

UNIVERSIDAD
INTERNACIONAL
DE LA RIOJA

unir

La regulación de los ficheros de solvencia patrimonial y de crédito en el nuevo RGPD: La causa de legitimidad del tratamiento.

Trabajo fin de máster presentado por:

Titulación:

Directora:

Doña Carlota García Poveda

Máster en Protección de Datos

Doña Mónica Arenas Ramiro

ÍNDICE

I. INTRODUCCIÓN.....	5
II. CUESTIONES BÁSICAS EN EL TRATAMIENTO DE DATOS PERSONALES.....	7
2.1 Sujetos que intervienen.....	7
2.2 Principios.....	7
2.3 Derechos y obligaciones.....	13
III. LOS FICHEROS DE SOLVENCIA PATRIMONIAL.....	18
3.1 Sujetos que intervienen.....	18
3.2 Principios.....	19
3.3 Derechos y obligaciones.....	21
IV. LA CAUSA DE LEGITIMACIÓN DEL RESPONSABLE DEL FICHERO DE SOLVENCIA PATRIMONIAL.....	25
4.1 Regulación por la Directiva 95/46/CE, la LOPD y el RLOPD.....	25
4.2 Criterio de la Agencia Española de Protección de Datos.....	30
4.3 El cambio del Reglamento General de Protección de Datos 679/2016.....	32
V. CONCLUSIONES.....	35
BIBLIOGRAFÍA	

LISTADO DE ABREVIATURAS Y SIGLAS

- AEPD Agencia Española Protección de Datos
- Art./arts. Artículo/artículos
- GT29 Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE
- LOPD Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- RDLOPD Real Decreto 1720/1997, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD
- RGPD 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 (Reglamento general de protección de datos)
- STC Sentencia del Tribunal Constitucional
- STJUE Sentencia del Tribunal de Justicia de la Unión Europea
- STS Sentencia del Tribunal Supremo

RESUMEN

El presente trabajo tiene por objeto analizar las posibles modificaciones en torno a los ficheros de solvencia patrimonial y de crédito introducidas por el nuevo Reglamento General de Protección de Datos. Dichas modificaciones se van a analizar en torno a los principios, derechos y obligaciones y causa de legitimidad del tratamiento.

PALABRAS CLAVE

Causa de legitimidad del tratamiento

Derechos y obligaciones en el Reglamento General de Protección de Datos

Fichero de morosos

Fichero de solvencia patrimonial y de crédito

Principios en el Reglamento General de Protección de Datos

I. INTRODUCCIÓN

El Reglamento General de Protección de Datos (en adelante, RGPD) entrado en vigor en mayo de 2016 y aplicable a partir del 25 de mayo de 2018, es una norma de aplicación directa en toda la Unión Europea, relativo a la protección de los datos de las personas físicas¹. Se estableció un margen de dos años desde su entrada en vigor a su aplicación directa a fin de que los Estados miembros adecuaran su normativa nacional al mencionado Reglamento.

La nueva normativa nacional aún no se encuentra publicada, por lo que si bien el RGPD deroga expresamente en su artículo 94 la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 a partir del 25 de mayo de 2018, guarda silencio en cuanto a la legislación nacional de cada país ya que es una norma de aplicación directa que no necesita transposición. Ello supone que mientras en España no se publique la nueva Ley Orgánica de Protección de Datos tendremos el siguiente panorama: aplicación directa del RGPD, y aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y del 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 (RDLOPD), en todo lo que no sea incompatible con el RGPD.

Los ficheros de solvencia patrimonial y de crédito encuentran su regulación actualmente en el artículo 29 de la LOPD y artículos 37 a 44 del RDLOPD, en tanto que el nuevo Reglamento no realiza ningún tipo de alusión directa a los conocidos “ficheros de morosos”. No obstante, introduce innovaciones que, de manera indirecta, van a afectar a los ficheros de solvencia patrimonial, sus responsables y el modo de efectuar el tratamiento, en concreto, los relativos a la causa de licitud del tratamiento y los derechos de los titulares de los datos.

Por lo tanto, el objeto del presente trabajo es el estudio de la regulación que el Reglamento General de Protección de Datos realiza sobre los ficheros de solvencia patrimonial y de crédito, en cuanto a la causa de licitud del tratamiento y los derechos de los interesados, realizando un estudio de los antecedentes más próximos a la regulación de

¹ 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 (Reglamento general de protección de datos).

La regulación de los ficheros de solvencia patrimonial y de crédito en el nuevo RGPD: La causa de legitimidad del tratamiento.

los conocidos como “ficheros de morosos”. La finalidad es entender los cambios producidos, por lo que previamente se analizará este objeto en la actual LOPD y su reglamento de desarrollo.

II. CUESTIONES BÁSICAS EN EL TRATAMIENTO DE DATOS PERSONALES

2.1 Sujetos que intervienen

En todo tratamiento de datos existen diversos agentes que pueden llegar a actuar en distintas etapas del mismo, y cuyos objetivos y funciones son diferentes².

La figura principal, y sin la cual no existe un tratamiento de datos, es el responsable de tratamiento, siendo definido por el RGPD en su artículo 4.7 como aquella persona física o jurídica que decide los fines y medios del tratamiento, y en el artículo 3.d) de la LOPD como aquella persona física que decide los fines, contenido y usos del tratamiento. Es fundamental por tanto, para distinguir al responsable de otros sujetos que pueden intervenir en un momento dado, que decida las finalidades del tratamiento, es decir, a qué se van a destinar, y cómo se van a recabar, usar y eliminar los mismos.

Por su parte, el encargado de tratamiento es definido por el RGPD en su artículo 4.8 como aquella persona física o jurídica que trata los datos por cuenta del responsable, y en el mismo sentido el artículo 3.g) de la LOPD como aquella persona física o jurídica que trata datos personales por cuenta del responsable.

Por lo tanto, la diferencia entre ambos estriba en que el responsable es el que decide sobre todo el ciclo de vida de los datos, siendo la actividad del encargado dirigida por el primero, sin que quepa otro tipo de actuación que ceñirse a las instrucciones dadas por el responsable.

2.2 Principios

El responsable de un tratamiento debe observar una serie de principios que han de guiar su actuación, a fin de que ésta se adecue al cumplimiento normativo pertinente. Tras la nueva regulación introducida por el RGPD se mantienen principios que ya se contenían plasmados en la legislación anterior, y se introducen algunos nuevos cuya posición en el

2 El tratamiento es definido por el Art. 4.2) RGPD como: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

ordenamiento pasan a ser de vital importancia. En el art. 5 del RGPD bajo la rúbrica “Principios relativos al tratamiento” se enumeran una serie de principios, los cuales vamos a examinar y comprobar las diferencias en relación a la legislación anterior.

a) Principio de transparencia

En primer lugar se establece la obligación de que los datos sean tratados de manera lícita, leal y transparente heredándose de la legislación anterior, y consistiendo la importante innovación en añadir la obligación de transparencia³. Si bien pudiera parecer que el cambio es insignificante, lo cierto es que en todo el cuerpo normativo del RGPD encontramos numerosas referencias a la transparencia, mostrando el interés del legislador en dotar de protección a las personas físicas en toda la Unión a través de un Reglamento que proporcione una mayor seguridad jurídica. Podíamos entender que el Considerando 39 resume el principio de la transparencia al señalar que, *“el principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo”*. Es voluntad del legislador que las personas físicas tengan conciencia sobre los datos que se están recogiendo, utilizando y tratando, y que conozcan en qué medida sus datos personales están siendo usados, con el fin de que conozcan los riesgos a que están expuestos, así como los derechos que les conciernan. Así se recoge en los Considerandos 13 (transparencia para dotar de seguridad a los operadores jurídicos), 39 (requisitos del principio transparencia), 58 (reiteración de los requisitos del principio), 78 (la transparencia como medida para cumplir con los principios de privacidad desde el diseño y por defecto) y el Considerando 100, donde se abre la posibilidad de utilizar mecanismos de certificación que garanticen la transparencia por parte del responsable del tratamiento .

El hecho de que el legislador haya hecho tanto hincapié en este principio denota una importante preocupación por el desconocimiento de los interesados acerca del tratamiento de sus datos (los cuales, en una gran mayoría, y hasta la publicación del RGPD, desconocían totalmente el uso que se está dando a sus datos personales). Es importante destacar que el principio de transparencia ha sido definido también por el Grupo de Trabajo del Artículo 29⁴ como *“el requerimiento de que cualquier información y*

³ Art. 5 RGPD: Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado (“licitud, lealtad y transparencia”).

⁴ El Grupo de trabajo del art.29 fue creado por el mencionado artículo de la Directiva 95/46/CE y está compuesto por un representante de la autoridad de control designadas por cada Estado miembro, por un representante de la

comunicación relacionados con el procesamiento de datos personales sea de fácil acceso y de fácil entender, usando un lenguaje claro y sencillo”⁵.

El principio de transparencia se concreta en una obligación de los responsables de facilitar a los interesados información sobre determinados puntos que aparecen definidos en el art. 13 RGPD para el supuesto de que los datos hayan sido obtenidos del propio interesado, y en el art. 14 RGPD para los casos en que la información no se haya obtenido del propio afectado.

Es por tanto, una de las principales bases fundamentales en las que se debe articular el tratamiento de datos por parte del responsable, debiendo ser guiada su actuación por la transparencia, desde el inicio del tratamiento hasta el fin. Dicha transparencia se hace efectiva, en virtud del art. 14 RGPD, facilitando al interesado en el caso de que los datos no se hayan obtenido de él (como ocurre en los supuestos de los ficheros de solvencia patrimonial y de crédito), la identidad y datos de contacto del responsable, los datos de contacto del delegado de protección de datos, los fines y base jurídica del tratamiento (en el caso de los ficheros de solvencia patrimonial y de crédito la base jurídica será el interés legítimo del responsable), la categoría de datos personales, los destinatarios de los datos personales, la realización de transferencias internacionales, el plazo durante el cual se van a conservar sus datos personales, cuál es el interés legítimo del responsable, la posibilidad de ejercitar sus derechos (arts.15 y ss RGPD), el derecho a presentar una reclamación ante la Autoridad de control, la fuente de la que proceden sus datos personales y la existencia de decisiones automatizadas, incluida la elaboración de perfiles, si se llevan a cabo.

En el supuesto de que los datos se obtengan del propio interesado, antes de obtener los mismos, se le deberá ofrecer información acerca del plazo durante el cual se van a conservar sus datos, la existencia de derechos que puede hacer efectivos (arts.15 y ss RGPD), derecho a retirar el consentimiento si el tratamiento se basa en éste, derecho a presentar una reclamación ante la Autoridad de control; si la comunicación de los datos personales es un requisito legal o necesario para celebrar un contrato, las consecuencias de no prestarlo y la existencia de decisiones automatizadas, como puede ser la elaboración de

autoridad creada por las instituciones y organismos comunitarios y por un representante de la Comisión. Tiene carácter consultivo e independiente y sus principales misiones son estudiar las cuestiones relativas a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva que lo crea, emitir dictámenes sobre el nivel de protección existente tanto en la Comunidad como en países terceros, asesorar a la Comisión en materia de protección de datos, formular recomendaciones, emitir dictámenes sobre códigos de conducta, entre otras.

5 GT29.*Directrices sobre transparencia publicadas el 29 de noviembre de 2017.* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Consultado el 18.06.2018

perfiles (Art.13.2 RGPD). Además, durante toda la vida del tratamiento de datos personales el interesado puede solicitar al responsable del tratamiento información acerca de sus datos a través del denominado derecho de acceso, información que se concreta en la identidad y datos de contacto del responsable del tratamiento, los datos de contacto del Delegado de protección de datos en caso de que hubiere designado uno, los fines del tratamiento y la base jurídica del mismo, los intereses legítimos del responsable en el caso de que el tratamiento esté basado en el interés legítimo, los destinatarios de los datos personales y la existencia de transferencias internacionales (Art. 13.1 RGPD).

Entendemos, por tanto, que el principio de transparencia exige por un lado que el responsable del fichero cumpla con lo preceptuado en el RGPD e informe al interesado de los extremos recogidos en los arts. 13 y 14 del mencionado cuerpo normativo, en un lenguaje claro, sencillo y que resulte de fácil comprensión, y por otro lado, que se deban seguir cumpliendo los requisitos establecidos en la LOPD y el RDLOPD, en tanto que dicha legislación continúa vigente en todo lo que no contradiga el RGPD y no esté regulado por éste.

b) Principio de calidad y finalidad

En siguiente lugar, se establece como principio que los datos sean recogidos con “*fines determinados, explícitos y legítimos*” y que no sean tratados posteriormente con fines incompatibles a los iniciales, exigencia recogida en el art. 5.b) RGPD. No presenta ninguna variación respecto a la regulación nacional, y su interpretación no presenta mayor dificultad, ya que pretende evitar, a toda costa, la recogida de datos de manera indiscriminada sin contar con ninguna finalidad, finalidad que debe ser definida previamente a la recogida de datos. Se mantiene en la nueva regulación la misma salvedad contemplada en la legislación anterior, de que no se considerará como finalidad incompatible destinar los datos a fines de investigación científica, histórica o de investigación (art.5.b) RGPD).

c) Principio de minimización

En tercer lugar se establece en el Reglamento el principio de minimización de los datos, es decir, que sean “*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*”. Dicho principio deberá ser aplicado, sobre todo,

en el momento de diseñar y conceptualizar la empresa o entidad público en particular, analizar qué datos necesita, para qué los necesita y con qué fines serán tratados. Se trata de evitar recogida indiscriminada de datos, y por tanto, este principio guarda también relación con el nuevo concepto introducido por el Reglamento conocido como “*privacy by design*”, el cual implica que la privacidad se tenga en cuenta desde el diseño de la aplicación o servicio que vaya a tratar datos. En palabras de Ignacio García-Perrote Escartín y Jesús R. Mercader Uguina “*ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales sólo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos*”.⁶

Es necesario también conectar este principio con el nuevo concepto introducido por el RGPD en el art. 25.2, la llamada “*privacy by default*” la cual implica que “*El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas*”.

d) Principio de exactitud

Por otro lado, el principio de exactitud, establece que los datos personales serán “*exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan*” (art. 5.d RGPD). Este principio lo encontramos en el art.4 LOPD, e implica que los datos deben ser exactos y concordar con la situación real del interesado, rectificando los datos erróneos en el caso de que éstos fueran detectados.

⁶ García-Perrote Escartín, Ignacio y Mercader Uguina, Jesús R. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo al tratamiento de datos personales, un primer acercamiento. (2017:2)

e) Principio de conservación de los datos

El principio de *“limitación del plazo de conservación”*, es una obligación innovadora que no encontrábamos regulada de forma expresa en la legislación anterior, y establece que los datos sean *“mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales”* (Art.5.e RGPD). En algunos supuestos será la legislación sectorial o autonómica la que establezca plazos máximos de conservación, como ocurre, por ejemplo, con la legislación sanitaria, siendo en otros casos el propio responsable del tratamiento el que deberá de tomar una decisión individual y determinar el plazo de conservación pertinente. Se establece, por tanto, la obligación de establecer en todos los tratamientos un plazo razonable de conservación de los mismos.

f) Principio de integridad y confidencialidad

Se establece el principio de integridad y confidencialidad señalando que los datos personales serán *“tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (“integridad y confidencialidad”)*” (Art. 5.f)RGPD).

El cumplir con todos estos principios debe encuadrarse dentro de la llamada responsabilidad pro activa. En este sentido, el nuevo Reglamento introduce como uno de sus principales cambios los principios denominados *privacy by design* y *privacy by default* (privacidad desde el diseño y privacidad desde el defecto), los cuales destacan por su importancia y podríamos atrevernos a afirmar que supone un cambio radical en relación a la legislación anterior, obligando a todos los responsables a revisar sus tratamientos de datos, adecuándolos a estos principios, lo que supone revisar, examinar y cuestionar, desde un punto de vista subjetivo y conforme a unos parámetros propios, cómo se están llevando a cabo estos tratamientos de datos personales. Suponen una obligación para el responsable definida en el artículo 25 del RGPD donde se establece que desde el momento de determinar los medios del tratamiento, como en el momento del propio tratamiento, se deberán aplicar las medidas técnicas y organizativas adecuadas para asegurar la protección de los datos personales (privacidad desde el diseño);e igualmente se establece la

obligación, como apuntábamos anteriormente, de que “solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento” (privacidad por defecto)⁷. Según Ignacio García-Perrote Escartín y Jesús R. Mercader Uguina “Se impone la obligación de “responsabilidad proactiva” que exige a las organizaciones el establecimiento de medidas que garanticen y permitan demostrar el cumplimiento del Reglamento (esto es, políticas de protección de datos que no solo han de existir, sino que han de estar adaptadas a las circunstancias de la organización, implementadas y funcionar en la práctica). Desarrollando este principio general, el Reglamento establece la obligación de las empresas de tener en cuenta la protección de datos desde el momento del diseño de sus procedimientos, productos y servicios (privacy by design) y a que por defecto solo sean objeto de tratamiento los datos personales mínimos que sean necesarios para alcanzar el fin legítimo perseguido (privacy by default)”⁸.

2.3 Derechos y obligaciones

Los derechos de los interesados en el RGPD sufren pequeñas modificaciones introduciéndose alguno nuevo, y manteniéndose los derechos que ya aparecían reconocidos por la legislación anterior.

Se mantiene el derecho de acceso, reconocido en el art. 15 del RGPD en virtud del cual el interesado tiene derecho a conocer si el responsable del tratamiento está tratando sus datos personales, así como una serie de extremos que aparecen marcados en el mencionado título (fines del tratamiento, categoría de datos, destinatarios a quienes se comunicarán los datos, el plazo de conservación de los datos, derecho a solicitar rectificación o supresión, derecho a presentar una reclamación a la AEPD, información sobre el origen de los datos, la existencia de decisiones automatizadas y la existencia de transferencias internacionales). Existe el pequeño inciso de que el responsable facilitará

7 Art. 25.1 RGPD “Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados”.

8 García-Perrote Escartín, Ignacio y Mercader Uguina, Jesús R. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo al tratamiento de datos personales, un primer acercamiento (2017:3).

una copia de los datos personales al interesado , pudiendo percibir por cualquier otra copia solicitada un canon razonable basado en los costes administrativos. Supone un cambio respecto a la regulación contenida en la antigua LOPD que establecía la gratuidad del ejercicio de estos derechos, mientras que en la actualidad será gratuita la primera copia, pudiendo exigirse un *canon* para las posteriores.

El derecho de rectificación se regula en el art. 16 del RGPD y el derecho de limitación del tratamiento en el art. 19 del RGPD, siendo derechos de difícil efectividad por parte del interesado en los ficheros de solvencia patrimonial y de crédito, como luego veremos.

El derecho de supresión, que es lo que se ha venido a llamar “derecho al olvido” se regula en el art. 17 RGPD estableciéndose la obligación del responsable de suprimir los datos personales del interesado cuando concurra alguna de las siguientes circunstancias:

- Los datos ya no son necesarios para los fines que fueron recogidos.
- El interesado retira el consentimiento.
- El interesado se opone al tratamiento, ejercitando su derecho de oposición (art.21 RGPD).
- Los datos personales han sido tratados ilícitamente.
- Los datos personales deben suprimirse para el cumplimiento de una obligación legal.
- Los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información.

Continúa señalando el artículo que no se aplicará el derecho de supresión cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión, para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; por razones de interés público en el ámbito de la salud; con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; y para la formulación, el ejercicio o la defensa de reclamaciones. Entendemos que este artículo no es operable en los ficheros de solvencia patrimonial y de crédito, pues como veremos posteriormente la causa de licitud del tratamiento no se encuentra en el consentimiento, y por tanto, será irrelevante que el afectado intente retirar su consentimiento.

En los supuestos en que proceda rectificar, suprimir o limitar el tratamiento, el responsable del fichero de solvencia patrimonial debe notificar a cada uno de los destinatarios a los que se hayan comunicado los datos personales, estas circunstancias, a menos que sea imposible o exija un esfuerzo desproporcionado, en virtud del artículo 19 del RGPD.

Por último, se regula el derecho a la portabilidad de los datos en el art. 20 y el derecho de oposición en el art. 21 RGPD, entendiéndose que no son aplicables a los ficheros de solvencia patrimonial y de crédito, por no basarse el mismo en el consentimiento del interesado. En cuanto al derecho a la portabilidad se ha referido la AEPD estableciendo que *“El considerando 68 del Reglamento general de protección de datos ya introduce ciertos indicios relacionados con la naturaleza y alcance del derecho, aparte de los expresamente recogidos en el artículo 20 del citado Reglamento al que posteriormente se hará referencia. Así, se indica que el objeto del derecho es reformar aún más el control sobre sus propios datos por el afectado al que aquéllos se refieren, limitando el derecho, como señala el artículo 20.1 a los supuestos en que el tratamiento tiene como base jurídica el consentimiento del interesado o la existencia de un contrato y no cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, toda vez que en estos casos el tratamiento no depende de la propia voluntad del interesado que presta su consentimiento al tratamiento o al contrato”*⁹. En este caso, la AEPD examina una solicitud de informe remitida por la Asociación Española de Banca, en la que se plantean varias cuestiones en relación a la plena aplicación el día 25 de mayo de 2018 del RGPD y las dudas sobre su contenido.

Por tanto, entendemos que existen ciertos derechos que cuando el tratamiento no esté basado en el consentimiento o en la existencia de un contrato entre el interesado y el responsable del tratamiento, éstos no podrán hacerse efectivos, encontrándose limitados por la causa de licitud en la que se base el tratamiento en cuestión.

En el ejercicio de derechos por parte de los interesados comprobamos cómo confluyen ambas normativas, tanto la comunitaria como la nacional, al no resultar incompatibles entre si y complementarse perfectamente, mientras que en los arts. 14 y 15

9 Informe Jurídico de la Agencia Española de Protección de Datos 0195/2017

RGPD se establece qué información es la que se debe facilitar al interesado, en el art. 44 RDLOPD se establecen normas de carácter procedimental, es decir, cómo se gestionan las solicitudes de los afectados cuando se presentan en diferentes entidades.

Pasando a examinar las obligaciones de los responsables de los tratamientos tras la entrada en vigor del RGPD, destacar que el rol de los responsables ha cambiado drásticamente, estando obligados a acreditar cuatro aspectos clave que Jorge García Herrero en una entrevista realizada por Fernando J. Biurrún Abad los resume así:

“-Que se ha evaluado, y en caso necesario, rediseñado adecuadamente sus tratamientos de datos personales.

-Que las medidas de seguridad implementadas son adecuadas y eficaces.

-Que se aplica una política interna en materia de privacidad con obligaciones claras, acciones concretas anudadas a cada una, y se han designado responsables de su cumplimiento.

-Que exige ese mismo cumplimiento responsable a sus encargados de tratamientos y cadena de subcontratación.”¹⁰

Como mencionábamos anteriormente, se introduce por el Reglamento los conceptos de *privacy by design* y *privacy by default*, que básicamente suponen la obligación de todo responsable, en primer lugar, de aplicar las medidas técnicas y organizativa apropiadas para aplicar los principios de protección de datos, a fin de cumplir con el Reglamento; y en segundo lugar, de aplicar las medidas técnicas y organizativas apropiadas para que sólo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento.

Es decir, que cada responsable de manera pro activa analizará y examinará sus flujos de datos personales, cuestionando si son necesarios, y si están bajo la salvaguarda de las medidas de seguridad apropiadas a fin de evitar su alteración, pérdida o sustracción.

Y finalmente, el responsable tiene las obligaciones de notificar las violaciones de seguridad¹¹ a la AEPD (art. 33RGPD), elegir a encargados del tratamiento que cumplan con lo dispuesto en el reglamento, así como redactar por escrito los oportunos contratos (art.

10 Biurrún Abad, Fernando J. “Accountability” o responsabilidad activa en el Reglamento General de Protección de Datos (2017: 1-2).

11 Se entiende por violación de seguridad, según el art.4.12) del RGPD “Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.

La regulación de los ficheros de solvencia patrimonial y de crédito en el nuevo RGPD: La causa de legitimidad del tratamiento.

28 RGPD), y en definitiva cumplir con todas las medidas técnicas y organizativas que aseguren la protección de los datos personales (art. 25 RGPD).

III. LOS FICHEROS DE SOLVENCIA PATRIMONIAL

3.1 Sujetos que intervienen

Los ficheros de solvencia patrimonial que son aquellos cuya finalidad es determinar el cumplimiento o incumplimiento de obligaciones dinerarias por parte de los sujetos, consta de determinadas especialidades en relación al número de sujetos que intervienen. La AEPD determina que los sujetos que suelen intervenir en este tipo de tratamientos son cuatro: el deudor, el acreedor que notifica la deuda, el responsable del tratamiento de solvencia patrimonial y las entidades que consultan esa información.¹²

Podemos definir al deudor, en este sentido, como aquella persona física o jurídica que tiene la obligación de entregar una cantidad de dinero determinada y pasado el plazo no lo hace, siendo el acreedor aquella persona física o jurídica al que no se le entregó lo debido y notifica la deuda a un fichero de solvencia patrimonial y de crédito.

En tercer lugar, y en cuanto al responsable del tratamiento de solvencia patrimonial y de crédito, señalar que el art.29.4 LOPD establece que este tipo de ficheros sólo pueden registrar y ceder los datos de carácter personal que sean “*determinantes para enjuiciar la solvencia económica de los interesados*”. En opinión de Javier Álvarez Hernando, la cesión de los datos contenidos en los ficheros de morosidad se encuentra admitida siempre y cuando tenga por finalidad el enjuiciamiento de la solvencia económica de los interesados, siendo los datos necesarios para tal fin, y exigiéndose que la cesión quede delimitada por “*la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar*” (art. 11.3 LOPD).¹³

En último lugar, intervienen en este tipo de tratamientos aquellas entidades que solicitan información al fichero sobre la solvencia económica y patrimonial de aquellas personas con las que pretenden concertar un contrato de crédito, a fin de conocer si es fiable o no establecer tal relación jurídica con el sujeto en cuestión.

12 Agencia Española Protección de Datos. Protección de Datos: Guía para el ciudadano.

13 Álvarez Hernando, Javier. Guía práctica sobre protección de datos. Cuestiones y formularios (2011). <http://www.asesoriayempresas.es/articulo/JURIDICO/81037/proteccion-de-datos-requisitos-de-inclusion-en-un-fichero-de-morosos>. Consultado el 22-07-2018.

3.2 Principios

a) Principio de transparencia

En relación a los ficheros de solvencia patrimonial y de crédito, cabe destacar que este principio es plenamente operativo, aunque habrá que esperar a la nueva Ley Orgánica de Protección de Datos Personales para conocer con exactitud cómo se hará efectivo. En la LOPD y RDLOPD podemos considerar que el principio de transparencia, aún cuando no se use este nombre, implica cierta información que debe facilitarse al interesado, manifestándose en los siguientes requisitos a cumplir por el responsable del fichero¹⁴:

-Notificar al interesado por un medio auditable y fiable, que sus datos personales han sido registrados en el fichero de solvencia patrimonial y de crédito, así como informarles de su derecho a recabar la totalidad de la información de los datos que hubieren sido incluidos y de los derechos que le asisten. Esta comunicación se tiene que hacer por el responsable del fichero en el plazo de 30 días a contar desde la inclusión, y se deberá realizar una comunicación independiente por cada deuda que se incluya (Art. 29 LOPD, art. 40 RDLOPD).

-Si el interesado lo solicita, el responsable del fichero de solvencia patrimonial y de crédito debe comunicarle los datos y las evaluaciones y apreciaciones que sobre él se han comunicado durante los seis últimos meses y el nombre y dirección de la persona o entidad a quien se hubieran revelado los datos (Art. 29 LOPD)

-Se exige que antes de la inclusión en el fichero, el acreedor informe al deudor, en el momento de celebrar el contrato y, en todo caso, al tiempo de requerirle el pago de la deuda, de que en caso de no producirse el pago se le podrá incluir en el fichero de solvencia patrimonial y de crédito (art. 39 RDLOPD)

b) Principio de calidad y finalidad

En relación a este principio es importante destacar que en relación a los ficheros de solvencia patrimonial y de crédito la finalidad legítima se encuentra amparada por la causa de licitud del tratamiento denominada “interés legítimo del responsable” (art. 6.1.f) RGPD), cuyo estudio es objeto del siguiente epígrafe.

¹⁴ Consideramos vigentes los arts. 29 de la LOPD y los arts. 37-44 RDLOPD en tanto que el RGPD deroga expresamente la Directiva 95/46/CE, entendiéndose que se deroga de manera implícita toda normativa que le contradiga. En el caso de ficheros de solvencia patrimonial y de crédito, al no haber mención expresa en el RGPD, se considera vigente el articulado mencionado.

c) Principio de exactitud

El art. 38 del RDLOPD establece como requisito para la posibilidad de inclusión de una persona en el fichero de solvencia patrimonial y de crédito la *“existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobados por Real Decreto 303/2004, de 20 de febrero”*. Es decir, que es necesario, como manifestación del principio de exactitud, la existencia de una deuda cierta, vencida y exigible, concretando el art. 41 del mismo cuerpo normativo que sólo pueden ser objeto de tratamiento los datos que respondan en cada momento a la situación real de la deuda, eliminándose inmediatamente los datos del afectado en el supuesto de que la deuda haya sido cancelada. Con dicha previsión, se evita que pueda existir un fichero donde se contengan las deudas pasadas de una persona, así como que en dicho fichero únicamente pueda contener deudas ciertas, vencidas y exigibles.

Nuestro Tribunal Supremo se ha pronunciado en este aspecto en numerosas ocasiones, señalando que el principio de calidad de los datos, derivado del art. 4 de la LOPD exige que los datos personales recogidos para su tratamiento sean *“adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinandas, explícitas y legítimas para las que se hayan obtenido, exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado”*. Es interesante conocer que la STS 174/2018, de 23 de marzo de 2018 señala que no basta con que los datos que se incluyan en los registros de morosos sean ciertos y exactos, si no que además es necesario que sean pertinentes, pues puede ocurrir que dichos datos no sean determinantes para enjuiciar la solvencia económica de los interesados, entendida ésta como la negativa fundada a pagar la deuda. Sigue señalando nuestro Tribunal Supremo que en el supuesto de los ficheros que nos ocupan, además de la exigencia de que la deuda sea vencida y exigible, no puede ser incierta, dudosa, no pacífica o sometida a litigio, señalando que *“Si la deuda es objeto de controversia, porque el titular de los datos considera legítimamente que no debe lo que se le reclama, la falta de pago no es indicativa de la insolvencia del afecto. Puede que la deuda resulte finalmente cierta y por*

tanto pueda considerarse como un dato veraz. Pero no era un dato pertinente y proporcionado a la finalidad del fichero automatizado, porque este no tiene por finalidad la simple constatación de las deudas, sino la solvencia patrimonial de los afectados. Por ello solo es pertinente la inclusión en estos ficheros de aquellos deudores que no pueden o no quieren, de modo no justificado, pagar sus deudas”.

La STS 176/2013 de 6 de marzo manifiesta que la inclusión en los ficheros de solvencia patrimonial y de crédito no puede ser utilizada por las grandes empresas para cobrar las cantidades que estiman pertinentes, dado que los consumidores pueden no estar de acuerdo con dichas cantidades que se reclaman, pero no poder costearse los gastos de un procedimiento judicial, y constituir por tanto dicha inclusión, en una presión ilegítima.

Por tanto, el principio de exactitud así como el de calidad o minimización de los datos exigen en los ficheros de solvencia patrimonial y de crédito, no sólo que los datos sean exactos, si no que además dichos datos sean pertinentes para evaluar la solvencia patrimonial del afectado, no pudiendo constituir la inclusión, bajo ningún concepto, en una medida de presión para forzar el pago de deudas que pueden resultar ilegítimas.

d) Principio de conservación de los datos

En el supuesto de los ficheros de solvencia patrimonial y de crédito, dicha limitación aparece contemplada en la legislación anterior de manera expresa en el art. 38.1.b) RDLOPD cuando establece como requisito para la inclusión de los datos “*que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico*”¹⁵.

3.3 Derechos y obligaciones

En el supuesto concreto que nos ocupa, los llamados ficheros de morosos, los derechos que incumben al interesado encuentran su regulación específica en el art. 44 RDLOPD, el cual seguirá siendo de aplicación siempre que no contradiga al RGPD y

15 En el mismo sentido el art. 29.4 LOPD cuando establecía que “Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos”.

mientras no entre en vigor la normativa nacional pertinente. En primer lugar, y en relación al derecho de acceso se establecen una serie de particularidades:

- Si la solicitud se dirige al titular del fichero, no existe mayor problema, debiendo el titular informar de los datos que obran en el fichero (entendemos que se deberá informar de lo preceptuado en el arts. 14 y 15 del RGPD).

- Si la solicitud se dirige frente a otra entidad que no es el titular del fichero, ésta deberá comunicar los datos a los que ella puede acceder, así como la identidad y la dirección del titular del fichero, para que tenga acceso al resto de los datos (se deberán facilitar todos los datos relacionados en el art. 14 y 15 del RGPD).

Si se ejercita el derecho de cancelación o rectificación, se observarán las siguientes normas:

-Si la solicitud se dirige al titular del fichero, será éste quien adopte las medidas oportunas para trasladar la solicitud a la entidad que haya facilitado los datos, ordenando la rectificación o cancelación cautelar de los mismos si no recibe respuesta en el plazo de siete días.

-Si la solicitud se dirige a la entidad que ha comunicado los datos al fichero común, ésta procederá a rectificar o cancelar los mismos en plazo de diez días.

-Si la solicitud no se dirige a ninguna de las otras dos entidades, ésta informará al afectado sobre este hecho en el plazo de diez días, informando además de la entidad y dirección del titular del fichero para que pueda ejercitar sus derechos ante el mismo.

Como obligaciones concretas a los responsables de ficheros de solvencia de crédito y patrimonial establecidas en el RGPD, entendemos que, en primer lugar, deben realizar una Evaluación de impacto relativa a la protección de datos regulada en el art. 35 RGPD, ya que es un tratamiento que entraña un riesgo para los derechos y libertades de las personas. No obstante, dicho tratamiento no se encaja, hasta que la AEPD manifieste lo contrario, en ninguna de los supuestos en que sin ningún género de duda debe realizarse dicha evaluación. El art. 35.2 RGPD establece la obligación de realizar la misma cuando:

-Exista una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles¹⁶. En el supuesto que nos ocupa no existe una evaluación sistemática que se base en un

16 Art.4.4) RGPD “Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física”.

tratamiento automatizado, si no que el tratamiento se basa en datos financieros aportados por supuestos acreedores a un tercero a fin de que se conozca la existencia de la deuda por otros operadores económicos.

-Tratamiento a gran escala de categorías de datos especiales o condenas e infracciones penales. El tratamiento objeto del presente trabajo utiliza datos financieros e identificativos, pero no datos referentes a origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud, vida sexual u orientación sexual; ni datos relativos a condenas penales.

-Observación sistemática a gran escala de una zona de acceso público.

A pesar de que los ficheros de solvencia patrimonial y de crédito no encajan con ninguno de los supuestos en los que claramente se debe realizar una evaluación de impacto, entendemos que dada su incidencia sobre los derechos fundamentales y libertades públicas de las personas físicas, es recomendable que se realice. El apartado 4 del art. 35 establece que la AEPD publicará una lista de los tipos de operaciones que requieran una evaluación de impacto, publicación que al día de hoy no ha tenido lugar, pero que prevemos que incluirá los datos relativos a supuestos deudores.

Entendemos, al igual que con la Evaluación de Impacto, que es recomendable que el responsable de los ficheros de solvencia patrimonial y de crédito, designen a un Delegado de Protección de Datos. El art. 37 RGPD establece que el responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

- el tratamiento sea llevado a cabo por una autoridad u organismo público (excepto los tribunales).

- las actividades principales consistan en operaciones de tratamiento que requieran una observación sistemática y habitual de interesados a gran escala.

- las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales.

Al igual que en el caso de la evaluación de impacto, existe cierta incertidumbre sobre si los ficheros de solvencia patrimonial requieren la designación de un delegado de protección de datos. No obstante, mientras no se pronuncie la AEPD, entendemos más que recomendable su designación, dada la repercusión del tratamiento de la información que

provocan este tipo de ficheros, y la gravedad de la afectación en los derechos fundamentales del individuo.

Otra obligación aplicable al responsable del fichero de solvencia patrimonial y de crédito es realizar un registro de actividades, conforme lo ordenado y expresado en el art.30 RGPD. El registro de actividades no es obligatorio para aquellas empresas que empleen a menos de 250 trabajadores, a menos que el tratamiento pueda suponer un riesgo para los derechos y libertades de los interesados y que no sea ocasional, tal y como es el caso de los ficheros de solvencia patrimonial y de crédito.

IV. LA CAUSA DE LEGITIMACIÓN DEL RESPONSABLE DEL FICHERO DE SOLVENCIA PATRIMONIAL

4.1 Regulación por la Directiva 95/46/CE, la LOPD y el RLOPD

El responsable de un tratamiento de datos personales debe contar con una causa que legitime dicho tratamiento a fin de que el mismo pueda considerarse lícito. La normativa comunitaria y nacional ha regulado de manera taxativa las causas de licitud del tratamiento de datos personales, siendo la causa que legitima el tratamiento de los datos personales en los ficheros de solvencia patrimonial y de crédito, el interés legítimo del responsable, al no ser posible obtener el consentimiento del interesado. Resulta evidente que ningún usuario que pueda resultar perjudicado, va a dar su consentimiento a fin de que se le incluya en un fichero de solvencia patrimonial y de crédito, siendo el objetivo de estos ficheros, precisamente, incluir datos relativos a deudas contraídas que afectan negativamente a la esfera jurídica de los afectados. Es por ello que, dentro de las mencionadas causas de legitimación, estos ficheros se han amparado desde su creación en “el interés legítimo del responsable o de un tercero”.

La Directiva 95/46/CE establecía en la Sección II bajo el epígrafe “Principios relativos a la legitimación del tratamiento de datos”, en su artículo 7 que “*Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado*”.

Por su parte, nuestra LOPD, redactó en su artículo 6.2 el interés legítimo como causa legitimadora del tratamiento al siguiente tenor “*No será preciso el consentimiento(...) o cuando los datos figuren de fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*”

Fue con motivo del artículo 10.2.b) del RDLOPD, que se elevó por parte de nuestro Tribunal Supremo una cuestión prejudicial al TJUE, dando lugar a la Sentencia del

Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C-469/10)¹⁷.

El artículo 10.2.b) RLOPD exigía como causa de legitimación para que un tratamiento de datos pudiera efectuarse, además de que fuera necesario para la satisfacción del interés legítimo del responsable del tratamiento o por el tercero, y que no prevalecieran el interés o los derechos y libertades fundamentales del interesado, que dichos datos proviniesen de fuentes accesibles al público.

El TJUE señaló que *“los Estados miembros no pueden ni añadir al artículo 7 de la Directiva 95/46 nuevos principios relativos a la legitimación de los tratamientos de datos personales ni imponer exigencias adicionales que vendrían a modificar el alcance de alguno de los seis principios establecidos en dicho artículo”*. Nuestro Tribunal Supremo declaró nulo el artículo 10.2.b) del RLOPD, a fin de que nuestra normativa nacional se ajustase a lo dispuesto por la Directiva 95/46/CE, entendiéndose por tanto, que era causa legítima para el tratamiento de los datos personales cuando concurriesen dos requisitos¹⁸:

- El interés legítimo del responsable del tratamiento.
- Que no prevaleciesen los derechos y libertades fundamentales del interesado.

No declaró nulo el citado artículo 6 de la LOPD, en tanto que el Tribunal Supremo carece de competencia para anular normas con rango de ley, pero tal y como establece en su sentencia el TJUE el artículo 7.f) de la Directiva tiene efecto directo, dado que *“es una disposición suficientemente precisa para poder ser invocada por un particular y aplicada por los órganos jurisdiccionales nacionales. Además, si bien no puede negarse que la Directiva 95/46 confiere a los Estados miembros un margen de apreciación más o menos grande para la aplicación de algunas de sus disposiciones, el citado artículo 7, letra f), enuncia, por su parte, una obligación incondicional”*¹⁹.

Por lo tanto, comprobamos cómo desde la Directiva 95/46/CE la causa de legitimación para tratar datos personales podía sustentarse en el interés legítimo del

17 En dicha sentencia se resuelve la cuestión prejudicial que tenía por objeto la interpretación del art.7.f) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en tanto que el art. 10.2 del RDLOPD 1720/2007 exigía que los datos objeto de tratamiento que no contaran con el consentimiento del interesado debían provenir de fuentes accesibles al público. Contra este artículo la Asociación Nacional de Establecimientos Financieros de Crédito y la Federación de Comercio Electrónico y de Marketing Directo plantearon un recurso contencioso-administrativo, decidiendo el Tribunal Supremo suspender el procedimiento y plantear la cuestión prejudicial al TJUE sobre la interpretación citada.

18 Sentencia del Tribunal Supremo 8 de febrero de 2012.

19 Art.1.1 de la ya derogada Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contenciosa-Administrativa.

responsable siempre que no prevaleciesen los derechos fundamentales de los interesados, sin necesidad de concurrencia de ningún requisito más.

Ahora bien, ¿qué se entiende por interés legítimo? Nos encontramos con un concepto jurídico indeterminado, que no aparecía definido ni en la Directiva ni en ninguna norma nacional. Es por ello que el Grupo de Trabajo del Artículo 29 y con motivo de la publicación de las sentencias mencionadas emite un informe ofreciendo ciertas pautas para acotar el término “interés legítimo”, y por tanto poder realizar la ponderación pertinente a fin de comprobar si se vulneran o no los derechos de los interesados.

Para el Grupo del Artículo 29 el interés está relacionado con el concepto de “finalidad”²⁰. Así, la “finalidad” es el motivo por el cual los datos personales son tratados, mientras que el “interés legítimo” supone el beneficio que puede obtener el responsable, o incluso la sociedad, cuando realice el tratamiento de datos. En este sentido, el “interés” debe ser claro, de manera que permita realizar el “balance de intereses”. En ocasiones, este “interés” está estrechamente vinculado al interés que busca la colectividad, como sería el caso de publicar datos relacionados con la corrupción o investigaciones científicas. En otras, nos podemos encontrar que lo que existe es un “interés” económico de una compañía por conocer sus clientes potenciales. No obstante, se debe precisar que el hecho de que el responsable tenga un “interés legítimo” no supone la aplicación efectiva del artículo 7.f) de la Directiva, ya que es necesario realizar un balance de “intereses” con los derechos fundamentales de los afectados.

Para que el interés sea legítimo, el GT29 exige que sea lícito, es decir, conforme a la legislación nacional y de la Unión Europea; suficientemente concreto, lo que requiere que quede claramente delimitado y definido; y representativo de un interés real y actual, es decir, que no sea especulativo²¹.

Una vez se ha establecido y afirmado la existencia del interés legítimo del responsable, es necesario dar el siguiente paso, es decir, comprobar que no prevalecen los derechos y libertades fundamentales de los interesados, es la denominada “ponderación de intereses”. El GT 29 estableció en su dictamen una serie de cuestiones a fin de que sus

20 El Grupo del Art.29 elaboró el Dictamen 06/2014, de 9 de abril de 2014, sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE <http://ec.europa.eu/newsroom/article29/news-overview.cfm>. Consultado el 18.06.2018

21 Benito Martín, Ruth. Blog jurídico “Con la venia, señorías”. <https://conlaveniasenorias.com/2017/08/31/examen-del-interes-legitimo-como-base-del-tratamiento-de-datos/>. Consultado el 18.06.2018.

respuestas arrojaran luz a los responsables del tratamiento y pudieran establecer como causa de licitud el interés del responsable, o no. Estas preguntas son:

- 1. ¿Coincide el interés legítimo del responsable o de un tercero con un derecho fundamental, un interés público o un interés de la comunidad en general aun cuando éste no se encuentre legalmente estipulado?*
- 2. ¿Concurren en el tratamiento algún elemento característico de otras bases jurídicas que, aunque no pudiendo legitimar por sí solo el tratamiento, sí aporte refuerzo al interés legítimo? (Por ejemplo, si se obtuvo el consentimiento del interesado, aunque no en el modo que exige el RGPD para que dicho consentimiento pueda actuar como base jurídica).*
- 3. ¿Existe reconocimiento jurídico, cultural o social de la legitimidad del interés? Es decir, si se puede contar con directrices, políticas, recomendaciones, guías, declaraciones, manifiestos, demandas sociales, etc., que impulsen la consecución del interés legítimo. En realidad, este podría ser un subtipo de la primera cuestión o una forma de demostrar que aquella se da positivamente.*
- 4. ¿El análisis de riesgo del tratamiento o una evaluación de impacto en protección de datos sobre el mismo, arroja un resultado de riesgo alto para los derechos y libertades fundamentales de los interesados?*
- 5. ¿El tratamiento afecta negativamente a algún otro derecho fundamental de los interesados?*
- 6. ¿Se tratan datos de categorías especiales?*
- 7. ¿Se revelan los datos al público o a un gran número de personas?*
- 8. ¿Se combinan dichos datos con otros obtenidos por otras vías o de otras fuentes?*
- 9. ¿Les cabe esperar a los interesados que sus datos puedan ser objeto del tratamiento en cuestión o para la finalidad del mismo?*
- 10. ¿La/s categoría/s de interesados cuyos datos son objeto del tratamiento en cuestión pertenecen a un segmento más vulnerable de la población (menores, personas con discapacidad, solicitantes de asilo o refugio, víctimas de violencia de género, víctimas de terrorismo, etc.)?*
- 11. ¿Se deriva del tratamiento algún beneficio para los interesados?*
- 12. ¿Cuál es el grado de invasión en la privacidad de los interesados (bajo, medio o alto)?*

13. *¿Cuál es la duración del tratamiento (una semana o menos, 1 mes, 3 meses, 6 meses, 1 año, más de 1 año...)?*
14. *¿Cuál es la frecuencia del tratamiento (puntual, esporádica, continua)?*
15. *Al margen del nivel de invasión en la privacidad de los interesados y del riesgo que conlleve el tratamiento para éstos, ¿cabe esperar que el tratamiento en sí mismo les ocasione algún perjuicio o consecuencia negativa?*
16. *¿Existe relación directa entre el responsable los interesados?*
17. *¿Mantiene el responsable una posición dominante respecto a los interesados?*
18. *¿Existe algún tipo de contraprestación o compensación a favor de los interesados por el tratamiento de sus datos?*

La ponderación de intereses implica que cuando dos derechos colisionan, y el ejercicio de uno supone el detrimento de otro, es necesario que las limitaciones que sufren los derechos estén justificadas en la protección de otros derechos o bienes constitucionales, incurriéndose en arbitrariedad en caso contrario. En palabras de Vicente Guasch Portas y José Ramón Soler Fuensanta *“La aplicación del artículo 7.f) exige una prueba de equilibrio: lo que es necesario para los intereses legítimos de una de las partes con los intereses o los derechos fundamentales y las libertades de las personas afectadas. El resultado de la prueba de equilibrio determina si el artículo 7.f) puede ser invocado como motivo legal para el tratamiento. El GT29 entiende que la naturaleza abierta de esta disposición no significa necesariamente que esta opción deba ser vista en el sentido de que solo puede utilizarse para llenar los vacíos de situaciones raras e imprevistas como último recurso si no se aplica ningún otro motivo. Pero tampoco puede verse como una opción preferida por medio de un uso indebidamente ampliado porque sería considerada menos restrictiva que el resto de opciones del artículo 7”*²².

Para el GT29 a la hora de realizar la ponderación y conocer si prevalece el interés de uno u otro sujeto es necesario tener en cuenta el interés legítimo del tratamiento, es decir, si nos encontramos ante el ejercicio de un derecho fundamental, un interés general u otros intereses legítimos; el impacto de los titulares de los datos, forma en que están siendo tratados los datos, expectativas del interesado, naturaleza de los datos; un balance provisional de cuál de los intereses o derechos prevalece, y por último, y en caso de que

22 Guasch Portas, Vicente y Soler Fuensanta, José Ramon. “El interés legítimo en la protección de Datos”. Revista de derecho UNED, NÚM 16 (2015: 428)

prevalezca el interés legítimo del responsable ofrecer garantías adicionales para poder llevar a cabo el tratamiento (limitar volumen de los datos, por ejemplo).

En los ficheros de solvencia patrimonial y de crédito, por tanto, colisionan el derecho fundamental a la intimidad y a la vida privada del sujeto afectado por la inclusión de sus datos económicos en un fichero, que en nuestro texto constitucional se garantiza en el artículo 18 CE, y el derecho a la seguridad económica del resto de los sujetos que se ven favorecidos por la publicidad de estos datos, que lo podemos encuadrar en el art. 40 de la CE, prevaleciendo en dicha ponderación, el interés general a la seguridad económica en el tráfico jurídico. En este aspecto también se pronunció nuestro Tribunal Constitucional en la sentencia de 26 de noviembre de 1984, señalando que si bien los datos económicos de una persona forman parte de la esfera de su intimidad, no existe un derecho absoluto a su intimidad, y por tanto su protección no es ilimitada²³.

Por su parte, el artículo 6 LOPD establece que no será necesario el consentimiento del interesado cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos. Como hemos visto, se trata de dos requisitos acumulativos, es decir, que para que el responsable del fichero de solvencia patrimonial y de crédito pueda tratar los datos, es necesario además de que figuren en fuentes accesibles al público, que se trate de satisfacer un interés legítimo del responsable. No fue declarado nulo por el Tribunal Supremo por carecer de competencia para ello. Por su parte, el RDLOPD, en su artículo 10.2. a) establece que no será necesario el consentimiento del interesado cuando el tratamiento de datos tenga por objeto la satisfacción de un interés legítimo del responsable del tratamiento.

4.2 Criterio de la Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos emitió una Nota informativa el 24 de noviembre de 2011 con motivo de la publicación de la STJUE de fecha 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C-469/10) señalando que *“Ello no significa, sin*

²³ En el Fundamento Jurídico 5 de la Sentencia 110/1984 de fecha 26 de noviembre de 1984 el Tribunal Constitucional establece que *“Todo derecho tiene sus límites que en relación a los derechos fundamentales establece la Constitución por sí misma en algunas ocasiones, mientras en otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos (Sentencia 11/1981, de 8 de abril, fundamento jurídico 7, y Sentencia 2/1982, de 29 de enero, fundamento jurídico 5).*

embargo, que la mera invocación de un interés legítimo deba considerarse suficiente para legitimar el tratamiento de datos personales sin el consentimiento del afectado. En los fundamentos de la Sentencia, el propio Tribunal precisa la interpretación que debe darse a dicho artículo, subrayando la necesidad de realizar en cada caso concreto una ponderación entre el interés legítimo de quien va a tratar los datos y los derechos fundamentales de los ciudadanos afectados, con el fin de determinar cuál prevalece atendiendo a las circunstancias concurrentes. En este sentido, recuerda que el artículo 7 f) de la Directiva “establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado.”

Dicha ponderación exigida por el TJUE se había venido realizando tanto por la AEPD como por los órganos judiciales, atendido a criterios como la finalidad del tratamiento, la existencia de una Ley que amparase intereses legítimos u otras. Por lo que, en palabras de la AEPD de dicha sentencia *“no parece derivarse una alteración sustancial del marco vigente de protección de los datos personales en España ni que el fallo comporte una merma en el grado de protección de los derechos de los ciudadanos, si bien en el futuro será preciso acentuar la ponderación de las circunstancias que concurran en cada supuesto concreto para decidir sobre la legitimidad del tratamiento”*²⁴.

En este mismo sentido se pronuncia la AEPD en su Informe 0178/2012, señalando además, que para la ponderación de si prevalecen o no los derechos fundamentales de los ciudadanos sobre los intereses legítimos del responsable, se tendrá en cuenta si los datos obtenidos lo han sido de fuentes accesibles al público²⁵. Son fuentes de acceso público como establece el art. 3 LOPD únicamente las que dice la norma. Según criterio de la AEPD la mera invocación de un interés legítimo no puede considerarse suficiente para legitimar el tratamiento de datos personales sin el consentimiento del afectado.

La LOPD en su art.3.j) enumera taxativamente las fuentes accesibles al público, señalando en su inciso segundo que *“tienen la consideración de fuentes de acceso público,*

24 AEPD. Nota informativa de 24 de noviembre de 2011.

25 Informe AEPD 178/2012 se emite por la AEPD como consecuencia de la publicación de la Sentencia del Tribunal de Justicia de la Unión Europea en su sentencia de 24 de noviembre de 2011, así como de las Sentencias del Tribunal Supremo de 8 de febrero de 2012 por las que se anuló el apartado b) del artículo 10.2 del RDLOPD 1720/2007, de 21 de diciembre, recogándose la doctrina sentada por las Sentencias de la Audiencia Nacional de fechas 14 de mayo de 2009 y 21 de enero de 2010.

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

En otro Informe de la AEPD se exige en los supuestos que no se hayan obtenido los datos mediante consentimiento del interesado, que éste sea informado de forma expresa, precisa e inequívoca de la inclusión de sus datos en un registro²⁶.

En conclusión, podemos decir que el criterio de la AEPD viene siendo admitir el interés legítimo del responsable como causa de legitimación del tratamiento, pero no siendo suficiente alegar ésta para justificar el tratamiento de datos. La utilización de dicha causa debe reforzarse con la utilización de otro instrumento previo como es la realización de una ponderación previa. En la ponderación para saber si prevalecen los derechos fundamentales de los interesados o el interés legítimo del responsable, será relevante que los datos personales provengan de fuentes accesibles al público o no. No obstante, y en el supuesto de que no provengan de fuentes accesibles al público, no supondrá de manera automática que no pueda legitimarse el tratamiento de datos en cuestión.

4.3 El cambio del Reglamento General de Protección de Datos 670/2016

El Reglamento General de Protección de Datos dedica su artículo 6 a regular las condiciones que pueden determinar la licitud de un tratamiento de datos, estableciendo en su apartado 1.f) como causa de licitud que *“el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño”.*

Para que opere esta causa de licitud, es por tanto necesario que se cumplan dos requisitos:

²⁶ Informe AEPD 164/2008 y Art.5.4LOPD “éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo”.

- El interés legítimo del responsable del tratamiento.
- Que no prevaleciesen los derechos y libertades fundamentales del interesado.

Encontramos que la redacción de este artículo es similar a la establecida en el artículo 7.f) de la Directiva 95/46/CE, con la única salvedad de la mención específica que se realiza a los derechos del niño. De esta manera nos encontramos que, lo desarrollado tanto por el Grupo del artículo 29, como por las autoridades judiciales nacionales e internacionales, así como lo dictaminado por la Agencia Española de Protección de Datos, en cuanto a causa legitimadora del tratamiento de datos en los ficheros de solvencia patrimonial y de crédito seguirá plenamente vigente tras la entrada en vigor del nuevo Reglamento.

Ahora bien, el nuevo Reglamento desarrolla y completa lo previsto en la escueta normativa comunitaria anterior, que como hemos visto planteaba serias dudas en cuanto a determinados conceptos jurídicos indeterminados, y sobre los cuales tuvieron que elaborar y desarrollar doctrina diversos órganos e instituciones, tales como la Agencia Española de Protección de Datos, el Tribunal Supremo, el Tribunal de Justicia de la Unión Europea, entre otros.

De esta manera en el Considerando 47 del RGPD establece la posibilidad de que el interés legítimo del responsable constituya una base jurídica para el tratamiento, señalando que tal interés legítimo podrá darse:

- Cuando existe una relación pertinente y apropiada entre el interesado y el responsable.
- Cuando el interesado es cliente o está al servicio del responsable.

Ahora bien, se sigue exigiendo como *conditio sine qua non* que para que el tratamiento pueda ampararse en la base jurídica del interés del responsable, se haya realizado una evaluación meticulosa (en este sentido entendemos que se hace obligatoria la ponderación a la que hacíamos referencia con ocasión del dictamen del GT29). En esta ponderación de intereses, podrá prevalecer los derechos fundamentales del interesado, cuando se proceda al tratamiento de sus datos personales en circunstancias en las que el interesado no esperase razonablemente un tratamiento ulterior. Se recomienda que el interés legítimo no constituya la base jurídica del tratamiento de datos personales efectuado por autoridades públicas. Por último, en este Considerando se establece como

interés legítimo del responsable del tratamiento la prevención del fraude y el tratamiento de datos personales con fines de mercadotecnia directa.

El Considerando 48 RGPD permite, en base al interés legítimo, que un grupo empresarial pueda transmitir datos personales dentro de las empresas del mismo grupo para fines administrativos internos, incluido el tratamiento de datos personales de clientes y empleados, aplicándose esta regla aunque alguna de las empresas se encuentre en un tercer país. En relación al mismo, es importante recordar las particularidades establecidas por el art. 44 RDLOPD cuando señala los distintos supuestos que podían darse a la hora de que el interesado ejercitase sus respectivos derechos. Como bien apuntábamos anteriormente, el interesado podía ejercitar su derecho ante el titular del fichero, en cuyo caso no existía problemática, debiendo éste comunicar los datos personales del afectado que obrasen en el fichero y/o en el caso de que se ejercitase el derecho de cancelación o rectificación proceder a comunicarlo a la entidad que había facilitado los datos para que resolviese lo que procediera. El afectado podía ejercitar su derecho de acceso ante otra entidad participante en el sistema, pero que no fuera la titular del fichero, en cuyo caso comunicaría al interesado los datos a los que tuviera acceso, remitiendo al titular del fichero para los datos restantes, e igual remisión se haría para la efectividad de los derechos de cancelación o rectificación. Y, por último, en el supuesto de que se ejercitase el derecho de cancelación o rectificación ante la entidad que hubiera facilitado los datos, procedería ésta a resolver lo que procediese y a comunicarlo al titular del fichero si fuera pertinente.

V. CONCLUSIONES

Con la publicación del Reglamento General de Protección de Datos se estableció un plazo de dos años antes de su entrada en vigor a fin de que todos los Estados miembros tuvieran adaptadas sus normativas nacionales a la nueva norma comunitaria, de aplicación directa, pero cuyo cumplimiento efectivo exige de la voluntad legisladora nacional. Dicho plazo ha resultado insuficiente, tanto para los entes públicos como para los privados, no habiéndose publicado a fecha actual la nueva Ley Orgánica de Protección de Datos, y existiendo un panorama, cuanto menos peculiar, en tanto que el Reglamento se aplica desde el pasado 25 de mayo de 2018 de manera directa, pero existiendo supuestos a los cuales le son de aplicación la anterior normativa nacional al no estar regulados por la legislación comunitaria.

En primer lugar, destacar que el RGPD supone un cambio drástico y radical respecto a la forma en que se venían realizando los tratamientos de datos personales. Es voluntad, manifiestamente clara, del legislador, de dotar de una enorme transparencia y claridad a los tratamientos de datos personales. Atrás quedan los consentimientos oscuros y genéricos, en virtud de los cuales el interesado consentía de manera tácita, indiscriminada, sin voluntad ni conciencia de para qué prestaba su conformidad. Tras la entrada en vigor del Reglamento, existen obligaciones bien definidas para los responsables de los tratamientos, tanto en información que debe suministrarse al interesado, como la forma de prestar el consentimiento.

No es el consentimiento la causa de licitud de los ficheros de solvencia patrimonial y de crédito. No obstante, se les aplica, como a cualquier otro tratamiento, los mismos principios rectores de la nueva normativa en materia de protección de datos personales, como hemos podido ver. Por lo tanto, los titulares de los ficheros de solvencia patrimonial y de crédito, quedan directamente obligados a suministrar la información mencionada en los arts. 14 y 15 del RGPD, ya que aunque el tratamiento no tenga como causa de licitud el consentimiento, es necesario que los interesados conozcan determinados aspectos, tales como la identidad del responsable, fines del tratamiento, las fuentes de donde proceden los datos, entre otros aspectos. Dicha información en la que cristaliza el principio de transparencia, hay que añadir la normativa aplicable a los ficheros de solvencia patrimonial y de crédito regulada, aún, en la LOPD y en el RDLOPD. Por lo tanto, y en este supuesto particular, es necesario informar al afectado en el momento de celebrar el

contrato (de que sus datos podrán ser incluidos en un fichero de solvencia patrimonial y de crédito en el caso de impago), en el momento de requerir de pago, y en el momento de la inclusión efectiva. Se entiende que dada la gravedad, y los posibles perjuicios que puede suponer al afectado la inclusión en un denominado “fichero de morosos”, es necesario dotar la misma de mayor transparencia e información, con el fin de evitar, en la mayor medida posible, abusos por parte de las grandes empresas.

Cambio trascendental supone la introducción de los principios “privacidad desde el diseño” y “privacidad por defecto”, lo que implica un giro radicalmente opuesto a la forma en que se venía realizando el tratamiento de los datos personales. Anteriormente al RGPD, existían determinadas obligaciones que los responsables cumplían, sin entrar a analizar las características particulares en que incidían sus respectivos tratamientos, ni los riesgos a los que estaban expuestos los datos personales que trataban, ni qué incidencia tendría una violación de las medidas de seguridad en la vida de los particulares. Con la nueva normativa se pretende que cada responsable analice, de forma mucho mas profunda y particular, qué tipos de tratamientos está realizando, qué datos recaba y para qué, cuáles son los riesgos a los que está expuesto su tratamiento, qué supondría una fuga de información para los interesados, cuáles son las medidas idóneas para cada uno de sus tratamientos en particular. Este giro en la normativa viene motivado porque ya no es suficiente con catalogar los datos personales en función del tipo que sean (identificativos, bancarios, especialmente sensibles...), sino que hay que atender a otra serie de parámetros como el volumen de datos que se tratan, las cesiones a terceros, las transferencias internacionales, los usos y finalidades que se le va a dar a los datos (decisiones automatizadas, elaboración de perfiles, y un largo etcétera imposible de catalogar debido a la rapidez con la que evoluciona la tecnología, los usos y las finalidades de ésta). Es por ello, por la rapidez con la que evoluciona la tecnología, por cómo ésta puede incidir en los derechos y libertades de las personas, y por lo intrusiva que puede llegar a ser, por lo que el legislador apuesta por que cada responsable cuestione, decida y ponga en práctica, aquellas medidas necesarias para salvaguardar los derechos fundamentales y las libertades públicas de los seres humanos.

La “privacidad desde el diseño” implica que desde el momento mismo de la concepción del servicio/producto se tenga en cuenta la privacidad como un parámetro más. Es decir, que al diseñar el producto y/o servicio se haga teniendo en cuenta qué datos

se van a utilizar, a qué riesgos están expuestos, y cuáles son las medidas idóneas para mitigarlos o eliminarlos. Para ello, se crea un instrumento, la Evaluación de Impacto en la Protección de Datos Personales, a fin de que se obtengan las conclusiones pertinentes en relación a la seguridad del producto y/o servicio antes de comercializarlo. Junto esta “privacidad desde el diseño” se encuentra la “privacidad por defecto”, que implica que sólo se utilicen los datos estrictamente necesarios para la finalidad que se persigue, evitando a toda la cosa la acumulación indiscriminada de datos sin finalidades predeterminadas antes de la recogida de los mismos. En ambos casos, en relación con los ficheros de solvencia, debemos señalar que si tenían adaptados sus tratamientos a la normativa de protección de datos anterior a la publicación del RGPD, las medidas de seguridad aplicadas y las políticas de privacidad podrán suponer un buen punto de partida para cumplir con la nueva legislación. No obstante, los responsables deberán analizar y cuestionar los tratamientos realizados y las medidas de seguridad aplicadas, plasmando estos análisis en los instrumentos pertinentes (Evaluación de impacto o registro de actividades) para cumplir con las nuevas obligaciones establecidas por el RGPD.

Por otro lado, existen obligaciones genéricas que son de aplicación a los denominados “ficheros de morosos”, las cuales podemos resumir en ser transparentes en sus políticas de privacidad, realizar una evaluación de impacto sobre los datos personales, contar con un registro de actividades, y con contratos firmados por escrito con los encargados de tratamiento respectivos.

En relación a los derechos de los interesados, podemos concluir que pocas innovaciones existen en los ficheros de solvencia patrimonial y de crédito, manteniéndose prácticamente la misma regulación que existía anteriormente al Reglamento, y produciéndose pequeños cambios en cuanto al tipo de información que el titular del fichero debe suministrar al interesado. Si existen importantes novedades a nivel genérico, como es el derecho a la portabilidad y el derecho al olvido, ambos con poca incidencia en los denominados “ficheros de morosos”, ya que en cuanto a la portabilidad no le encontramos aplicación real, y en cuanto al derecho al olvido entendemos que ya existía este derecho reconocido de manera implícita en el art. 38.1.b) del RDLOPD al limitar la inclusión de los datos financieros al período de 6 años desde la fecha en que hubo de procederse al pago de la deuda (previsiblemente, y según consta en el anteproyecto de la

Ley Orgánica de Protección de Datos, este plazo disminuirá un año, en concordancia con los nuevos plazos de prescripción de acciones).

Otro aspecto analizado en el presente trabajo, con mayor detalle, es la causa de licitud de tratamiento de los ficheros de solvencia patrimonial y de crédito. Con anterioridad al RGPD dicha causa era el entendido “Interés legítimo del responsable”, manteniéndose en la regulación actual con idénticos parámetros. Dicha causa no es posible que cambie debido a la especial naturaleza de los ficheros objeto del presente trabajo, habiendo resultado de la ponderación de intereses que prevalece el interés legítimo del responsable del fichero, amparado en la seguridad económica que ofrecen dichos ficheros en el tráfico jurídico, sobre el derecho fundamental del interesado a la intimidad.

Cabe concluir, por tanto, que a pesar de que el RGPD introduce cambios generales que serán de aplicación a los ficheros de solvencia patrimonial y de crédito, tal y como acabamos de ver, será necesario esperar a la promulgación de la nueva Ley Orgánica de Protección de Datos personales a fin de conocer cuáles son los requisitos para la inclusión de los datos personales de los afectados en los mencionados ficheros.

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución 33/2011, de 24 de enero.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Nota informativa. El Tribunal de Justicia de la Unión Europea resuelve la cuestión prejudicial planteada por el Tribunal Supremo relativa a la interpretación del artículo 7 f) de la Directiva 95/46/CE.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Protección de Datos: Guía para el ciudadano.

ÁLVAREZ HERNANDO, JAVIER. *Guía Práctica sobre protección de datos. Cuestiones y formularios*. Lex Nova. Junio de 2011.

ÁLVAREZ HERNANDO, JAVIER. *Practicum Protección de Datos 2015*. Aranzadi. Enero de 2014.

BIURRUN ABAD, FERNANDO J. “Accountability” o responsabilidad activa en el Reglamento General de Protección de Dato.

DE MIGUEL ASENSIO, PEDRO ALBERTO. *Estudios y Comentarios Legislativos (Civitas)*. Derecho Privado de Internet. Aranzadi. Enero 2015.

ESTANCONA PÉREZ, ARAYA ALICIA. *Solvencia patrimonial y tratamiento automatizado de datos personales. Protección desde el derecho privado*. Editorial Aranzadi. 2013.

GARCIA-PERROTE ESCARTÍN, IGNACIO y MERCADER UGUINA, JESÚS R. *El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo al tratamiento de datos personales, un primer acercamiento*. Publicación: Revista de Información Laboral num. 2/2017 parte Artículos doctrinales. Aranzadi. 2017.

GELJO CASTANY, MIGUEL. *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*. Editorial Aranzadi. 2010.

GUASH PORTAS, VICENTE y SOLER FUENSANTA, JOSÉ RAMÓN. *El interés legítimo en la protección de Datos*. Revista de derecho UNED, 2015.

MENDOZA LOSANA, ANA ISABEL. *Guía práctica sobre la inclusión en un registro de morosos*. Revista CESCO de Derecho de Consumo n.º 4/2012.

MORALES BARCELÓ, JUDITH. *Big data y protección de datos, especial referencia al consentimiento del afectado*. Editorial Aranzadi. 2017

ZARZA RODRÍGUEZ, JOSÉ ENRIQUE. *Los ficheros de solvencia negativa: análisis jurídico y valoración sobre su adaptación a la normativa vigente sobre protección de datos*. http://tecnologia.elderecho.com/tecnologia/privacidad/ficheros-solvencia-negativa-proteccion-datos_11_1020055003.html. Noviembre, 2016. Consultado 18/6/2018.