicho de otra manera, aquellas personas sobre las que versan los datos y pueden llegar a ser identificados por éstos. Así pues, amparados por el derecho a la protección de datos, los titulares de los datos son quienes, en última instancia, tienen el control sobre sus datos y deciden sobre si son tratados o no. Así lo declaró el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre: "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero […], o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales,[....] se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*".[51]

No obstante, en aquellas situaciones en las que la Ley exonere del requisito del consentimiento, el titular de los datos sigue teniendo un cierto control sobre sus datos, pues debe ser informado sobre tal hecho, además, de los derechos de los que disponga en su caso.[52] En el caso de los ficheros de morosos, los titulares de los datos serían "los morosos" o personas que han incumplido la deuda.

2.2. Responsable del Tratamiento y Encargado

La figura del responsable del tratamiento encuentra su definición, junto con la figura del responsable del fichero, en las definiciones recogidas tanto en el artículo 3.d) LOPD como en el artículo 5.1.q) RLOPD, trascrita esta última a continuación, por ser la más

[51] STC 292/2000 de 30 de noviembre, FJ 7º.

[52] Véase a este respecto: STC 292/2000 de 30 de noviembre, FJ 10º y 11º; en cuanto a los límites y garantías que debe proporcionarse al limitar el derecho fundamental a la protección de datos.

completa: "*Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente…".* La normativa vigente suele tender a identificar ambas figuras. Y la relevancia de su distinción en la práctica es prácticamente inexistente. Así ambas figuras deben cumplir con las obligaciones impuestas por el marco normativo del derecho de protección de datos y responder de las vulneraciones y perjuicios que puedan llegar a producirse por causa del tratamiento de datos de carácter personal. No obstante, a pesar de ser utilizados de forma indistinta por el marco jurídico del derecho a la protección de datos, dichos responsables no son lo mismo y se diferencian según expone el Tribunal Supremo en su sentencia del 5 de Junio del 2004 en: *"…función de que el poder de decisión vaya dirigido al fichero o al propio tratamiento de datos. Así, el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir, quien tiene capacidad de decisión sobre la totalidad de los datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica. Se trataría de todos aquellos supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento".*[53]

Asimismo, la figura del responsable, dentro del ámbito de los registros de morosos, suele ser, en la gran mayoría de los casos, una empresa especializada en proporcionar información sobre el patrimonio o la capacidad económica de empresas y particulares. Además, es muy posible que dicha empresa especializada también sea responsable de un fichero de solvencia patrimonial y crédito, con el cual pueda llegar a proporcionar un servicio más amplio. Sin que en ningún caso la gestión de ambos ficheros pueda ser la misma.[54]

[53] STS de 5 de Junio de 2004, FJ. 3º, segundo párrafo.
[54] En este punto, téngase en cuenta que, aunque, una empresa pueda llegar a tener varios ficheros de datos de carácter personal dichos ficheros deben ser gestionados de acuerdo a lo establecido por el marco jurídico.

En lo que respecta al encargado del tratamiento encuentra su definición en el artículo 3.g) LOPD y en el artículo 5.1.i) RLOPD, trascrita esta última a continuación, por ser la más completa: "*La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio…*". Además, hay que tener en cuenta que tal relación jurídica debe seguir los requisitos mínimos establecidos en el articulo 12 LOPD, para el acceso por cuenta de terceros.

Así pues, la figura del encargado del tratamiento adquiere una gran importancia dentro del ámbito del derecho de protección de datos pues, tal como manifiesta la AEPD, en su Informe Jurídico 0227/2010: "*…. responde a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso no pueda considerarse como una cesión de datos. […] cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"*[55]. Máxime cuando algunos de esos tratamientos, encomendados a terceros vienen impuestos por la necesidad de cumplir imperativos legales, tales como las auditorias impuestas por el artículo 96 RLOPD o la necesidad de utilizar un medio de comunicación independiente (encargado) para realizar las notificaciones del articulo 40 RLOPD.

En consecuencia, la figura del encargado del tratamiento sirve para evitar que el responsable del tratamiento tenga que recabar el consentimiento de los titulares de los datos cada vez que tenga la necesidad de que un tercero le preste un servicio. En muchos casos son necesarios debido al nivel de especialización que tales tratamientos requieren. Piénsese, sino, en el caso, de las medidas de seguridad, las cuales según van aumentando los niveles va aumentado su complejidad.

[55] Véase a este respecto: Informe Jurídico 0227/2010, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 1.

Igualmente, hay que resaltar que, aunque el responsable del tratamiento recurra a los servicios del encargado del tratamiento, ello no le exonera de las posibles vulneraciones que puedan llegar a producirse a lo largo del tratamiento. Por esta razón, la figura del encargado del tratamiento volverá a ser retomada en el apartado dedicado a los problemas prácticos en relación con las obligaciones del responsable.

Para finalizar, conviene mencionar la diferencia entre el responsable del tratamiento y el encargado, que tal como manifiesta la AEPD en su Informe Jurídico 0287/2006: *"...lo importante para delimitar los conceptos de responsable y encargado del tratamiento no resultan ser la causa que motiva el tratamiento de los mismos, sino la esfera de dirección, control u ordenación que el responsable pueda ejercer sobre el tratamiento de los datos de carácter personal que obran en su poder en virtud de aquella causa y que estaría enteramente vedado al encargado del tratamiento"*[56].

3. Problemas en su puesta en práctica

El tratamiento de datos de carácter personal, como ya se ha hecho mención a lo largo de este trabajo, no es una tarea sencilla, máxime, cuando se tratan datos personales los cuales pueden llegar a perjudicar al titular de los datos como puede ser el caso del tratamiento de datos relativos al incumplimiento de obligaciones dinerarias. Así pues, las cautelas que se deben llevar a cabo a la hora de tratar dichos datos son mucho más estrictas.

3.1. En relación con los principios del tratamiento.

La aplicación de los principios del tratamiento de datos personales, dentro del ámbito de los registros de morosos, adquiere una gran importancia debido a la repercusión o efectos negativos de los datos en ellos recogidos. Puesto que su aplicación no está carente de problemas prácticos, su cumplimiento debe ser mucho más rígido para proteger los derechos de los titulares de los datos. Así pues, dicha problemática será tratada en el presente apartado siguiendo el orden en que fueron explicados los principios del tratamiento.

[56] Véase a este respecto: Informe Jurídico 0287/2006, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 5 y también; Informe Jurídico 0227/2010, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 1 a 2.

Los problemas prácticos surgidos en torno al principio de información suelen darse a la hora de proporcionar dicha información, que suelen ser tres momentos concretos: al celebrarse el contrato, cuya obligación dineraria se incumplió; al efectuar el requerimiento previo de pago; y en una comunicación final realizada por el responsable del fichero común, una vez inscrito los datos en el registro de morosos. De estos tres momentos, los dos primeros serán tratados a continuación por ser ambos obligaciones que debe cumplir el acreedor de forma acumulativa si quiere inscribir los datos personales de la obligación incumplida, y el último será tratado más adelante dentro de las obligaciones del responsable.

En lo que respecta al primero de estos momentos *"el momento de celebrar el contrato"* se encuentra recogido en el artículo 39 RLOPD y es el inicio de un doble deber de información.[57] Así pues, dicha obligación no puede ser subsanada por medio de la información proporcionada después en el requerimiento previo de pago. Ya que de otro modo, tal como, manifiesta la AEPD en su Informe Jurídico 0348/2013: "*se llegaría* a *la conclusión absurda de que nunca sería preciso el cumplimento del deber de información en el contrato".*[58]

El segundo de los momentos *"el requerimiento previo de pago"* concentra la mayor parte de la problemática práctica, debido a que el marco jurídico de protección de datos no establece ningún formalismo concreto ni para su cumplimiento, ni para certificarlo. Además, hay que tener en cuenta la evolución que ha sufrido la obligación, pues antes se encontraba recogida en la Norma primera de la Instrucción 1/1995, de la AEPD y en la actualidad se encuentra recogido en el articulo 39 RLOPD, sin que ninguna de esas normas concrete el proceso de ejecución.

Así pues, al principio se establecía una obligación por parte del acreedor de demostrar el cumplimento del requerimiento previo, aunque sin imponer ningún criterio concreto sobre cómo llevarlo a cabo[59]. No obstante, con el paso del tiempo, la obligación de

[57] Véase: STS de 15 de julio de 2010, FJ 17º.
[58] Informe Jurídico 0348/2013, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 3
[59] Véase al respecto: SAN de 28 de mayo de 2008, FJ 3º.

demostrar el cumplimento aún continúa, pero, dicha obligación, ha sido concretada por la labor jurisprudencial de la Audiencia Nacional y el Tribunal Supremo.[60]

En consecuencia, gracias a la labor jurisprudencial de la Audiencia Nacional y del Tribunal Supremo, podemos entender que el requerimiento previo cuenta con los siguientes requisitos:[61]

- Debe ser una comunicación fehaciente, dirigida a una persona concreta, en la que conste de forma expresa la posibilidad de la inscripción en caso de incumplimiento. Además de existir una concordancia entre la cantidad adeuda y la que finalmente se inscriba en el fichero.
- Cualquier defecto en el requerimiento, ya sea tanto en contenido (datos del deudor, cuantía de la deuda, posibilidad de inclusión en caso de incumplimiento, etc.…) como en la forma (envió posterior a la inscripción, documento o formato que no pueda acreditar de forma fehaciente el envió, etc.…) es insubsanable.
- En caso de requerimiento erróneo se debe volver a hacer otro requerimiento para poder inscribir en el registro de morosos y si se dio la inscripción responder por las vulneraciones provocadas por la misma.
- No se puede ni inscribir antes de realizar el requerimiento, ni antes de que pase el plazo ofrecido en dicho requerimiento para cumplir con la obligación.
- El acreedor debe probar la realización del requerimiento o, al menos, tener un indicio de su envió o recepción al deudor en cuestión, cuando éste niegue su recepción. Así pues, la constancia de su realización por los registros informáticos del obligado, no es una prueba suficiente de su realización.
- No se considera válidamente hecho el requerimiento (a efectos del ámbito de protección de datos), cuando se hace por medio de la remisión de facturas, la referencia de llamadas no grabadas, llamadas telefónicas automatizadas, o la realización de mensajes de texto sms.

Sin embargo, a pesar de la labor jurisprudencial de la Audiencia Nacional y del Tribunal Supremo, no disminuye la incertidumbre y los problemas prácticos que pueden llegar a

[60] Véase: San Martín Arias. Ignacio, "*Protección de datos en el crédito al consumo". Aranzadi, Pamplona,* 2015, pp. 55 y ss.
[61]Véase al respecto: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 533 y ss. y también; San Martín Arias. Ignacio, "*Protección de datos*…", cit., pp. 55 y ss.; en concreto el estudio sobre este punto.

surgir por la falta de un proceso concreto. Por ello algunos autores, como Ignacio San Martín Arias han llegado a preguntarse, incluso, "*si podría darse el caso de que un requerimiento de pago no se haga por escrito"*, concluyendo que "sí cabe la posibilidad" con base a los artículos 38.3, 5.1.f), 12, 17 y 24.4 RLOPD, además de algunos procedentes de otros normas como el artículo 7 de Ley 16/2011, de 24 de junio, de contratos de crédito al consumo[62] apoyándose en ciertas sentencia de la Audiencia Nacional sobre este respecto.[63] En síntesis, los argumentos de Ignacio San Martín Arias se basan en tres ideas: [64]

1. La imprecisión del término *"documentación"* del artículo 38 RLOPD, en concreto cuando dice: *"El acreedor […] estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento…"*.
2. Las disparidad de formas de comunicación que admite y ofrece el RLOPD, en concreto las recogidas en los artículos anteriormente mencionados.
3. El uso de servicios de terceros para acreditar tanto el envió como la recepción del requerimiento, evitando de este modo problemas en cuanto a la acreditación.

Así pues, es cierto que de la lectura de los artículos anteriormente mencionados se puede llegar a la conclusión de que el RLOPD ofrece una gran libertad, en cuanto a la elección del medio para la comunicación con el titular de los datos, e igualmente que el uso de los servicios de un tercero independiente para acreditar los requisitos del requerimiento previo (envió y recepción), puede llegar a solucionar muchos problemas de acreditación.

No obstante, en mi opinión, no considero que dichas características permitan la utilización de cualquier tipo de requerimiento no escrito, por mucho que pueda llegar a certificar el envió y la recepción del requerimiento. Pues, tal como manifiesta la AEPD en su Informe jurídico 0453/2013: "*…se trata de una verdadera manifestación de voluntad por la cual el acreedor requiere al deudor para que cumpla su obligación, […] Se trata, en definitiva, de un acto que trasciende con creces de un mero*

[62] Ley 16/2011, de 24 de junio, de contratos de crédito al consumo (BOE de 25 de Junio de 2011, núm. 151).
[63] Véase: San Martín Arias. Ignacio, "*Protección de datos*…", cit., pp. 57 y ss.; en especial el apartado dedicado al requerimiento previo.
[64] Ídem.

cumplimiento formal, puesto que se otorga al deudor, […] una nueva oportunidad para cumplir su obligación…". Por consiguiente, a mi entender, para que el medio por el cual se realiza el requerimiento sea valido no basta únicamente con poder acreditar tanto el envió y la recepción, sino que, también, debe permitir su conservación por parte del deudor para poder comprender plenamente su contenido. Dicho de otro modo, el hecho de que se realice válidamente un requerimiento no quiere decir, necesariamente, que el deudor entienda el contenido del requerimiento, pues debido a la pluralidad de relaciones contractuales que pueden llegar a tener, necesitará un tiempo para poder situarse y comprender si es verdaderamente un incumplimiento suyo o por si el contrario es un incumplimiento ajeno a él.

Igualmente, continuando con la figura del requerimiento previo, y antes de pasar al principio del consentimiento, conviene hacer una leve referencia a las obligaciones dinerarias cuyo incumplimiento puede darse de manera sucesiva, ya que en este caso basta con realizar un único requerimiento.

En lo relativo a los problemas surgidos por el principio del consentimiento son mínimos, ya que el consentimiento no es necesario para tratar los datos de carácter personal en este tipo de registros. Aunque, no hay que olvidar, la obligación dineraria incumplida o cumplida requirió del consentimiento en su momento.

No obstante, su falta influye considerablemente en el resto de los principios, pues hace su cumplimiento más rígido y restrictivo. Como bien dice el Tribunal Supremo en su Sentencia 21 Mayo de 2014: *"Si la inclusión de datos personales en un fichero se hace excepcionalmente sin el consentimiento del afectado, y si además, por la naturaleza del fichero, la inclusión en él de los datos personales del afectado puede vulnerar, además del derecho del art. 18.4 de la Constitución , otros derechos fundamentales y causar graves daños morales y patrimoniales a los afectados, no pueden rebajarse las exigencias en cuanto a calidad de los datos ni establecerse restricciones u obstáculos […] por cuanto que ello supondría restringir de un modo injustificado el derecho de control sobre los propios datos personales …."*.[65]

[65] STS de 21de mayo de 2014, FJ 8º tercer apartado.

Por todo ello, dentro de los registros de morosos, no basta con el cumplimiento literal de la normativa de protección de datos, sino que, además, dicho cumplimento debe ir encaminado a un efectivo respeto de los principios del tratamiento de datos de carácter personal y el derecho a la protección de datos en general. Así lo vemos en la Sentencia anteriormente mencionada en la que no se admitió que el responsable del fichero común se desentendiera del cumplimiento del principio de calidad bajo el argumento de que dicha obligación excedía sus funciones.[66]

En este orden de cosas, siguiendo con la explicación de los problemas prácticos en cuanto a los principios del tratamiento, pasamos a tratar el principio de calidad. Éste principio es quizás el principio más importante para la defensa del derecho a la protección de datos. Además, debemos indicar que la falta del requerimiento previo de pago es entendida como una vulneración del principio de calidad.[67]

El principio de calidad centra su problemática en el cumplimiento de los requisitos del articulo 38 RLOPD, es decir, en la necesidad de que exista *"una deuda cierta, vencida, exigible, que haya resultado impagada"* y cuya antigüedad no sea superior a 6 años como legal y reglamentariamente se establece. Además de haberse hecho un requerimiento previo de pago (requisitos ya tratados en anteriores apartados, por lo que nos remitimos a los mismos).

Sin embargo, antes de empezar a tratar la problemática surgida en relación con dichos requisitos, conviene hacer una breve mención sobre cuándo considera la Audiencia Nacional vulnerado el principio de calidad de datos. Así pues atendiendo a las palabras de la Audiencia Nacional, en su Sentencia de 8 de Enero de 2006: *"El principio de calidad del dato comienza a infringirse en el momento en que se facilitan datos erróneos a un fichero que presta información a terceros sobre el incumplimiento de obligaciones dinerarias…"*.[68] Por lo tanto, los problemas surgidos por la puesta en práctica de dicho principio versarán sobre los errores relativos a los requisitos del artículo 38 RLOPD, anteriormente mencionados, o los requisitos generales del artículo

[66] Véase: STS de 21 de mayo de 2014, FJ 8º cuarto apartado y siguientes, y téngase en cuenta que sobre este aspecto se volverá a tratar más en profundidad dentro del apartado III 3.3. *En relación con las obligaciones del responsable.*
[67] Véase al respecto: SAN de 21 de marzo de 2014, FJ 3º y 4º.
[68] SAN de 8 de enero de 2006, FJ 5º.

4 LOPD (adecuados, pertinentes y no excesivos, además de exactos y actualizados entre otros). Así pues, para lo que aquí nos interesa, la inexactitud es considerada como una infracción grave del articulo 44.3.c) LOPD, con pena de multa de entre 40.001 a 300.000 €, según dispone el artículo 45.2 LOPD.[69]

En relación con el primero de los requisitos del articulo 38 RLOPD *"una deuda cierta, vencida, exigible, que haya resultado impagada"* encuentra una gran problemática en el momento de inscribir datos sobre una deuda discutida, pues por regla general los órganos que velan por el derecho fundamental a la protección de datos (AEPD y los órganos judiciales que conocen del recurso de sus resoluciones) no tienen competencia para pronunciarse sobre la existencia o no de la deuda, ya que es un tema civil. [70] Ello unido a la declaración de nulidad de los artículos 38.1.a), inciso final, y 38.2 RLOPD por parte de la Sentencia del Tribunal Supremo de 15 de julio del 2010 junto con la vertiente iniciada por la Sentencia de la Audiencia Nacional de 15 de marzo del 2012, obliga a tener cierta cautela a la hora de inscribir este tipo de datos.

Así pues, nos encontramos en un contexto en el que no se puede decidir sobre la existencia o no de la deuda, y en el que también se debe tener en cuenta, por un lado, la Sentencia del Tribunal Supremo de 15 de julio del 2010, que anula la posibilidad ofrecida por el artículo 38 de cancelar de forma automática los datos sobre deudas discutidas, por entender que la vaguedad de la redacción la hacía insegura, además de que permitía *"considerar que incluso cuando la reclamación se formule por el acreedor exista la imposibilidad de inclusión de los datos en el fichero"*[71]. Y, por el otro lado, la Sentencia de la Audiencia Nacional de 15 de marzo del 2012, que entiende, en síntesis, que a pesar de dicha anulación ello no quita la obligación de justificar la existencia de la deuda y, mucho menos, el ser cancelados los datos, si de los indicios se aprecia la inexistencia de la deuda.[72]

[69] Véanse al respecto: SAN de 19 de Julio de 2016, FJ 3º y también; SAN de 22 de marzo de 2016, FJ 3º.
[70] Véase al respecto: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección…*", cit., p. 526.
[71] Véase: STS de 15 de julio de 2010, FJ 14º.
[72] Véase: SAN de 15 de marzo 2012, FJ 5º y también; SAN de 30 de mayo de 2012, FJ 5º.

En consecuencia, el resultado final de ambas sentencias es que hay que estar a la casuística del caso para poder determinar si la deuda es o no cierta (a efectos de la inscripción), puesto que ya no se permite la cancelación preventiva de forma automática, pero tampoco se puede permitir la inscripción de deudas inexistentes. Así pues, a modo de ejemplo, y sin ánimo de ser taxativo, expondré a continuación algunas situaciones, en donde se ha considerado la deuda discutida como no cierta:[73]

- La existencia de una causa civil pendiente, sobre la deuda en cuestión o diligencias previas en un procedimiento penal, contra el acreedor por un presunto delito de estafa. En ambos casos se cuestiona la existencia o certeza de la misma.
- Reclamaciones contra la deuda hechas ante una de estas entidades: la Secretaria de Estado de Telecomunicaciones, Juntas arbitrales de consumo, Oficina Municipal de Información al Consumidor.
- La existencia de un acuerdo transaccional que redimía parte de la deuda, pues ello implicaría que parte de la deuda ha sido perdonada y, por tanto, que ya no es exigible. Lo que se traduce en que parte de esa deuda (la no exigible) no cumple con el principio de calidad de datos y no puede ser inscrito en el registro, porque el principio de calidad de datos debe ser cumplido por todas los elementos de la deuda; no siendo admisible un mantenimiento parcial de la misma.

En lo que respecta al segundo de los requisitos que *"no hayan transcurrido seis años"*, responde a la necesidad de veracidad y actualidad de los datos recogidos en el registro, y su cómputo se inicia, según entiende la Audiencia Nacional, en su Sentencia de 3 de marzo de 2000:" *Lógicamente, la determinación del "dies a quo" para el cómputo de los seis años no podrá ser otro que el día del vencimiento de la obligación impagada…* ".[74] Asimismo, hay que tener en cuenta que el plazo de 6 años, puede dejar sin inscribir obligaciones aún vigentes y exigibles, pero, no hay que olvidar, que los registros de morosos tienen la función de enjuiciar la solvencia económica de los titulares de los datos y no la de asegurar el cobro de la deuda o servir como medio coercitivo para el pago. Por lo tanto una deuda de una antigüedad superior a 6 años aún vigente poco puede llegar a decirnos sobre la solvencia económica actual.

[73] Véase: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 527 y ss.
[74] SAN de 3 de marzo de 2000. FJ. 1º apartado cuarto.

Otra cuestión relevante es la referida al contenido o carácter de la deuda, pues el marco jurídico del derecho a la protección de datos sólo indica que la deuda debe ser de carácter dinerario. Por tanto, al no establecer ni limitaciones ni concreciones sobre la deuda, todas las deudas que se inscriban serán tratadas de la misma manera, sin importar, ni su cuantía, sea de 1 ó 30.000 €, ni las circunstancias, sea o no intencionado el incumplimiento, ni quién lo hizo, sea un deudor primerizo o un auténtico profesional del incumplimiento.

Antes de pasar a tratar el principio de finalidad, es interesante hacer una mención a la inclusión en el registro de morosos de deudas procedentes clausulas penales, esto es, de deudas consensuales derivadas del incumplimiento de una obligación, las cuales permiten en la práctica inscribir en el registro de morosos el incumplimiento de obligaciones no dinerarias que se han cuantificado. Además de no cumplir, en mi opinión, con la finalidad buscada por el registro de morosos, pues, por un lado, la clausula penal es una pena por el incumplimiento de una obligación y no la obligación incumplida en sí. Y por otro lado, en nada ayuda a enjuiciar la solvencia económica del titular de los datos el conocer la pena de dicho incumplimiento, pues no refleja la realidad de la deuda incumplida, sino la pena impuesta por el incumplimiento, ni las circunstancias que motivaron su inscripción.

No obstante, puesto que las clausulas penales pueden llegar a cumplir los requisitos del principio de calidad, pueden ser inscritas en el registro de morosos siempre y cuando no sean, en la práctica, un intento unilateral del acreedor de penar al deudor, tal como se deduce de la Sentencia del Tribunal Supremo del 16 de febrero de 2016: *"... Los datos que comunicó al registro de morosos no eran veraces ni exactos pues no existía previamente una deuda cierta, vencida, exigible, que hubiera resultado impagada, sino una reclamación derivada de la unilateral liquidación por la demandada de una cláusula penal redactada en términos que no permitían, por sí solos, fijar la cantidad en que se concretaba su aplicación…".*[75]

[75] STS de 16 de febrero de 2016, FJ 4º, apartado 10, y también; véase al respecto Carrasco Perera. Ángel, "*Cuidado con la inclusión de un cliente en un registro de morosos por el impago de cláusulas penales"*. *Revista CESCO de Derecho de Consumo*, Nº. 17, 2016, pp. 252 y 253.

En lo concerniente al principio de finalidad, como, ya se mencionó en su momento, dicho principio está estrechamente relacionado con el principio de calidad. Así pues, su uso tradicionalmente se hacía en conexión como un elemento del principio de calidad de datos, y nunca de forma autónoma. Como así se puede deducir de la Sentencia de la Audiencia Nacional de 16 de Mayo de 2011: *"Principio de calidad del dato del que deriva, según esta Sala ha declarado en numerosísimas ocasiones, no solo la exigencia de que los datos se recojan para su tratamiento de acuerdo con una serie de criterios (principio de proporcionalidad), y que los mismos se empleen para finalidades compatibles a las que motivaron la recogida (principio de finalidad), sino también que sean exactos y puestos al día. Se trata en definitiva de garantizar y proteger la veracidad y calidad de la información sometida a tratamiento, por la que debe velar quien recoge y trata dichos datos de carácter personal".*[76]

Sin embargo, como bien demuestra Antonio Linares Gutiérrez en su artículo "*El chantaje de los ficheros de morosos: el principio de finalidad como requisito para la inclusión de datos en los ficheros sobre solvencia patrimonial y crédito tratamiento jurisprudencial"*[77] el principio de finalidad tiene una importancia propia, más allá de un mero criterio accesorio para comprobar si se ha infringido otro principio (principalmente el de calidad). Así pues, para tratar el principio de finalidad se profundizará, por un lado, en la finalidad buscado por los ficheros de morosos y, por el otro, la problemática que llevan aparejadas estos ficheros, para así poder llegar a entender un poco mejor cuándo se incumple dicho principio.

En relación con la finalidad perseguida por el fichero de morosos, la misma se encuentra recogida en el artículo 29.4 LOPD y consiste, como ya se ha hecho referencia varias veces en este trabajo, en enjuiciar la solvencia económica de los titulares de los datos, por medio de la exposición al público de datos sobre el incumplimiento de obligaciones dinerarias. En concreto dicha exposición va dirigida a terceros que quieran entablar un negocio jurídico con el titular. También, conviene mencionar, en mi opinión, que la mera exposición (sin ningún otro dato complementario) de una conducta

[76] SAN de 16 de mayo de 2011, FJ 3º, último párrafo.
[77] Linares Gutiérrez, Antonio, "El chantaje de los ficheros de morosos: el principio de finalidad como requisito para la inclusión de datos en los ficheros sobre solvencia patrimonial y crédito: tratamiento jurisprudencial", *Dereito: Revista xuridica da Universidad de de Santiago de Compostela*, Nº 1, 2014, pp. 113-126.

referida al incumplimiento de una obligación no es un dato objetivo para llegar a enjuiciar la solvencia económica de una persona; pues un incumplimiento puede deberse a una gran diversidad de causas ajenas a la capacidad económica del deudor y, en consecuencia, no válidas para llegar a clasificar un dato objetivo como es la solvencia económica. En todo caso, con ello podría llegarse a enjuiciar la fiabilidad de la persona.

Asimismo, la citada finalidad del registro de morosos es un hecho plenamente aceptado por los órganos judiciales, como, por ejemplo, la Audiencia Nacional que en su Sentencia 9 de enero de 2009 señalo que *"Esta Sala efectivamente conoce las funciones que realizan estos ficheros en su contribución a la salvaguarda del sistema financiero y de la economía en general, por cuanto permiten a las entidades financieras, principalmente, conocer la solvencia de sus presentes o futuros clientes. Consciente de esta importante función, la Ley ha establecido un sistema de acceso al fichero más ágil, […] se hace a instancias del acreedor y sin consentimiento del afectado, aunque con notificación posterior al mismo,…".*[78]. Esta finalidad también es reconocida por la AEPD, tal como demuestra su Resolución de 22 de enero del 2001 al señalar: *"…este tipo de ficheros contribuye sin duda a la salvaguarda del sistema financiero y de la economía en general por cuanto van a permitir a las entidades financieras por un lado, el conocer la solvencia de sus clientes y quienes de estos clientes o potenciales clientes han incurrido en morosidad y por qué cuantía y por otro proporcionar igual conocimiento a las empresas, sobre todo a las pequeñas y medianas a las que una situación de incumplimiento de sus clientes pudiera arrastrar a situaciones irreparables con grave quebranto no sólo económico sino también incluso social".*[79]

Igualmente, es interesante abordar la finalidad del registro de morosos desde una perspectiva económica y en concreto su fundamento económico. Tal como hace Julián Timoner Giménez, en su artículo *"Una visión crítica de los registros de morosos: alegalidad de los mismos"*, donde expone:"*…el fundamento económico de los registros de morosos nace para reducir la información asimétrica y especialmente asociado al riesgo ético, calidad del deudor, y a la reducción de los costes de monitorización. […]*

[78] SAN de 9 de enero de 2009, FJ 4º.
[79] Véanse, Resolución de la AEPD de 22 de enero del 2001 o Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 522.

como medida para reducir el coste del riesgo ético y el coste de monitorización o de seguimiento de las operación de sus deudores". Es decir, de forma más sencilla, su fundamento es reducir los costes producidos por los distintos niveles de información con los que cuentan las distintas partes del negocio jurídico (información asimétrica), surgidas, o bien, por la capacidad del deudor de eludir sus obligaciones con respecto del acreedor; aprovechando el desconocimiento de éste de su patrimonio (riesgo ético), o bien, por las operaciones que tiene que asumir el acreedor para descubrir la verdadera capacidad económica del deudor (coste de monitorización).[80]

En resumen, la finalidad perseguida por el registro de morosos es proporcionar mayor información a las empresas o terceros que quieran contratar, para que puedan tomar una mejor decisión y distribución de sus recursos, en vez de usar parte de los mismos en monitorizar una relación contractual con un resultado incierto. Una idea bastante noble si no fuera por la problemática accesoria que trae consigo de la que trataremos a continuación.

La problemática aparejada al registro de morosos viene dada por los efectos o el carácter negativo de los datos en ellos recogidos, pues, no hay que olvidar, que tratan sobre incumplimiento de obligaciones que se dan a conocer a terceros específicos (en concreto, aquéllos que estén pensando en entablar un relación contractual con el titular de los datos). Así pues, en la práctica los registros de morosos llevan aparejado un importante elemento de descrédito y exclusión, o en palabras, bastante acertadas, de Julián Timoner Giménez, *"... la inclusión ilícita estigmatiza de tal modo a una persona dentro de la sociedad al imputarle el adjetivo de incumplidor que puede ello acabar creándole perjuicios en todas las facetas de su vida, limitando así sus derechos de ciudadano al negarle su condición de "sujeto del crédito""*.[81]

Por lo tanto, esos elementos de descrédito y exclusión se unen dentro de los ficheros de morosos para hacer de ellos una medida de coacción. Y así lo han aceptado ampliamente los órganos judiciales, tal como demuestra, por ejemplo, la Sentencia de la

[80] Timoner Giménez, Julián, "*Una visión crítica de los registros de morosos: alegalidad de los mismos". Aletheia: Cuadernos Críticos del Derecho*, Nº. 1, 2009, p. 72.
[81] Timoner Giménez, Julián, "*Una visión crítica…",* cit., p. 73 y téngase en cuenta, el concepto de *"sujeto de crédito"* hace referencia a la necesidad de las personas de acceder al crédito para llevar a cabo alguna negocio, de cuyo conste no puedan asumir solos (comprar una cosa, iniciar un negocio. Etc.), provocando su denegación; por estar inscrito en un fichero de moroso, un perjuicio considerable.

Audiencia Nacional del 9 de enero de 2009 cuando dice: *"En conclusión debe considerarse, que aquel que utiliza un medio extraordinario de cobro como es el de la anotación de la deuda en un registro de morosos, debe garantizar el cumplimiento de todos los requisitos materiales (exactitud del dato) y formales (requerimiento previo) que permitan el empleo de este modo accesorio para conseguir el cobro de la deuda. No aplicar esta exigencia supondría, por el contrario, utilizar este medio de presión al recurrente sin el suficiente aseguramiento de las mínimas garantías para los titulares de los datos que son anotados en los registros de morosos"*, una coletilla bastante frecuente en las sentencias sobre ficheros de morosos desde la Sentencia de la Audiencia Nacional del 20 de abril de 2006.[82]

En síntesis, podemos comprobar cómo los registros de morosos tienen la finalidad de ofrecer información sobre la capacidad económica de los titulares de los datos, pero debido a sus particularidades no pueden evitar ofrecer exclusión y descrédito a los mismos. Así pues, partiendo de esta premisa podemos decir que el principio de finalidad se considera vulnerado cuando el objetivo de la inclusión en estos registro es causar un desprestigio a los titulares de los datos en vez de informar sobre su solvencia.

Por todo ello, resulta tranquilizador que desde hace unos años se empiece a tener en cuenta el principio de finalidad como un elemento necesario para la inscripción, en vez de un mero complemento de la deuda que motiva la inscripción. Así se puede comprobar de la Sentencia del Tribunal Supremo del 6 de Marzo de 2013, cuando expone *"La inclusión en los registros de morosos no puede ser utilizada por las grandes empresas para buscar obtener el cobro de las cantidades que estiman pertinentes, amparándose en el temor al descrédito personal y menoscabo de su prestigio profesional y a la denegación del acceso al sistema crediticio que supone aparecer en un fichero de morosos, evitando con tal práctica los gastos que conllevaría la iniciación del correspondiente procedimiento judicial, muchas veces superior al importe de las deudas que reclaman"*[83] . O en la Sentencia del mismo órgano del 16 de Febrero de 2016, cuando dice: *"no se respetaron los principios de prudencia y*

[82]Véanse, SAN de 9 de enero de 2009; FJ 4º, SAN de 13 de diciembre de 2013; FJ 3º, SAN de 10 de junio de 2011; FJ 5º, SAN de11 de marzo de 2011; FJ 7º, SAN de 1 de octubre de 2010; FJ 6º. Y también; el listado de sentencia recogidos en la nota número 7 del artículo; Linares Gutiérrez. Antonio, "El chantaje de los ficheros de morosos:...", cit., p. 117.
[83] STS de 6 de marzo de 2013, FJ 6º.

proporcionalidad, puesto que los datos no eran determinantes para enjuiciar la solvencia económica. No es controvertido que los clientes demandados habían pagado las cuotas del servicio de vigilancia hasta que decidieron darse de baja. Si a continuación se negaron a pagar la cantidad que la empresa de seguridad demandada fijó unilateralmente en aplicación de la cláusula penal […] ha de afirmarse que la negativa de un cliente que ha pagado regularmente las cuotas mensuales correspondientes al servicio prestado, a abonar la penalización por desistimiento cuando la cláusula que la prevé no es precisa y deja un amplio margen al predisponente para fijar el importe de la sanción, no es, en estas circunstancias, determinante para enjuiciar la solvencia del cliente, porque es evidente que no viene determinada por su imposibilidad de hacer frente a sus obligaciones, que es en lo que consiste la insolvencia, ni por su negativa maliciosa a hacerlo, sino por su discrepancia razonable con la conducta contractual de la demandante ".[84]

Sin embargo, es necesario resaltar que el principio de finalidad (y quizás el resto de principios) sólo pueden ser apreciados en toda su plenitud por los órganos jurisdiccionales del ámbito civil, pues los del ámbito contenciosos-administrativo y la AEPD no tienen competencia para tratar todas las vicisitudes relacionadas con la inscripción de los registros de morosos.[85] Ya que, no hay que olvidar, que las deudas que motivan la inscripción son un asunto civil.

3.2. En relación con los derechos de los titulares. Especial mención al derecho al honor.

El ejercicio de los derechos de los titulares dentro del ámbito de los registros de morosos adquiere gran importancia debido a los datos que en ellos se inscriben. Encontramos intereses contrapuestos recogidos, tales como, por un lado, el interés de informar sobre la solvencia patrimonial del interesado y, por el otro, el de salvaguardar los derechos del titular de los datos.

La problemática práctica que se da en relación al ejercicio de los derechos de los titulares se centra en torno al ejercicio de los derechos ARCO, además, de otras características propias de su ejercicio dentro de los registros de morosos. Así pues, en el

[84] STS de 16 de febrero de 2016, FJ 4º, apartado 10.
[85] Véase al respecto: STS de 16 de febrero de 2016, FJ 4º, apartado 10.

presente apartado se tratará el proceso por el cual se ejercitan los derechos con las características propias que adquiere cada derecho dentro del ámbito de los registros de morosos. Además, se analizará una tutela complementaria ofrecida por los órganos jurisdiccionales del ámbito civil, en cuanto a la indemnización por el mal uso de los datos de los titulares.

No obstante, se hace necesario desde un principio, antes de empezar a tratar dicha problemática, resaltar que a pesar de ser tratados en este mismo apartado el derecho a la protección de datos, ejercitado por medio de los derechos ARCO, y el derecho al honor, ambos derechos son diferentes y autónomos, y cuyo único nexo de unión (dentro del presente trabajo) es que ambos se pueden ver vulnerados por un mal uso de los datos de carácter personal en este tipo de ficheros.

En referencia al ejercicio de los derechos ARCO, como ya se dijo en su momento, gozan de una gran libertad en cuanto a la elección del medio para llevar a cabo el ejercicio de estos derechos. No obstante, aunque dicha libertad es beneficiosa a la hora de facilitar la comunicación entre el responsable del tratamiento y el titular de los datos, también es perjudicial a la hora de acreditarlo, pues tanto el titular de los datos como el responsable del tratamiento no pueden estar seguros de que se haya producido y de la forma de probarlo. Así, en caso de discrepancias el medio utilizado sirve para acreditar efectivamente su ejecución, puesto que (como bien se ha abordado en apartados anteriores) una cosa es que exista un amplio margen en la elección del medio y otra muy diferente que tal hecho permita cualquier tipo de acreditación.[86]

Asimismo, el marco normativo del derecho a la protección de datos no establece ningún proceso concreto, pero sí indica, en sus artículos 23 y 24 RLOP una serie de criterios mínimos a tener en cuenta a la hora de ejercitar los derechos ARCO, tales como: [87]

- La solicitud debe ser ejercida por el afectado debiendo el mismo identificarse al momento de dicha solicitud bajo pena de denegarse (siempre y cuando el

[86] Para este punto téngase en cuenta lo dicho en el apartado 3.1. "En relación con los principios del tratamiento", cuando se trata sobre el requerimiento previo y sus requisitos, pp. 29 y ss. de este mismo trabajo.
[87]Véase: Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 210 a 214.

responsable del fichero haya requerido al afectado para subsanar y éste no lo hubiera hecho).

- En caso de optar por la representación, ésta deberá estar debidamente acreditada siendo necesario cuando se trate de una representación voluntaria, acreditar la identidad del representado por medio de una copia del DNI o documento equivalente e indicar los términos exactos de dicha representación.
- La solicitud de cualquiera de los derechos ARCO no influye ni condiciona el ejercicio futuro de cualquier otro derecho ARCO.
- El proceso por el cual se lleve a cabo dicha solicitud debe ser sencillo y gratuito para el afectado, no representando en ningún caso un ingreso adicional para el responsable del fichero.
- En el caso de que el responsable o encargado cuente con su propio servicio de atención al público, la solicitud se podrá llevar a cabo por medio de dicho servicio y de acuerdo con las normas en él establecidas, siempre y cuando su uso no se traduzca en un sobrecoste para el afectado, como podría ser, por ejemplo, el requerir el envió de cartas certificadas; el uso de servicios de telecomunicaciones que implique una tarificación adicional.etc.
- Como criterio final, si el afectado decidiera usar un proceso ajeno al ofertado por el responsable, éste se verá obligado a contestar dicha petición pero, ni deberá asumir el coste del mismo (siempre y cuando se pueda llegar al mismo objetivo por otros medios menos costosos) ni responder de los posibles fallos que dicho medio elegido por el afectado pueda llegar a tener.

En consecuencia, podemos comprobar que existe una cierta disposición a permitir que sea el responsable del tratamiento el que decida como gestionar las solicitudes de los derechos ARCO aunque permitiendo a los titulares de los datos, en última instancia, decidir el proceso por el cual quiere ejercitar dichos derechos. Sin embargo, dicha situación provoca que puedan darse tantos procesos como ficheros haya, lo que provocaría *de facto* que los titulares de los datos tuvieran que adaptarse a cada proceso dependiendo de contra quien ejercieran sus derechos.

Igualmente, es necesario tratar las particularidades que los derechos ARCO adquieren dentro de los ficheros de morosos, referidas tanto al contenido del derecho como a los plazos. Así pues, dichas particularidades se encuentran recogidas en el artículo 44 RLOPD y afectan a los derechos de acceso, de rectificación y cancelación.

En relación con el derecho de acceso el articulo 44 RLOPD modifica la información que el responsable (o el encargado en su caso) debe ofrecer al titular de los datos, ya que a parte de la información básica que debe acompañar a la respuesta del ejercicio del derecho de acceso *"datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismo*"[88], también debe proporcionar una información añadida dependiendo de ante quién se ejercite dicho derecho de tal modo, que si dicho derecho se ejercita ante el responsable del fichero de morosos (la empresa especializada titular del fichero común) éste deberá comunicar al solicitante toda la información que conste en sus ficheros sobre el mismo, además de las evaluaciones y apreciaciones que pudieran haberse realizado en los últimos seis meses con el correspondiente nombre y dirección de los cesionarios. Mientras, que, en el caso de ejercitar dicho derecho ante un fichero de una entidad participante en el sistema; ésta deberá comunicar toda la información a la que tenga acceso, así como las señas del fichero común donde estén inscritos los datos.

Sin embargo, es conveniente recalcar, como ya se hizo en apartados anteriores, que el derecho de acceso no puede ser utilizado para obtener información ajena al titular, como, por ejemplo, aquella relativa al funcionamiento interno del fichero. Así lo demuestra la Sentencia de la Audiencia Nacional del 12 de febrero de 2014, cuando dice "*Pero es que además, se solicita también información sobre extremos que no son propiamente datos de carácter personal, como los cambios de configuración del servicio, dispositivo empleado para el cambio de contraseña, entrega de una copia de seguridad, etc. Por ello, la petición excede del cauce establecido para el derecho de acceso en el ámbito de la protección de datos personales regulada en la LOPD"*.[89]

[88] Articulo 15 LOPD.
[89] SAN de 12 de febrero de 2014, FJ 4º.

Con respecto a los derechos de rectificación y cancelación, el artículo 44.3 RLOPD, establece una serie de plazos específicos, que dependen para su concreción de la entidad o persona contra la que se ejerza la solicitud de estos derechos, expuestos a continuación:

- 7 días, si se ejercita contra el titular del fichero común, para que comunique a quién le facilitó los datos y éste se pronuncie sobre la solicitud de estos derechos. De no recibir respuesta dentro de este plazo el titular del fichero deberá rectificar o cancelar de forma preventiva los datos en cuestión.
- 10 días, si se ejercita contra quien facilitó los datos al fichero común, para que rectifique o cancele los datos dentro de sus ficheros y lo comunique tanto al fichero común como al interesado en el caso de hacerlo.
- 10 días, si se ejercita contra una entidad participante al sistema pero que no hubiera facilitado dichos datos al fichero común, para que comunique tal circunstancia e indique las señas del fichero común al interesado.

Cuestión obligada resulta, una vez tratados estos plazos especiales, volver a abordar el tema de la conservación de los datos, o dicho de otro modo el tema del bloqueo. Pues como bien establece el marco jurídico de protección de datos antes de eliminar los datos por medio de cancelación estos deben ser conservados por un periodos de tiempo determinado para ponerlos a disposición de los jueces y tribunales en caso de que así lo soliciten, pero sin poder el responsable o encargado acceder ni disponer de los mismos ni mucho menos dejar acceder a terceros.[90]

Así pues, el plazo de conservación de los datos es difícil de establecer. Habrá que atender al caso concreto como manifiesta la AEPD, en su Informe Jurídico 0408/2010, *"resulta imposible establecer una enumeración taxativa de los períodos en que el dato habrá de permanecer bloqueado".* No obstante, en ese mismo Informe se establecen

[90] Téngase en cuenta que el proceso de bloqueo se debe llevar a cabo tal como indica la AEPD, en su Informe Jurídico de 5 de junio de 2007, de forma*: "que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia".*

una serie de criterios para llegar a determinar el plazo a aplicar. Las conclusiones del Informe son las siguientes: [91]

1. *"En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, además de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto "en las disposiciones aplicables" o a la "atención de las posibles responsabilidades nacidas del tratamiento", tal y como prevé dicha Ley."*

2. *"En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes)."*

3. *"A los períodos mencionados en el informe citado cabe añadir el plazo de prescripción de 3 años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave, sin perjuicio de que otras normas con rango de Ley, en aquellos concretos sectores en los que actúe en representación o defensa de su cliente, puedan establecer otros plazos de conservación de los datos."*

[91] Véase: Informe Jurídico 0408/2010, Agencia de Española de Protección de Datos, Gabinete Jurídico, pp. 2 y 3.

De estos criterios se puede llegar a observar que el bloqueo cuenta con una gran disparidad de plazos, dispersos por el ordenamiento jurídico y cada uno de ellos con su propia duración. Además, dichos plazos tienen que venir impuestos por una norma con rango de ley y en concreto en relación con la normativa aplicable al caso concreto o con la responsabilidad que dicho tratamiento haya podido producir.

En consecuencia, para poder determinar el plazo del bloqueo o el tiempo por el que se conservarán los datos, dentro del ámbito de los registros de morosos, debemos estar a lo dispuesto en la normativa aplicable y al plazo de la prescripción de las responsabilidades nacidas por el tratamiento. Y por tanto, debemos acudir al RLOPD, en concreto a su artículo 44 con su plazo de 6 años de conservación, como normativa aplicable, aunque también debemos tener en cuenta 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[92] (LOPCDH, en adelante), en concreto su artículo 9.5 con su plazo de 4 años de caducidad, como plazo de interposición para las acciones de protección frente a intromisión ilegitima en el derecho al honor, intimidad y la propia imagen. Dentro de la compleja cuestión de la responsabilidad en el ámbito de los registros de morosos se hace más probable que el afectado ejercite sus acciones de protección por medio del derecho al honor, ya que su plazo de "caducidad" es superior al de la acción de responsabilidad extracontractual y la inclusión errónea en uno de estos registros es también *de facto* una vulneración a dicho derecho.

No obstante, dichos plazos se pueden ver alterados, pues la responsabilidad, aquí tenida en cuenta, tiene como inicio del cómputo para el plazo de caducidad, desde, o bien, cuando los datos dejan de estar incluidos en el registro, o bien, el titular de los datos es conocedor de tal hecho. Sin perjuicio de que, en caso de que exista una acción penal pueda plantearse la prejudicialidad penal para suspender el plazo de caducidad.[93]

Igualmente, para acabar con la explicación referida a la problemática de los derechos ARCO dentro de los registros de morosos y antes de pasar a explicar la tutela ofrecida por el ámbito civil, es necesario hacer mención al último de estos derechos, el derecho

[92] 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 (BOE de 14 de Mayo de 1982, núm.115)
[93] Véase al respecto, STS de 16 de julio de 2015, FJ. 9º.

de oposición. El mismo no se ve afectado por lo establecido en el artículo 44 RLOPD, ya que su aplicación a los registros de morosos resulta muy reducida (por no decir casi imposible), pues resulta difícil imaginar el motivo requerido por el artículo 34.1 RLOPD *"legítimo y fundado, referido a su concreta situación personal"*, que justifique el ejercicio del derecho de oposición.

La tutela complementaria ofrecida por el ámbito civil se fundamenta en la necesidad de dar respuesta al derecho de indemnización de daños y perjuicios reconocido por el artículo 19 LOPD a los titulares de los datos, que hayan sufrido algún perjuicio por el mal uso de sus datos, ya que la AEPD y los órganos jurisdiccionales del ámbito contencioso-administrativo, que conocen de sus resoluciones, no son competentes para conocer sobre las indemnizaciones entre particulares ni mucho menos para cuantificarlas.[94]

Asimismo, la tutela complementaria ofrecida por el ámbito civil puede manifestarse tanto en una acción de responsabilidad (contractual o extracontractual) que es en realidad la acción que recoge el artículo 19 LOPD, como en una acción de protección del derecho al honor [95] . Igualmente, es necesario concretar que la acción de responsabilidad en el ámbito civil sólo podrá ser ejercitada contra el caso de ficheros de titularidad privada (artículo 19.3 LOPD), mientras, que en el caso de ficheros de titularidad pública se deberá ejercitar una acción de responsabilidad, pero en el ámbito contenciosos-administrativo y bajo el régimen de responsabilidad de las Administraciones públicas (artículo 19.2 LOPD). No obstante, en el presente trabajo nos vamos a detener en la defensa por medio del derecho al honor por ser la más relacionada con los registros de morosos. Ya que la inscripción errónea en un fichero de morosos es de por sí una vulneración al derecho al honor.

En consecuencia, para llegar a entender mejor la tutela ofrecida por este ámbito es necesario hacer una pequeña aproximación a lo que entiende la jurisprudencia por

[94] Téngase en cuenta que cuando sea una Administración pública la que haya hecho un mal uso de los datos personales, los órganos jurisdiccionales del ámbito contencioso-administrativo si serán competente para conocer del asunto de la indemnización.
[95] Véase a este respecto Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., p. 556.

derecho al honor, para así tener una mejor compresión de lo que implica para el titular de los datos la inscripción en un registro de morosos.

En relación con lo que entiende la jurisprudencia por el derecho al honor garantizado por el artículo 18.1 CE, y sin ánimo de profundizar mucho sobre la cuestión, podemos citar algunas Sentencias: la Sentencia del Tribunal Constitucional 180/1999, de 11 de octubre, cuando expone: *"El "honor", […], es un concepto jurídico normativo cuya precisión depende de las normas, valores e ideas sociales vigentes en cada momento, de ahí que los órganos judiciales dispongan de un cierto margen de apreciación a la hora de concretar en cada caso qué deba tenerse por lesivo del derecho fundamental que lo protege. No obstante esta imprecisión del objeto del derecho al honor, este Tribunal no ha renunciado a definir su contenido constitucional abstracto afirmando que ese derecho ampara la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que lo hagan desmerecer en la consideración ajena al ir en su descrédito o menosprecio o que sean tenidas en el concepto público por afrentosas"*[96]. Y la Sentencia del Tribunal Constitucional 219/1992, de 3 de diciembre, cuando dice "*derecho al respeto y reconocimiento de la dignidad personal que se requiere para el libre desarrollo de la personalidad en la convivencia social, sin que pueda "ser escarnecido o humillado ante uno mismo o los demás".*[97] En base a la lectura de ambas sentencias, podemos concluir, para lo que el objeto del trabajo importa, que el honor es la imagen que tienen las terceras personas sobre el titular del derecho.[98]

Así pues, resulta bastante comprensible la consolidación de la doctrina, que entiende que la inscripción errónea en los registros de morosos constituye una vulneración al derecho al honor[99]. No hay que olvidar que tal inscripción conlleva un fuerte elemento de descrédito que señala y marca a los titulares de los datos inscritos como incumplidores ante terceros, que planean entablar una relación contractual con ellos. Se produce, Además, una posible situación de riesgo de exclusión social, tal como manifiesta Julián Timoner Giménez, en su obra anteriormente mencionada, puesto que

[96] STC 180/1999, de 11 de octubre, FJ.4º.
[97] STC 219/1992, de 3 de diciembre, FJ. 2º.
[98] Téngase en cuenta a este respecto que, aunque, el derecho al honor tiene una concepción más profunda y compleja su estudio y características no son objeto de este trabajo y por lo tanto no se va a profundizar sobre el mismo.
[99] Véase al respecto Rubio Torrano. Enrique, "*Inclusión indebida en fichero de morosos intromisión ilegítima en el derecho al honor". Aranzadi civil-mercantil. Revista doctrinal*, Nº. 7 (noviembre), 2012, p. 94, o en su defecto; STS de 24 de abril de 2009, FJ.2º.

la inclusión en los registros de morosos *"... implica la negación de una plena autonomía del individuo al carecer de las condiciones que en una sociedad desarrollada se requieren y exigen para una plena integración en la esfera económica de ésa sociedad, por la imposibilidad de acceso a los servicios financieros, al aparecer como moroso."*[100]

Una vez llegado a este punto resulta necesario tratar sobre las características propias que tiene dicho ámbito, con respecto a la protección de datos que juega un papel instrumental respecto de las garantías de otros derechos, como en este caso, del derecho al honor. La vulneración del derecho al honor se recoge en el articulo 7.7 LOPCDH y este a su vez requiere, por medio del articulo 2 LOPCDH, que no haya una previsión legal que lo justifique. Justificación que vendría por el cumplimiento de la normativa de protección de datos. Por lo tanto si se incumple con la del derecho a la protección de datos, de forma indebida se lesiona el derecho al honor. Este es una vez producida la inclusión indebida en el registro de morosos se produce *de facto* una vulneración al derecho al honor, para la cual es indiferente que haya llegado a ser conocida por terceros tal como expone la Sentencia del Tribunal Supremo del 24 de abril de 2009, por *"ciudadano particular o profesionalmente comerciante, se ve incluido en dicho registro, lo cual le afecta directamente a su dignidad, interna o subjetivamente e igualmente le alcanza, externa u objetivamente en la consideración de los demás, ya que se trata de un imputación de un hecho consistente en ser incumplidor de su obligación pecuniaria que, como se ha dicho, lesiona su dignidad y atenta a su propia estimación, como aspecto interno y menoscaba su fama, como aspecto externo. 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. Sí, 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".*[101]

[100] Timoner Giménez, Julián, "*Una visión crítica…",* cit., p. 90.
[101] STS de 24 de abril de 2009, FJ.2º, último párrafo.

Para acabar, con la tutela ofrecida por el ámbito civil en lo que respecta al derecho a la protección de datos es necesario recalcar que, a diferencia del ámbito contencioso-administrativo, el ámbito civil si es competente para conocer de todas las vicisitudes que rodean a los registros de morosos, en concreto, de todas las circunstancias que rodean a la existencia, certeza y veracidad de la deuda, de forma definitiva.

3.3. En relación con las obligaciones del responsable.

En relación con las obligaciones del responsable la gran mayoría de las mismas ya han sido tratadas en apartados anteriores, como es el caso de responder a las solicitudes del ejercicio de los derechos ARCO (apartado III.3.2 **"***En relación con el derecho de los titulares especial mención al derecho al honor"*) o la obligación de asegurarse del respecto a los principios del tratamiento (apartado III.3.1 *"En relación con los principios del tratamiento"*). Por lo que a ellos nos remitimos.

Igualmente, se hace necesario para tratar las obligaciones del responsable recordar de forma sucinta el funcionamiento de los ficheros de morosos, consistente en la actuación "conjunta" de dos tipos de ficheros diferentes e independientes entre sí, los ficheros de los acreedores que inscriben los datos y el fichero común, o registro de morosos de los que es responsable otra organización diferente y en donde se vierten dichos datos esto es, a donde se ceden los datos. De la descripción de éste funcionamiento se entiende la existencia de dos responsables diferenciados: los acreedores, por un lado, y la empresa especializada titular del fichero común, por el otro, ambos responsables con sus propias obligaciones y por ende sus propias responsabilidades.

En lo relativo a las obligaciones de los acreedores versan, básicamente, en el respeto a los principios del tratamiento y en el cumplimento de los derechos ARCO. Así pues, como dichas obligaciones ya han sido tratadas en apartados anteriores a ellos nos remitimos. Aquí cabría plantearse si la comunicación que realiza el acreedor a la empresa responsable del fichero común cumple con los citados principios del tratamiento de datos, y especialmente, si se ha cumplido con el requisitos del consentimiento. Si éste era necesario. En caso de no cumplirlo, lógicamente, el acreedor estará vulnerando el derecho.

No obstante, en el presente apartado se tratará principalmente sobre la responsabilidad en la que puede incurrir el responsable titular del fichero común y sobre la figura del encargado del tratamiento, que, aunque, su designación no sea del todo obligatoria, si tiene un gran peso en el cumplimento de las obligaciones, sobre todo en aquellas, que debido a su especialización, requieren o aconsejan el uso de terceros especializados, tales como, por ejemplo, las medidas de seguridad referidas a procedimientos informáticos.

En lo que respecta a la responsabilidad en que puede incurrir el responsable titular del fichero común hasta hace poco se consideraba que los acreedores eran los únicos que debían responder de la veracidad y calidad de los datos, dejando así al responsable titular del fichero común como un tercero ajeno, cuyas únicas obligaciones eran: servir de mero intermediario entre el acreedor y el titular inscrito para las cuestiones relacionadas con los derechos ARCO, asegurarse de inscribir bien los datos proporcionados por el acreedor de acuerdo a sus instrucciones, presente y futuras. Se pensaba que la comprobación de la veracidad y calidad de los datos podrían sobrepasar sus competencias.[102]

No obstante, con el pronunciamiento del Tribunal Supremo en su Sentencia del 21 de mayo de 2014, se ha entendido que el hecho de que el titular del registro de morosos sea considerado un tercero en dicha relación no le excluye de la obligación de velar por el cumplimento del principio de calidad de datos, dentro de sus competencias; y, en especial, cuando se trata de atender a las solicitudes de los derechos ARCO, ni le posibilita para tomar una actitud pasiva ante tal circunstancia. Así se entiende de la sentencia anteriormente mencionada cuando expone: *"La interpretación de estas normas reglamentarias no puede llevar a que el responsable del "registro de morosos", esto es, la empresa titular del fichero común en el que se incluyen los datos sobre incumplimientos de obligaciones dinerarias procedentes de los ficheros de distintos acreedores, esté excluido de la obligación de velar por la calidad de los datos, y, por tanto, de cancelar o rectificar de oficio los que le conste que sean no pertinentes, inexactos o incompletos. Como responsable del tratamiento de los datos obrantes en el registro de morosos del que es titular, le compete atender la solicitud de cancelación o*

[102] Véase a este respecto Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 540 y ss.

rectificación del afectado cuando la misma sea suficientemente fundada porque los datos incluidos en el fichero no respetan las exigencias de calidad derivadas de las normas reguladoras del derecho. Y por las mismas razones ha de responder de los daños y perjuicios causados al afectado cuando se hayan incumplido estas obligaciones". A esta consideración hay que unirle lo dicho por esa misma Sentencia unos párrafos más abajo: "*Esta previsión reglamentaria no puede interpretarse de modo que cuando el interesado haya ejercitado sus derechos de rectificación o cancelación de forma motivada y fundamentada, justificando ante el titular del fichero común el incumplimiento de los requisitos de calidad de los datos, éste no pueda y no deba rectificar o cancelar los datos no pertinentes, inexactos o incompletos a no ser que así se lo indique el acreedor que le ha suministrado los datos. Esta interpretación supondría una restricción injustificada del derecho a la protección de datos del interesado y es por tanto inatendible. Ha de tenerse en cuenta que el responsable del fichero común es quien comunica al afectado que sus datos han sido incluidos en el fichero, notificándole una referencia de tales datos e informándole de su derecho a recabar información de la totalidad de los datos, por lo que será frecuente que el derecho de rectificación o cancelación se ejercite frente al responsable del fichero común, que es el que constituye el "registro de morosos" y tiene una mayor potencialidad ofensiva pues puede ser consultado por terceros."*[103]

En consecuencia, a raíz de la Sentencia del 21 de mayo de 2014 del Tribunal Supremo, los titulares de los registros de morosos deben ser más cuidadosos a la hora de dar respuesta al ejercicio de solicitudes de los derechos ARCO, pues si de la documentación aportada por el titular de los datos se desprende la pertinencia de dichos derechos (rectificación o cancelación) deben llevarlos a cabo.

En la actualidad no es admisible que los titulares de los registros de morosos se desentiendan del cumplimento de los principios del tratamiento y denieguen el ejercicio de los derechos ARCO con base, únicamente, a que el acreedor se ha ratificado en los datos. Pues no se puede excusar el no cumplimiento de los principios del tratamiento, en la incorrecta idea de que como son los acreedores los que deben responder de la veracidad y calidad de los datos, basta únicamente con su afirmación para dar por

[103] STS de 21de mayo de 2014, FJ 8º; cuarto apartado; último párrafo, para el primero de los fragmentos, y misma sentencia, FJ 8; quinto apartado, párrafo tercero, para el siguiente fragmento.

cumplido dicha obligación. Los titulares de los registros de morosos deben hacer una comprobación efectiva del cumplimento de dichos principios.

Así pues, es necesario resaltar que, aunque el titular del registro de morosos sea un tercero en la relación jurídica que fundamente la inscripción en el registro (y, por tanto, no puede tener pleno conocimiento de todas las vicisitudes de la relación jurídica), es quien admite y publica, por propia voluntad. Ningún precepto obliga a crear este tipo de ficheros privados, ni muchos menos publicar este tipo de datos desfavorables. También se debe recalcar que su titular crea este tipo de fichero con el único fin de obtener un beneficio a cambio de proporcionar información sobre el incumplimiento de los titulares de los datos. [104]

Por todo ello, resulta bastante lógico la conclusión adoptada por la Sentencia, anteriormente mencionada, de que el titular del registro de morosos debe tener, al menos, un mínimo de diligencia a la hora de responder las peticiones del ejercicio de los derechos ARCO. Resulta del todo absurdo el establecer unos criterios restrictivos para la inscripción de los datos en los registros de morosos cuando es el propio titular del registro común el que se desentiende del cumplimiento de los mismos, bajo el pretexto de que es el acreedor; el obligado a responder de la veracidad y calidad de los datos.

Igualmente, hay que mencionar que no sólo el adecuado cumplimento de las solicitudes de los derechos ARCO pueden llegar a provocar que el responsable del fichero común incurra en responsabilidad por una negligencia en cuanto el cumplimento de esas obligaciones, sino que, además, también, puede incurrir en dicha responsabilidad por el incumplimiento de otras obligaciones relacionadas con el correcto cumplimiento de los principios legitimadores del tratamiento de datos, especialmente, en lo relacionado con el requisito del consentimiento. Así, pues hechos tales como proporcionar información a terceros fuera de los supuestos legales, o el no informar al titular de los datos sobre la inclusión de sus datos en el citado fichero.

[104] Para profundizar más sobre la responsabilidad del responsable del fichero de morosos véanse: Rubio Torrano, Enrique, **"***Responsabilidad del titular de un registro de morosos"*. *Aranzadi civil-mercantil. Revista doctrinal*, Nº. 6 (octubre), 2014, pp. 11-15, y también; Salas Carceller, Antonio, "La responsabilidad de las entidades que gestionan los llamados «ficheros de morosos". *Revista Aranzadi Doctrinal*, Nº. 2, 2015, pp. 103-109.

En lo relativo a quién puede se proporcionar la información que consta en el fichero de morosos, el titular del registro, como ya se ha dicho anteriormente, sólo puede proporcionar la información a un determinado tipo de personas, en concreto, a aquéllas que quieran establecer una relación jurídica con el titular de los datos, como bien se puede llegar entender de la lectura de los supuestos habilitantes del artículo 42 RLOPD. Sólo podrán acceder a la información los sujetos mencionados en dicho artículo, sin que quepa entender una interpretación extensiva permitida por aplicación directa del articulo 7.f) de la Directiva 95/46/C, tal como expone la AEPD, en su Informe Jurídico 0147/2013.[105] Así pues, sólo podrán tener acceso los casos en:

1. Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
2. Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
3. Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

El acceso a los datos por estos terceros específicos impide que la cesión o comunicación de datos sea considerada como una cesión ilícita, pero ello no elimina ni el descrédito que conlleva para los titulares de los datos dicha cesión. No obstante para que este tipo de cesiones sea lícita no basta con comunicarlo únicamente a un tipo determinado de personas, sino que, además, debe cumplir con todos los requisitos necesarios para la inscripción de los datos, de otro modo sería considerada como ilícita y por tanto una infracción grave del articulo 44.3.k). No hay olvidar que son cesiones sin el consentimiento del titular y sobre datos perjudiciales para la imagen del titular de los mismos.

En lo que respecta a la obligación por parte del responsable del fichero de comunicar la inscripción al titular de los datos, se encuentra recogida tanto en la LOPD, articulo 29.2 como en el RLOPD, articulo 40. Así pues, es una obligación más estricta que el requerimiento previo y no admite tanta libertad de medios, ya que desde un principio establece de forma clara sus requisitos, tales como:

[105] Véase: Informe Jurídico 0147/2013, Agencia de Española de Protección de Datos, Gabinete Jurídico, p. 1 a 3.

- Ser cumplida en el plazo de 30 días desde la inscripción, comunicando en la misma los datos inscritos y la posibilidad de ejercitar los derechos ARCO.
- Ser llevada a cabo por *"un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos"* (o dicho de otro modo, por medio de un encargado del tratamiento, a menos que tenga el consentimiento de cada titular para ceder los datos y que luego le notifique.)
- Las actuaciones a seguir dependiendo de si ha sido o no notificada la inclusión al titular de los datos, como, por ejemplo, en el caso de no conocer que si la notificación ha sido devuelta no podrá llevar a cabo el tratamiento, o en el caso de conocer la devolución de la notificación (por otra causa distinta a que haya sido rehusado por el titular de los datos) requerir al acreedor inscriptor que le acredite que la dirección utilizada para la notificación corresponde con la pactada contractualmente y hasta que no lo haga no podrá tratar los datos.

Asimismo, siguiendo el hilo de la explicación, pasamos a tratar la figura del encargado del tratamiento céntranos principalmente en el contrato que regula la relación entre el responsable y el encargado previsto en el artículo 12 LOPD. Dicho contrato no sólo regula la relación entre ambos, sino que, además, fundamenta la figura del encargado, tal como expone la Sentencia de la Audiencia Nacional del 19 de noviembre del 2003 *"para tener la condición legal de encargado del tratamiento, […] es necesario cumplir una serie de exigencias necesarias, que operan a modo de garantías, establecidas en el artículo 12 de la Ley Orgánica 15/1999. Así es, cuando el tratamiento se realice por cuenta de un tercero debe de constar "por escrito o en alguna otra forma que permita acreditar su celebración y contenido", por lo que no basta con acreditar que existe una relación jurídica entre el responsable del fichero y el encargado del tratamiento, sino que ésta ha de constar por escrito o por otra forma que permita acreditar su "celebración y contenido…"*[106]

Así pues, para que el contrato que regula las obligaciones entre ambos sea válido, el contrato debe estar escrito y hacer mención expresa a las cuestiones recogidas en el artículo 12 LOPD, además de otras relacionadas con el derecho a la protección de datos, expuestas a continuación:[107]

[106] Véase SAN de 19 de noviembre de 2003, FJ 4º y 7º.
[107] Álvarez Hernando, Javier / Cazurro Barahona, Víctor, "*Practicum Protección*…", cit., pp. 171 y ss.

- La descripción del servicio prestado.
- El carácter del servicio prestado por el encargado si es remunerado o no, y si va a ser temporal o indefinido.
- Que los datos sólo se tratarán conforme a las instrucciones del responsable del fichero.
- Que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas
- Las medidas de seguridad a que se refiere el artículo 9 LOPD que el encargado del tratamiento está obligado a implementar, de acuerdo al nivel de protección que esté obligado a implementar el responsable del tratamiento, o cualquier otra establecida por leyes especiales.
- La forma de devolución o destrucción de los datos de carácter personal una vez finalizado el encargo.
- La posibilidad de subcontratar servicios y los requisitos para llevar a cabo tal subcontratación.
- La obligación de respetar el deber de secreto durante la duración del tratamiento.

En resumen, la problemática práctica en que puede incurrir el responsable con respecto al encargado del tratamiento se centra, principalmente, en cómo están dispuestas en el contrato las obligaciones de la relación. Pues, no hay que olvidar que, a pesar de que el responsable haga uso de los servicios de un encargado, el responsable sigue respondiendo de las vulneraciones surgidas por el tratamiento, aunque en caso de que el encargado se desvié de las indicaciones establecidas por el responsable, éste también responderá de la vulneración provocada.

Asimismo, se debe recalcar la importancia que el encargado juega en el ámbito objeto del trabajo, pues como ya se ha dicho en su momento, muchas de las obligaciones a las que tiene que hacer frente el responsable tienen que hacerse o es conveniente que se hagan por medio de un encargado. Pero si el contrato es defectuoso o no está escrito, no sólo no se llegaría a realizar la obligación encomendada, sino que además, se estaría incurriendo en una falta leve por infringir el articulo 44.2.d) LOPD penado con multa de 900 a 40.000€. Sin contar con otras vulneraciones que dicho defecto provocaría.

Para acabar, piénsese, por ejemplo, en la obligación del responsable del fichero de informar al titular una vez que sus datos han sido inscritos. Si en dicho caso hubiera cualquier tipo de defecto en el contrato o las condiciones de llevarlo a cabo, no sólo nos encontraríamos ante la infracción del artículo 44.2d) (con las consecuencia anteriormente mencionadas), sino que además el cumplimiento de la propia obligación de informar estaría en entredicho, pues los datos que se comunicaron no se hicieron por medio de ninguna habilitación legal. Por consiguiente no sólo se debería responder de los defectos de dicho encargo sino también de los defectos y deficiencias producidos por los servicios prestados por el encargado.

IV. Conclusiones

La búsqueda de garantizar el derecho a la protección de datos dentro del ámbito de los ficheros de morosos no es una cuestión baladí, sino que es el reflejo de una búsqueda constante que intenta asegurar por medio de la imposición de rígidos principios y el establecimiento de medidas de seguridad igual de rígidas el respeto de un derecho fundamental. Además, dicha importancia se refleja en la obligación de cumplir con estrictos requisitos para poder tratar los datos personales ante la evidencia de que un tratamiento ilícito de los mismos tiene difícil reparación.

Así pues, es interesante comprobar cómo, a pesar de establecer unos criterios tan rígidos para el uso de los datos de carácter personal (principios del tratamiento, medidas de seguridad, etc.…), el marco de protección de datos intenta respetar el fundamento del derecho a la protección de datos, permitiendo a los interesados en última instancia decidir cómo llevarlo a cabo, siempre, con el respeto de los requisitos mínimos establecidos en la normativa.

No obstante, a pesar de las cautelas establecidas en relación con el tratamiento de los datos en los ficheros de morosos, los mismos han demostrado ser un dudoso mecanismo para determinar la capacidad económica de los titulares de los datos, además de un excelente medio de coacción para obligar a dichos titulares a hacer frente a sus obligaciones incumplidas bajo la pena del descrédito y la pérdida de futuras relaciones contractuales (entre las que se incluye, obviamente, la posibilidad de acceder a otro crédito).

Asimismo, dichos registros se han convertido *de facto* en un *"medio extraordinario de cobro"* utilizado por los acreedores para "motivar" a sus deudores a satisfacer las obligaciones que tuvieran pendiente con ellos. Ésta práctica se fundamenta en la asimetría de información que permiten estos registros, puesto que para inscribir una deuda sólo se requiere la información proporcionada por una de las partes, principalmente la del acreedor. Además, en ningún caso puede llegar a darse la situación contraria porque, en su mayoría, los incumplimientos producidos por los acreedores no son obligaciones dinerarias, y aunque lo fueran, el deudor no podría inscribirla, ya que no tienen la condición jurídica de responsable del tratamiento.

En la práctica, aunque la implantación de normas rígidas y la imposición de cuantiosas multas han conseguido frenar o, al menos, disuadir la utilización del registro de morosos como medio de coacción, no han conseguido parar del todo dicha práctica. Como se ha visto en el trabajo, no todos los principios tienen la misma importancia e interpretación que se quisiera. Así pues, lo vemos en la importancia del principio de finalidad, lo que lleva a que las inscripciones hechas en el registro de morosos con el único fin de coaccionar son una clara vulneración del principio de finalidad, permitiendo así proteger no sólo el derecho a la protección de datos, sino también el honor de la persona.

Igualmente, la indefinición de las características de la deuda tampoco ayuda a parar este tipo de práctica, pues la falta de criterios concretos en cuanto a sus características permiten, no sólo, que se inscriban obligaciones dinerarias procedentes de la casuística más dispar, sino que, además, dichas obligaciones sean tratadas de la misma forma sin tener en cuenta ningún otro criterio, de manera que un incumplimiento de una cuantía de 10 € será tratado de la misma manera que un incumplimiento de una cuantía muy superior, como, por ejemplo, 10.000 €.

Así pues, no es de extrañar la inscripción de deudas procedentes de cláusulas penales (deudas consensuales derivadas del incumplimiento de una obligación), las cuales, como ya dije en su momento, son ajenas al fin del registro de morosos, puesto que distorsionan la realidad de la obligación incumplida. Además, su inscripción fácilmente podría considerarse como una doble pena, la cantidad superior impuesta por no cumplir y el perjuicio a su imagen que la exposición de la pena provocaría.

Asimismo, y siguiendo con la problemática que permite la inscripción de cláusulas penales, es necesario resaltar uno de los problemas más relevantes que se produce para el derecho a la protección de datos, dentro del ámbito de los registros de morosos: la dificultad de dar una respuesta adecuada al cumplimiento del derecho a la protección de datos por medio del ámbito contencioso-administrativo, pues muchas de las circunstancias que rodean éstos registros son del ámbito civil, lo que debería ser tenido en cuenta, pero la AEPD y los órganos judiciales que conocen de sus recursos no pueden pronunciarse sobre las mismas por exceder de sus competencias.

Sin embargo, a pesar de todo, tampoco se puede llegar a afirmar que los registros de morosos sean un mecanismo del todo inseguro e inservible para enjuiciar la solvencia económica del titular los datos, ni tampoco que busquen por sí mismos ser un medio de presión para el cobro de una deuda.

Así pues, por un lado, los registros de morosos son capaces de advertir sobre verdaderos profesionales del incumplimiento, aunque también tenemos que indicar ciertas matizaciones al respecto, pues este tipo de ficheros no resultan tan efectivos con incumplidores primerizos o con la constatación de un solo incumplimiento, pues, en estos casos, dicho incumplimiento más que aportar información sobre su solvencia, aporta un claro desprestigio tanto a la relación inscrita (pues la señala como incumplida) como a la persona del titular de los datos (pues la marcan como incumplidora).

Por otro lado, la presión infundida por los registros no es un objetivo buscado por los mismos (o, al menos, no es su finalidad desde el punto de vista legal), ni tampoco es una situación que los registros de morosos puedan controlar una vez inscritos los datos. La presión viene dada por el comportamiento autónomo de aquellos terceros que ven los datos inscritos en el registro, y no porque una norma les obligue a adoptar una actitud de exclusión o les prohibía entablar relaciones contractuales con los titulares inscritos en el fichero. Además, hay que tener en cuenta, las estrictas medidas de seguridad impuestas para la protección de los datos personales, que intentan, en la medida de lo posible, salvaguardar los derechos de los titulares de los datos.

En consecuencia, a pesar de no buscar infundir tal presión y de las medidas impuestas para salvaguardar los derechos de los titulares, los registros de morosos no pueden evitar el descrédito y la presión, una vez inscritos los datos. Por lo tanto, lo único que pueden hacer para evitarlo es incrementar el control antes de publicar los datos, ya que, una vez publicados, el daño causado a los titulares de los datos resulta complicado de reparar. Y para ello se debe dar un estricto cumplimiento de los principios del tratamiento de datos, especialmente, los requisitos del consentimiento y de la información.

Por todo lo anterior, los ficheros de morosos han resultado ser un mecanismo bastante complejo, en donde no sólo se contraponen los intereses enfrentados de salvaguardar los derechos del titular de los datos, por un lado, y el interés de informar sobre su capacidad económica y evitar el peligro de nuevos incumplimientos, por el otro, sino que, además, está la dificultad añadida de tutelar el derecho a la protección de datos con un razonamiento de Derecho administrativo cuando las circunstancias que motivan tal vulneración tienen un marcado origen de Derecho civil. Por esta razón, no es de extrañar que, a pesar de todas las cautelas a veces sea difícil detener el uso incorrecto de los ficheros como medio de coacción, puesto que para determinar dicho uso es necesario poder profundizar en cuestiones que sobrepasan las competencias del ámbito contencioso-administrativo.

Así pues, el uso complementario de la jurisdicción civil para paliar el daño causado por el mal uso de los datos y, en última instancia, parar la práctica del uso de los registros de morosos como medida de coacción es una solución bastante eficaz, pues otras soluciones menos recomendables serian, por un lado, la opción de dejar en manos de la jurisdicción civil la tutela del derecho a la protección de datos para el resarcimiento del daño causado y, por el otro, la opción de aventurarse a una especie de solución mixta, permitiendo que relaciones contractuales nacidas con base a razonamientos de Derecho civil sean juzgadas a partir de razonamiento de Derecho administrativo, pero esto causaría inseguridad jurídica

Por consiguiente, la forma de mejorar el uso de estos ficheros puede parecer difícil y compleja, pero no imposible. Así pues, una posible forma de mejorar su funcionamiento, vendría por un cambio en la legislación en la que se establecieran

criterios extras para completar vacíos como la cuantía de la deuda o las características a tener en cuenta para determinar si cumple con el principio de finalidad, entre otros, o, por la creación de un fichero de anotaciones fallidas, en donde se recogieran todas las inscripciones fallidas. Incluso se podría mejorar el funcionamiento de estos ficheros por parte de las propias empresas titulares de los ficheros de morosos a través del uso de códigos tipos, sin necesidad de modificar la legislación.

En lo referente a un cambio de legislación para introducir criterios extra, opino que sería una medida un tanto gravosa, pues, por un lado, un cambio en el marco jurídico de protección de datos requeriría el correspondiente proceso legislativo (el cual puede llegar a alargarse mucho) y, por el otro, dicho cambio no aseguraría completamente que pueda llegar a solucionar todos los problemas, es más, puede llegar a solucionar unos problemas y crear otros. Por lo tanto, me remito a los criterios sugeridos en los códigos tipos

Así pues, la creación de un registro de inscripciones fallidas consistiría en la creación de un fichero público, cuyo responsable seria la AEPD y tendría la función de disuadir el uso incorrecto de los ficheros de morosos señalando a todo aquel que hiciera un mal uso de los mismos. Y, por ende, sólo perjudicaría, a aquellos que hicieran mal uso de los ficheros. De manera que si un acreedor inscribe sin las debidas garantías se vería perjudicado y desprestigiado, pero en cambio si cumpliera con las garantías no le pasaría nada.

Una cuestión interesante seria preguntarse si es posible, *de facto*, evitar el desprestigio producido por los ficheros de morosos por medio de un código tipo, pues con la simple indicación de que la inscripción ha sido fallida se podría redirigir el desprestigio al acreedor que inscribió.

Creemos, por lo tanto, que los códigos tipos serían una medida más recomendable que el cambio de legislación pues su creación es más sencilla y se adaptan de una mejor forma al ámbito en que son aprobados, ya que son los propios responsables (conocedores tanto de las practicas de su ámbito de actuación como de sus propios recursos) los que lo elaboran, además en caso de necesidad el proceso para su modificación sería mucho más rápido que un cambio legislativo. No obstante, su

eficacia dependería del número de empresas titulares de ficheros comunes; que hicieran este tipo de códigos tipo o se adhiriesen.

Para acabar, queremos concluir que consideramos que los registros de morosos son un mecanismo de dudosa eficacia. Reitero mi opinión de que no miden la capacidad, sino la fiabilidad, y cuyos efectos adversos han tenido un mayor protagonismo que la finalidad buscada. No obstante, los registros de morosos pueden llegar a ser una gran herramienta para determinar la fiabilidad de los titulares de los datos, siempre y cuando se establezcan medidas o se ejecuten los cambios legislativos necesarios, para evitar la inscripción de deudas ajenas a la finalidad de los ficheros y dirijan el desprestigio a aquellos que no hagan un correcto uso de dichos ficheros.

V. Bibliografía

- Álvarez Hernando, Javier / Cazurro Barahona, Víctor, *"Practicum Protección de Datos 2015",* Aranzadi, Pamplona, 2014, pp. 167 – 335, 439 – 452, 481 – 500 y 521 – 573.
- Carrasco Perera. Ángel, "*Cuidado con la inclusión de un cliente en un registro de morosos por el impago de cláusulas penales". Revista CESCO de Derecho de Consumo*, Nº. 17, 2016, pp. 252 y 253.
- Hualde Manso. María Teresa, "*Ficheros de morosos, nulidad del Reglamento de Protección de Datos y derecho al honor". Aranzadi civil-mercantil. Revista doctrinal, Nº. 8 (diciembre)*, 2013, pp. 49-58.
- Linares Gutiérrez, Antonio, "El chantaje de los ficheros de morosos: el principio de finalidad como requisito para la inclusión de datos en los ficheros sobre solvencia patrimonial y crédito: tratamiento jurisprudencial". *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, Nº 1, 2014, pp. 113-126.
- Rubio Torrano, Enrique, **"***Responsabilidad del titular de un registro de morosos". Aranzadi civil-mercantil. Revista doctrinal*, Nº. 6 (octubre), 2014, pp. 11-15.
- Rubio Torrano. Enrique, "*Inclusión indebida en fichero de morosos intromisión ilegítima en el derecho al honor". Aranzadi civil-mercantil. Revista doctrinal*, Nº. 7 (noviembre), 2012, pp. 91-95.
- Salas Carceller, Antonio, "*La responsabilidad de las entidades que gestionan los llamados «ficheros de morosos". Revista Aranzadi Doctrinal*, Nº. 2, 2015, pp. 103-109.
- San Martín Arias. Ignacio, "*Protección de datos en el crédito al consumo". Aranzadi, Pamplona*, 2015, pp. 49 – 71.
- Timoner Giménez, Julián, "*Una visión crítica de los registros de morosos: alegalidad de los mismos". Aletheia: Cuadernos Críticos del Derecho*, Nº. 1, 2009, pp. 68-113.

VI. Jurisprudencia

- STC 292/2000, de 30 de noviembre.
- STC 180/1999, de 11 de octubre.
- STC 219/1992, de 3 de diciembre.
- STS de 16 de febrero de 2016.
- STS de 16 de julio de 2015.
- STS de 21 de mayo de 2014.
- STS de 6 de marzo de 2013.
- STS de 15 de julio de 2010.
- STS de 24 de abril de 2009.
- STS de 5 de junio de 2004.
- SAN de 19 de julio de 2016.
- SAN de 22 de marzo de 2016.
- SAN de 21 de marzo de 2014.
- SAN de 19 de marzo de 2014.
- SAN de 12 de febrero de 2014
- SAN de 13 de diciembre de 2013.
- SAN de 3 de diciembre de 2013.
- SAN de 30 de mayo de 2012.
- SAN de 15 de marzo de 2012.
- SAN de 10 de junio de 2011.
- SAN de 16 de mayo de 2011.
- SAN de 11 de marzo de 2011.
- SAN de 1 de octubre de 2010.
- SAN de 9 de enero de 2009.
- SAN de 28 de mayo de 2008.
- SAN de 8 de enero de 2006.
- SAN de 19 de noviembre de 2003.
- SAN de 3 de marzo de 2000.

VII. Otra documentación.

- Informe jurídico 0453/2013, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0348/2013, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0147/2013, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0144/2012, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0408/2010, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0227/2010, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0237/2009, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Informe Jurídico 0287/2006, Agencia de Española de Protección de Datos, Gabinete Jurídico.
- Resolución de la AEPD de 22 de enero del 2001.