Informe 0195/2017

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por la Asociación Española de Banca, cúmpleme informarle lo siguiente:

I

La consulta plantea una serie de cuestiones relacionadas con la incidencia que sobre los tratamientos llevados a cabo por las entidades asociadas a la consultante tendrá la plena aplicación, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas en lo que respecta al tratamiento de sus datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46CE (Reglamento general de protección de datos).

Como cuestión previa, es preciso indicar que el presente informe no entrará a analizar lo mencionado en el apartado III de la consulta, relacionado con la aplicación de la Directiva (UE) 2015/2366, sobre servicios de pago en el mercado interior, por cuanto el momento oportuno para valorar el alcance que deba tener la comunicación de datos que la misma parece prever será aquél en que por esta Agencia Española de Protección de Datos se emita informe en relación con la disposición que trasponga la citada Directiva al ordenamiento interno, no pudiendo en el presente momento determinar la respuesta que ha de darse a lo planteado al no existir norma de derecho interno reguladora de esta cuestión.

II

Hecha la anterior precisión, y siguiendo el orden de la consulta, se hará en primer lugar referencia a los supuestos de legitimación para el tratamiento que se recogen en el apartado I de la misma.

En este sentido, como pone de manifiesto la consulta, el Reglamento general de protección de datos, en vigor desde el 25 de mayo de 2016, será planamente aplicable, conforme a su artículo 99.2 el día 25 de mayo de 2018.

El artículo 4.11 del Reglamento define claramente el consentimiento del interesado como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*".

A su vez, el considerando 32 del propio texto clarifica el modo en que podrá prestarse el consentimiento con arreglo a sus disposiciones, al recordar lo siguiente:

> *"El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta."*

De todo lo que se ha indicado cabe deducir que el consentimiento obtenido a través del procedimiento al que se refiere el artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1726/2007, de 21 de diciembre, no cumple los requisitos exigidos para el consentimiento por el Reglamento general de protección de datos.

Al propio tiempo, el considerando 171 del citado Reglamento señala que *"cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento*".

De ello se desprenden claramente dos consecuencias: una derivada directamente de la dicción del citado considerando será que los responsables que hubieran recabado el consentimiento del afectado no precisarán recabarlo nuevamente cuando el mismo cumpla con los requisitos del Reglamento y se

derive de una declaración o una clara acción afirmativa del afectado; otra, interpretado lo señalado en dicho considerando *a sensu contrario*, que cuando el consentimiento recabado con anterioridad a la plena aplicación del Reglamento no hubiera consentido en una declaración o una clara acción afirmativa del afectado, ese consentimiento no podrá considerarse por sí solo causa legitimadora del tratamiento, o lo que es lo mismo, que en ese caso el tratamiento respecto del que se recabó el consentimiento no se encontrará inmediatamente amparado por el artículo 6.1 a) del Reglamento general de protección de datos.

De este modo, para que pueda seguir llevándose a cabo el tratamiento respecto del que se recabó un consentimiento que no encaja en lo establecido en el artículo 4.11 del tan citado Reglamento deberá dejar de llevarse a cabo a menos que cuente con una legitimación suficiente a los efectos previstos en el artículo 6.1 del reglamento general de protección de datos.

III

Para que ello pueda tener lugar, y partiendo del hecho de que el tratamiento no encajará, con carácter general, en los supuestos enumerados en las letras b) a e) del citado artículo 6.1, dado que en ese caso no se hubiera recabado el consentimiento por no ser el mismo necesario, será preciso que el tratamiento se ampare o bien en la prestación de un nuevo consentimiento que sí dé cumplimiento a los requisitos establecidos en el Reglamento o bien que sea de aplicación el artículo 6.1 f) del Reglamento, según el cual podrá tener lugar el tratamiento, en el ámbito del sector privado, si el mismo "*es 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* ".

También los considerandos del Reglamento aportan ciertos elementos interpretativos en relación con la aplicación de la regla contenida en el precepto que acaba de transcribirse.

Así, el considerando 47 recuerda que el interés legítimo de un responsable, de un cesionario o de un tercero, *"puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable"*, añadiendo posteriormente que *"en cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular,*

los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior".

Además, el reglamento general de protección de datos enumera algunos supuestos que pueden ser tomados en consideración para determinar la aplicabilidad de dicha regla.

Así, en primer lugar, se señala que el interés legítimo *"podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable"*. Igualmente, en el propio considerando señala que *"el tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate"* y que *"el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo"*.

Por otra parte, el considerando 48 añade que *"los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados"*.

Finalmente, incluso con mayor detalle, el considerando 49 añade un ejemplo más, al señalar que *"constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas"*.

Como puede comprobarse, el propio Reglamento establece los criterios básicos a tomar en consideración para poder detectar intereses legítimos que

permitan valorar la aplicación de la regla de equilibrio establecida en el artículo 6.1 c).

Junto con estos criterios, debe tenerse en cuenta el marco actualmente vigente en que, como es sabido, si bien la Ley Orgánica 15/1999 no incorpora la regla de equilibrio de intereses, actualmente recogida en el artículo 7 f) de la Directiva 95/46/CE y similar a la establecida por el citado artículo 6.1 f) del Reglamento, el tribunal de Justicia de la Unión Europea en su sentencia de 24 de noviembre de 2011 (asunto Asnef, Fecemd) declaró que dicho precepto tenía efecto directo en el derecho español, siendo numerosos los supuestos en que esta Agencia o la doctrina derivada de la Audiencia Nacional e incluso del tribunal de Justicia han apreciado la existencia de un interés legítimo prevalente como base suficiente para la realización de un determinado tratamiento o cesión de datos.

A ello deben añadirse finalmente aquellos supuestos en que la prevalencia del interés legítimo del responsable o de un tercero cesionario viene determinada por una norma con rango de Ley habilitante del tratamiento y, en consecuencia, amparada en el presente momento en los artículos 6.1 u 11.2 a) de la Ley Orgánica 15/1999.

Como consecuencia de todo lo que se ha indicado, cuando el responsable del tratamiento hubiera recabado el consentimiento de los afectados a través del procedimiento señalado en el artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999, dicho responsable deberá, a partir de 25 de mayo de 2018, recabar un nuevo consentimiento del afectado, a menos que pueda considerar el tratamiento amparado en la regla de ponderación establecida en el artículo 6.1 f) del Reglamento general de protección de datos, para lo que será relevante tener en cuenta los criterios contenidos en el propio reglamento, los antecedentes derivados de los supuestos en que la regla ahora contenida en el artículo 7 f) de la Directiva 95/46/CE se ha considerado aplicable a un supuesto concreto y los casos en que existe una norma con rango de Ley que, sin imponer una obligación de tratamiento, ha reconocido precisamente la posibilidad de que el tratamiento pueda llevarse a cabo, al llevar a cabo la ponderación prevista a favor del interés legítimo del responsable o del cesionario.

IV

Hechas las anteriores precisiones corresponde ahora analizar si en los distintos supuestos enumerados en el apartado I de la consulta cabrá considerar aplicable la causa de legitimación contenida en el artículo 6.1 f) o si en estos supuestos debería recabarse un nuevo consentimiento de los afectados que cumpla con los requisitos establecidos en el artículo 4.11 del Reglamento general de protección de datos.

El primer supuesto enumerado en la consulta se refiere al *"tratamiento para fines de mercadotecnia, publicidad y comunicaciones comerciales en línea con el desarrollo del negocio que realice la entidad de sus propios productos y/o servicios"*. A tal efecto, la consulta indica que el citado tratamiento se funda en un interés legítimo de las entidades, que los clientes han venido aceptando durante el mantenimiento de su relación con la entidad, por lo que existe una expectativa razonable de que se sigan recibiendo esas comunicaciones comerciales, teniendo en cuenta en todo caso que el interesado puede en cualquier momento ejercer su derecho de oposición a seguir recibiendo todo tipo de comunicaciones.

En este punto es relevante indicar que, aun cuando en el encabezamiento de este apartado no se hace mención a los canales a través de los cuales pretende remitirse la publicidad o realizar acciones de mercadotecnia, la consulta hace referencia en un lugar posterior a dos circunstancias añadidas a las contenidas en ese encabezamiento: la publicidad podrá realizarse a través de cualquier medio y se llevará a cabo durante y con posterioridad al mantenimiento de la relación con el cliente.

Ello exige, antes de acudir a la aplicabilidad del artículo 6.1 f) del Reglamento general de protección de datos, que se tome en consideración la aplicación al caso, cuando las comunicaciones se llevan a cabo por medios electrónicos, de lo establecido en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, cuyo artículo 21 dispone lo siguiente:

> *"1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.*
>
> *2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.*
>
> *En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.*

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección."

La Ley 34/2002 constituye norma especial en relación con estas actividades, por lo que no podría acudirse para resolver la cuestión planteada en este punto a las previsiones del reglamento general de protección de datos, sino que habrá de tenerse en cuenta lo dispuesto en esta norma especial cuando las comunicaciones se lleven a cabo a través de medios electrónicos.

Ciertamente es consciente esta Agencia de la existencia de una propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) cuyo artículo 16 se referiría a la comunicaciones no solicitadas. No obstante, al margen de que dicho precepto parte igualmente del principio de consentimiento con una excepción similar a la contenida en el reproducido artículo 21.2, es preciso señalar que, aun cuando se pretenda que dicho Reglamento sea de aplicación en la misma fecha de plena aplicabilidad del Reglamento general de protección de datos, se trata en el presente momento simplemente de una propuesta de disposición cuyo contenido final no puede aún ser conocido, por lo que habrá de estarse a la norma actualmente vigente.

De este modo, el citado artículo 21 opera como límite al que habrá de estarse en todo caso cuando las acciones de mercadotecnia o publicidad se lleven a cabo a través de medios electrónicos, al establecerse para estos supuestos la regla general del consentimiento expreso del interesado para su realización a menos que dichas acciones se refieran a *"productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente"*.

Quiere ello decir que resultará irrelevante respecto de estas acciones el nuevo régimen del Reglamento general de protección de datos, que además tampoco afectaría al supuestos de hecho analizado por la consulta, toda vez que, exigido por la Ley 34/2002 el consentimiento expreso de los clientes, con la única excepción mencionada, no habrá sido posible, dentro del régimen actualmente vigente, la realización de este tipo de acciones sobre la base de un consentimiento obtenido conforme al procedimiento previsto en el artículo 14 del reglamento de desarrollo de la Ley Orgánica 15/1999, que además no resulta de aplicación.

Centrándonos en los restantes supuestos de acciones de publicidad o mercadotecnia a las que se refiere la consulta; es decir, las no realizadas a

través de medios electrónicos, el ya reproducido artículo 21 de la Ley 34/2002 ya permite, aun no siendo de aplicación a estas otras acciones, valorar los supuestos en los que el legislador de la Unión Europea puede considerar de aplicación una regla distinta del consentimiento para el tratamiento de estos datos.

En efecto, si las normas reguladoras de la privacidad en las comunicaciones electrónicas, que establecen un régimen especialmente estricto a la hora de obtener el consentimiento del interesado exceptúan de dicho consentimiento el supuesto referido a comunicaciones relativas a *"productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente"*, cabe deducir que esta regla sería aplicable por analogía a los supuestos en que dichos requisitos son menos exigibles; es decir, a las acciones realizadas a través de otros canales de comunicación.

Ahora bien, para que dicha ponderación deba efectuarse en beneficio de la entidad responsable será preciso que se haga una interpretación razonable de lo que debe ser considerado como un producto o servicio similar al previamente contratado por el cliente, de forma que la habilitación que podría ampararse en la regla a la que se está haciendo referencia debería igualmente vincularse con la naturaleza de los productos y servicios previamente contratados, no extendiéndose a aquéllos respecto de los que no pueda aplicarse una identificación lógica basada en la expectativa razonable del cliente.

De este modo, no cabría duda de que sería posible la oferta de otros productos relacionados con el ahorro o el crédito, pero sería necesario establecer ya un primer análisis restrictivo cuando la acción de publicidad se refiriese a servicios que pudieran encajar en el concepto amplio de "servicios financieros", como sucedería en el caso de los seguros. Finalmente, la ponderación a la que estamos haciendo referencia no operaría cuando se tratase de publicidad u oferta de productos o servicios que no guardan relación con la actividad de la entidad, sino que la acción publicitaria deriva de la existencia de un determinado acuerdo con el anunciante al que se refiriese la publicidad o afectase a productos o servicios no financieros pero ofrecidos por empresas del grupo o participadas por la entidad.

Por otra parte, la ponderación que acaba de realizarse sería aplicable a los supuestos en que el interesado mantuviera una relación con la entidad, sin afectar a aquéllos en que el cliente hubiese cesado en esa relación.

En este sentido, la propia consultante considera que son argumentos favorables a realizar la ponderación los derivados del hecho de que los clientes de una entidad vienen aceptando habitualmente esa publicidad, lo que convierte su recepción, a salvo siempre del ejercicio del derecho de oposición,

en una expectativa razonable derivada del propio tratamiento. Ello supone que la recepción de la publicidad de la entidad con la que se mantiene una relación puede resultar generalmente inocua para el cliente, de modo que sólo cuando éste ejerce expresamente su derecho de oposición podría considerarse que se aprecia por su parte una intromisión excesiva en su derecho fundamental a la protección de datos de carácter personal.

Sin embargo, esta conclusión no puede predicarse de aquellos supuestos en que el afectado ha decidido voluntariamente cesar en la relación con la entidad, bien por haber resuelto sobre la base de su propia decisión la relación con aquélla, bien por el hecho de haberse cumplido plenamente dicha relación sin que el afectado haya manifestado su voluntad de contratar nuevos productos o servicios de la entidad. En este caso, sin perjuicio de que pueda apreciarse un interés legítimo de la entidad en llevar a cabo la oferta de esos productos o servicios, no cabría considerar que exista una expectativa razonable en quien ya no es cliente de una entidad o lo ha sido eventualmente de seguir recibiendo las ofertas de productos o servicios de esa entidad a menos que manifieste su negativa a ello.

En consecuencia, respecto del primero de los supuestos citados, y siempre partiendo de que las entidades darían pleno cumplimiento a sus obligaciones de transparencia, conforme a los artículos 13 y 14 del Reglamento general de protección de datos, estableciendo además un procedimiento sencillo para el ejercicio del derecho de oposición, cabría considerar que el tratamiento podría ampararse en el artículo 6.1 f) del citado Reglamento cuando las acciones se llevasen a cabo por medios no electrónicos, el afectado siguiese siendo cliente de la entidad y los productos o servicios ofertados puedan considerarse “similares” a los contratados por el cliente.

V

La consulta se refiere, en segundo lugar al “tratamiento de datos con objeto de realizar un análisis de solvencia del clientes para una posterior financiación”.

La consulta bajo este supuesto se refiere realmente a dos tratamientos claramente diferenciados: aquél que llevaría a cabo la entidad para valorar la solvencia del cliente que solicitase concretamente un determinado producto de financiación para determinar el riesgo que pudiera generar el mismo y decidir sobre la conclusión o no del contrato, de aquél en que la evaluación del riesgo se lleva a cabo sin que el cliente haya solicitado producto de financiación alguno y que además sería empleado por la entidad para ofrecer al cliente ese producto o servicio no solicitado (por ejemplo, la “preconcesión” de un crédito que no ha sido solicitado por el cliente).

Ambos supuestos han de ser analizados de forma separada, dado que la intervención del cliente en el primero de ellos puede implicar que no sea preciso acudir a la previsión del artículo 7.1 f) del reglamento, a diferencia del segundo en que el tratamiento sólo podría basarse en el consentimiento del cliente o en la aplicación de la citada regla de ponderación.

En efecto, en los supuestos en los que la propia entidad financiera recabe los datos necesarios para enjuiciar la solvencia de quien, incluso siendo ya cliente de la misma, solicita la contratación de un producto que lleve aparejada una financiación, el tratamiento puede ampararse claramente en lo dispuesto en el artículo 6.1 b) del Reglamento general de protección de datos, en conexión con la propia normativa sectorial que resulte de aplicación e imponga el deber de recabar la información necesaria para la valoración del riesgo, como sucedería por ejemplo en relación con el accesos a los sistemas de información crediticia, expresamente previsto en la Ley 16/2011, de 24 de junio.

En este supuesto, el tratamiento puede considerarse *"necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales"*, dado que como bien señala la consulta existe un deber legal de verificación de la solvencia del cliente y la evaluación de su riesgo.

Sin embargo, la situación no es la misma en los supuestos en que el interesado no ha solicitado la contratación de ningún producto que implique financiación y es la propia entidad la que analiza su solvencia y riesgo atendiendo a determinados datos personales, con la finalidad, precisamente, de poner a su disposición esos productos o servicios financieros.

En este caso, la situación podría aparentemente no diferir de la mencionada en el apartado anterior de este informe, toda vez que se estaría procediendo al tratamiento de los datos con la finalidad de ofrecer a los clientes de la entidad un producto que podría ser considerado "similar" a los que el propio cliente mantiene contratados con la entidad.

En este sentido, y como punto de partida, ha de tenerse en cuenta que el primer límite para la determinación de la existencia de un interés legítimo prevalente en la entidad de crédito sería el que ya se ha delimitado, atendiendo al hecho de que los afectados sigan manteniendo una relación con la entidad y los productos o servicios sean similares a los contratados.

Sin embargo, frente al supuesto antes analizado, en que la realización de las acciones comerciales tenía, en principio, lugar sobre la información general facilitada por el cliente, de modo que no se producía su segmentación basada en la realización de un perfilado, en el supuesto ahora planteado, se plantea precisamente la realización de ese perfilado como tratamiento previo a

la remisión de las comunicaciones comerciales. Ello implica la necesidad de analizar si dicho tratamiento adicional podría considerarse igualmente fundado en el interés legítimo prevalente de las entidades asociadas a la consultante.

Para ello deberá partirse nuevamente de la expectativa razonable que los clientes pudieran tener de que la contratación de un producto o servicio de dichas entidades implicará un seguimiento posterior de los mismos con el fin de determinar si pueden o no ser potenciales beneficiarios de otras ofertas de productos o servicios de la entidad. Al propio tiempo, será igualmente preciso analizar en qué modo puede considerarse en estos supuestos que se produce una intromisión en los derechos e intereses de los clientes que habría de prevalecer sobre el interés legítimo de las entidades.

La primera consecuencia de lo antedicho es que debería excluirse de la aplicación del artículo 6.1 f) del Reglamento general de protección de datos el supuestos en que la entidad acudiera para la realización del perfilado a fuentes distintas de las que se derivasen de la relación del cliente con la entidad. De este modo, a juicio de esta Agencia, cualquier perfilado de los clientes que se llevase a cabo como consecuencia de enriquecer los datos de que dispone la entidad en virtud de su relación con el cliente con información procedente de otras fuentes requeriría o bien la solicitud del producto o servicio por el interesado, conforme ya se ha indicado, o bien que el mismo preste su consentimiento para el tratamiento. Ello se funda en que la obligación de las entidades de obtener la información disponible sobre la solvencia y el nivel de riesgo de un cliente o potencial cliente puede fundarse en la solicitud por éste del servicio, pero no en la decisión unilateral de la entidad de llevar a cabo ese perfilado.

Si los datos procediesen únicamente de la información de que dispusiera la entidad en relación con los productos o servicios contratados por el cliente, sin que la misma fuera completada con la originada en otras fuentes distintas, ciertamente la conducta de la entidad, consistente en la realización de un perfilado para la remisión de ofertas de productos o servicios a sus clientes, resultaría ser menos invasiva de los derechos e intereses de los clientes, pudiendo en este caso considerarse la aplicabilidad de lo dispuesto en el artículo 6.1 f) del Reglamento general de protección de datos.

Ahora bien, para que pueda llegarse a esta conclusión será imprescindible que las entidades diferencien claramente el tratamiento al que se está haciendo referencia del que ha sido analizado en el apartado anterior de este informe. Ello quiere decir que no podrá considerarse amparado en el artículo 6.1 f) un tratamiento de las características del ahora estudiado si en la información facilitada al interesado únicamente se indica que los datos será tratados con la finalidad de remitir publicidad de otros productos y servicios de la entidad, dado que, con carácter previo a esa remisión, se estaría llevando a

cabo otro tratamiento, consistente en la elaboración de perfiles a partir de la información de que dispusiera la entidad.

Del mismo modo, debería ser posible que el interesado pueda oponerse a este tratamiento aun cuando no se hubiera opuesto a recibir otro tipo de ofertas de la entidad.

Por todo ello, sería posible amparar en el artículo 6.1 f) del Reglamento general de protección de datos el tratamiento por parte de la entidad de la información de que disponga en relación con los productos y servicios contratados por sus clientes para evaluar su solvencia a efectos de ofrecerle nuevos productos que impliquen financiación, siempre que el cliente haya sido informado con la debida separación acerca de este tratamiento y tenga en todo caso la posibilidad de ejercer específicamente su derecho de oposición respecto del mismo.

VI

Se hace referencia en tercer lugar a *"la cesión de datos para la prevención del fraude (entre empresas del mismo grupo y/o ajenas al mismo)"*. En particular, la consulta se refiere a los supuestos en que un tercero accede fraudulentamente a la cuenta de un cliente y transfiere fondos a su propia cuenta, indicando que en estos supuestos la entidad destinataria de la transferencia no puede comunicar a la remitente *"los datos personales del titular que ha realizado el fraude cuando el mismo ha sido denunciado por la entidad"* remitente de la transferencia, invocándose como límite la normativa de protección de datos.

La prevención del fraude como interés legítimo que puede ser tomado en consideración para llevar a cabo la ponderación prevista en el artículo 6.1 f) del reglamento general de protección de datos aparece expresamente mencionada en el considerando 47 del citado reglamento.

Igualmente, en el dictamen 6/2014, de 9 de abril, del grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE también se hace expresa referencia a la prevención del fraude como uno de los supuestos en que puede ser posible la aplicación de la citada regla.

Asimismo, esta Agencia Española de Protección de datos ya ha emitido diversos dictámenes, a partir del primero emitido en fecha 2 de agosto de 2013, en que se considera amparada en el artículo 7 f) de la Directiva la creación de sistemas de prevención del fraude, de carácter sectorial o, eventualmente, multisectorial, en que las entidades pertenecientes a un mismo sector pueden acceder a determinadas operaciones que puedan considerarse sospechosas,

con la finalidad de poder realizar una evaluación más detallada acerca de las mismas.

Finalmente, y aun cuando no guarde relación con la cuestión planteada, en informe de 26 de octubre de 2016, esta Agencia española de Protección de Datos ha considerado amparadas en el artículo 7 f) de la Directiva 95/46/CE las cesiones de datos por parte de una entidad bancaria a un cliente ordenante de un gran número de transferencias dinerarias los datos identificativos de los beneficiarios de aquéllas respecto de las que se haya producido un error en la remisión, de forma que se hubiera producido un ingreso erróneo en una cuenta a la que el ordenante no pretendía transferir los fondos.

Quiere todo ello decir que incluso dentro del ámbito actual de aplicación de las normas de protección de datos, el supuesto concreto planteado en la consulta; es decir, que la entidad recetora de una transferencia respecto de la que la entidad remitente haya constatado la existencia de un fraude por haberse producido como consecuencia de un acceso indebido a la cuenta de uno de sus clientes, podría considerarse amparado en el artículo 7 f) de la Directiva, por cuanto resulta necesario el conocimiento de la identificación del beneficiario de la transferencia fraudulenta para el ejercicio de las acciones que resulten procedentes. Debe igualmente recordarse que el ya citado Dictamen del Grupo de Trabajo del artículo 29 se refiere expresamente al ejercicio de acciones en juicio como uno de los posibles intereses legítimos que pueden fundamentar, debidamente ponderados con los derechos del afectado, el tratamiento de datos de carácter personal.

En cuanto a la posibilidad de crear sistemas comunes en que las entidades de crédito intercambiasen información acerca de quienes hubieran llevado a cabo este tipo de conductas sería preciso conocer las circunstancias en que se produciría el intercambio de la información o la posible creación de un sistema común de información para la prevención de este tipo de fraudes, pudiendo ahora señalar simplemente que sería posible amparar los tratamientos en el artículo 6.1 f) del Reglamento general de protección de datos, aunque será necesario conocer su funcionamiento a fin de determinar las garantías o medidas adicionales de salvaguarda de los derechos de los afectados ante la posibilidad de que el sistema incorpore como fraudulentas operaciones que no tengan ese carácter. En este sentido, puede servir de orientación lo ya señalado por esta Agencia en el citado informe de 2 de agosto de 2013 y los emitidos con posterioridad al mismo.

En consecuencia, la transmisión de los datos de la entidad beneficiaria de una transferencia a la entidad de origen cuando la misma tenga indicios suficientes para apreciar la existencia de un acceso fraudulento a la cuenta del ordenante con la finalidad de realizar esa transferencia estará amparada en el artículo 6.1 f) del reglamento general de Protección de datos. En cuanto a la creación de sistemas comunes de prevención del fraude habrá de estarse a las

garantías que se determinen al establecerlos, no pudiendo darse una respuesta terminante a la cuestión, aunque indicando que sí será posible que esas garantías permitan la aplicación del citado artículo 6.1 f)

VII

En cuarto lugar, la consulta se refiere al *"análisis de los movimientos transaccionales y/o capacidad de ahorro del cliente, para realizar observaciones y ofrecer recomendaciones sobre productos y(o servicios de la entidad bancaria en beneficio de una mejor gestión de las finanzas de los clientes"*, de modo que la información referida a dichos movimientos permitiría a la entidad de crédito facilitar al cliente sobre los productos o servicios que más se ajustasen a su perfil con la finalidad de maximizar el rendimiento que pudiera obtener éste último u ofrecerle los mejores precios en productos o servicios que tuviera contratados o pudiera contratar en el futuro.

Si bien la consulta se refiere en este apartado al uso de la información para la creación de nuevos productos o servicios, dicha afirmación parece más vinculada al tratamiento mencionado en quinto lugar, por lo que se analizará cuando se haga referencia a éste.

Perfilados así los términos del supuesto ahora objeto de análisis, ciertamente guarda similitudes con los mencionados en primer y segundo lugar, dado que se trata en definitiva de utilizar la información disponible con la finalidad de que la entidad ofrezca al cliente productos y servicios de la misma que puedan ser de su interés. No obstante, supone un tercer nivel de utilización de los datos respecto de los dos supuestos mencionados.

En efecto, mientras en el primero de los supuestos los datos utilizados para la remisión de ofertas comerciales eran básicamente los identificativos de los clientes, sin llevar a cabo perfiles detallados de los mismos, y en el segundo supuesto se sumaban a aquéllos los relacionados con la solvencia o el riesgo de crédito de un determinado cliente, produciéndose ya un perfilado del mismo, en el supuesto ahora planteado se prevé el tratamiento de la totalidad de las transacciones del cliente a fin de poder realizar un perfilado más detallado que permita concretar con mayor precisión los productos o servicios que deben ofrecerse a aquél.

No obstante, como punto de partida deberá partirse de las premisas que se han indicado en los apartados IV y V del presente informe, dado que en las mismas se delimitaban los supuestos en que podría llegar a aplicarse la regla del artículo 6.1 f) del reglamento general de protección de datos.

Así, en el supuesto que va ahora a valorarse deberá partirse de que los datos son obtenidos únicamente a partir de la información de que la entidad

dispone como consecuencia de la gestión de los servicios o productos contratados y que los que a su vez será ofertados al interesado puedan considerarse procedentes de la entidad y guarden cierta similitud con los que hubieran sido ya objeto de contratación.

Dicho lo anterior, ya se ha avanzado que la intromisión derivada del perfilado al que se refiere este supuesto resulta mayor que la prevista en los dos casos anteriores, por cuanto se procederá el análisis masivo de toda la información que pueda resultar del uso por el interesado de los productos o servicios contratados.

Por este motivo, las garantías adicionales que se mencionaron en el apartado V de este informe deberán adoptarse en este caso incluso con una mayor precisión. Así deberá detallarse de forma más minuciosa el tratamiento que va a llevarse a cabo, y particularmente, el hecho de que los datos transaccionales van a ser empleados para la elaboración de perfiles y deberá igualmente ofrecerse al interesado la posibilidad de oponerse específicamente a este tratamiento adicional.

En todo caso, no cabría entender amparado en el artículo 6.1 c) citado el uso de estos datos y de los perfiles resultantes para la oferta de productos o servicios de terceras entidades y, evidentemente con mayor motivo, su posible cesión a entidades que presten servicios que no puedan considerarse "similares", incluso aun cuando se tratase de empresas del mismo grupo.

Finalmente, dado que la consulta no especifica el alcance temporal del tratamiento, es preciso señalar que habida cuenta del carácter intrusivo del mismo y de que en definitiva implicará la adopción de decisiones automáticas en lo que respecta a la oferta de unos determinados productos o servicios que se considerarán adecuados al perfile obtenidos, sería preciso que se delimitase claramente el período al que se referirán los movimientos analizados, que no debería exceder del que fuese suficiente para conocer la situación actual de la persona respecto de la que se elabora el perfil, pudiéndose plantear, por ejemplo, un plazo temporal no superior al año.

VIII

En quinto lugar, la consulta se refiere a *"la "anonimización" de datos transaccionales, obtenidos a través de los productos y/o servicios de la entidad bancaria, para desarrollar nuevos productos y/o servicios basados en datos anonimizados y agregados".* Se trata según se indica de analizar patrones de uso de los servicios para el desarrollo de notros nuevos, lo que parece guardar relación con la mención que el apartado anterior hacía ese desarrollo.

Como punto de partida, sería preciso que se clarificasen los términos de la consulta en este punto, toda vez que si bien se hace referencia a la agregación y al uso de datos anonimizados, también pudiera derivarse de la misma la generación de patrones a partir de estudios de carácter longitudinal sobre el uso de los servicios, lo que implicaría la imposibilidad material de llevar a cabo una anonimización de los datos en los términos previstos en el Reglamento general de protección de datos.

En este sentido, debe recordarse que el considerando 26 del Reglamento general de protección de datos indica lo siguiente:

> *"Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."*

Por su parte, añade el considerando 29 que "*Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas*".

En definitiva, de lo establecido en el Reglamento General de protección de datos se desprende que, en cuanto el mismo resulte de aplicación y al menos desde que éste entre en vigor, tanto la anonimización como la seudonimización de los datos personales llevarán aparejada la existencia de

dos tratamientos sucesivos: el que supone la propia anonimización o seudonimización a partir de los datos personales de que dispone el responsable y el que se lleve a cabo posteriormente con los datos ya anonimizados o seudonimizados. La diferencia entre ambos supuestos estribará en el hecho de que mientras la normativa de protección de datos no será de aplicación a este segundo tratamiento si los datos han sido anonimizados, sí resultará aplicable en caso de que se haya producido únicamente una seudonimización.

Y esta diferencia también incidirá en la ponderación exigida por el artículo 6.1 f) respecto del primer tratamiento llevado a cabo, dado que en caso de que la anonimización sea completa, siendo imposible la vinculación de la información de forma directa o indirecta con un determinado afectado, la afección del tratamiento a la esfera de derechos e intereses de aquél será sustancialmente menor que en el supuesto en que los datos sigan pudiendo identificarle al revertirse el procedimiento de seudonimización.

Incluso esta incidencia será aún menor en caso de que la anonimización implique desde su origen una agregación de los datos de carácter personal de un determinado universo de afectados, dado que a partir de ese momento, si los mecanismos de agregación son los adecuados, sería imposible disgregar del dato agregado la información referida a un sujeto concreto.

Quiere ello decir que en el supuesto planteado si el resultado del tratamiento fuera efectivamente la obtención de datos anónimos o, incluso en mayor medida, si los datos resultantes son agregados, de forma que no quepa en los términos mencionados en el considerando 26 del Reglamento volver a asociar la información con un afectado concreto, la incidencia mínima que pudiera existir en el derecho de los afectados como consecuencia de la aplicación sobre sus datos de un procedimiento de anonimización o agregación podría ceder ante el interés legítimo que pudiera justificar el que ese tratamiento se lleve a cabo, que en los términos de la consulta sería el desarrollo por la entidad de nuevos productos o servicios. Por ello, en estos casos no cabe duda de que sería posible la aplicación al proceso de anonimización y agregación de la legitimación fundada en el artículo 6.1 f) del reglamento general de protección de datos.

En el supuesto en que se lleve realmente a cabo un procedimiento de seudonimización y no de anonimización la ponderación dependerá de las garantías que se establezcan para garantizar la irreversibilidad del proceso, de forma que, siguiendo con lo establecido en el propio Reglamento, cuanto mayores y más fiables sean dichas garantías mayor será el peso en la ponderación del interés legítimo del responsable sobre los derechos e intereses de los afectados.

De este modo, a diferencia de los procesos de anonimización no es posible en los de seudoinimización dar una respuesta terminante a la cuestión planteada, por cuanto la aplicabilidad del artículo 6.1 f) del Reglamento depnderá de las garantías que se adopten para preservar la irreversibilidad del procedimiento de seudonimización.

En todo caso, como se ha indicado para los supuestos anteriormente indicados, será preciso informar a los interesados acerca de los tratamientos que van a tener lugar y garantizar el adecuado ejercicio por aquéllos de su derecho de oposición, al operar éste, según el artículo 21 del reglamento, en los supuestos en que el tratamiento se funde en la regla del equilibrio de derechos e intereses prevista en el artículo 6.1 f) del reglamento.

IX

Por último, el apartado I se refiere al supuesto de *"actualización de datos personales previamente facilitados por el interesado con base en otras fuentes, incluidas fuentes propias pero cuya obtención se ha basado en otro tipo de relación con el interesado"*.

Como punto de partida debe tenerse en cuenta que el artículo 5.1 d) del reglamento general de protección de datos consagra el denominado principio de exactitud, estableciendo que los datos sometidos a tratamiento deberán ser *"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"*. Quiere ello decir que el responsable, en este caso las entidades asociadas a la consultante deberán adoptar todas las medidas necesarias para garantizar la exactitud de los datos.

Por otra parte, no debe olvidarse que el Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone en el párrafo primero de su artículo 8.5 que *"si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste"*.

Partiendo de dichas premisas, no cabe duda de que cabe apreciar la existencia de un interés legítimo de las entidades en mantener sus datos exactos y actualizados. No obstante, para poder determinar si dicho interés legítimo ha de prevalecer sobre los derechos e intereses de los afectados a los que los datos se refieren deberían tomarse en consideración dos criterios esenciales para determinar el grado de intrusión que el tratamiento al que se está haciendo referencia puede presentar en la esfera íntima de los clientes: los datos respecto de los que se pretenda la actualización y las fuentes a las que se pretenda acudir.

En relación con el primero de los criterios mencionados, la intromisión en los derechos de los interesados será menor en los supuestos en que los datos que se mantengan actualizados sean los necesarios para el adecuado mantenimiento de la relación con los clientes o que el cliente estuviera obligado a facilitar para tal fin, mientras que el acceso a datos adicionales que pudieran permitir un mejor conocimiento del cliente o establecer un perfil más ajustado del mismo implicarían una mayor intromisión.

En cuanto a las fuentes de obtención de los datos debería comprobarse la naturaleza de dichas fuentes o si la obtención de los datos puede llevarse a cabo directamente por las entidades o exige la actuación de un tercero. Del mismo modo, el nivel de intromisión diferirá si las informaciones sometidas a tratamiento han sido facilitadas a esas fuentes por el usuario o provienen de terceros y el grado de accesibilidad de dichas fuentes.

A título de ejemplo, el dictamen 6/2014 del Grupo de Trabajo del artículo 29 se refiere al supuesto de contratación por un responsable de un tercero "agente de cobro" que lleva a cabo una intrusiva investigación "de estilo coercitivo" utilizando prácticas tales como la videovigilancia encubierta y las escuchas telefónicas. En este supuesto, que podría considerarse extremo, es evidente que, como señala el dictamen, la intromisión es de tal naturaleza que hace inviable la aplicación de la regla de equilibrio de intereses.

En el mismo sentido, es sabido que por esta Agencia Española de Protección de Datos han sido sancionadas actuaciones de entidades de esta naturaleza que llevan a cabo una política igualmente agresiva, aun cuando sea "de estilo menos coercitivo", consistentes en recabar información de personas del entorno o divulgar públicamente información referida a un determinado cliente, como su condición de moroso.

Como ejemplo también de conducta respecto de la que cabría apreciar la existencia de una injerencia mínima, puede hacerse referencia a lo señalado en el artículo 13 del Anteproyecto de Ley Orgánica de Protección de Datos, cuya tramitación acordó iniciar el Consejo de Ministros el 23 de junio de 2017, cuyo párrafo primero dispone que *"será lícito el tratamiento de los datos que el propio afectado hubiese hecho manifiestamente públicos siempre y cuando respete los principios establecidos en el artículo 5 del Reglamento (UE) 2016/679, se haya informado al afectado en los términos previstos en el artículo 14 del citado reglamento y se le garantice el ejercicio de sus derechos, en particular los previstos en sus artículos 17 y 19"*.

De este modo, se establece un principio general según el cual puede considerarse mínima la intromisión en la esfera privada de un interesado cuando el responsable procede al tratamiento de aquellos datos que él mimo ha hecho manifiestamente públicos, como podría ser los que incorporase a perfiles abiertos de redes sociales, a los que se refiere la consultante. En este

supuesto, el citado precepto del Anteproyecto establece una regla que consideraría amparado el tratamiento en el artículo 6.1 f) del Reglamento general de protección de datos, siempre que la divulgación se haya llevado a cabo directamente por el interesado y esa divulgación sea tan amplia que los datos puedan considerarse hechos "manifiestamente públicos".

Entre los dos ejemplos mencionados podrán existir otros en que habrá de estarse a las circunstancias de cada supuesto. Así, por ejemplo, podría ser de aplicación el artículo 6.1 f) si el acceso a la fuente se encuentra amparado en una habilitación legal, como sucedería en los supuestos de sistemas de información crediticia o el acceso a determinados registros públicos, mientras que en otros supuestos, como por ejemplo los referentes a información divulgada por terceros distintos del afectado en fuentes de acceso más restringido la afectación al derecho fundamental sería mayor, no pudiéndose sin más amparar la recogida en el artículo 6.1 f) del reglamento general de protección de datos.

A la vista de todo ello, cabría concluir que en los supuesto planteados en este caso habrá de estarse a la naturaleza de los datos y la fuente de la información, no siendo posible dar una respuesta genérica a la consulta, aunque sí podrán tenerse en consideración indicios como los que se han venido indicando en el presente apartado de este informe.

X

La consulta dedica su apartado II al derecho a la portabilidad de los datos, regulado por el artículo 20 del Reglamento general de protección de datos. En particular, la consulta toma en consideración las directrices establecidas en el documento del Grupo de Trabajo del artículo 29 (nº 242), adoptado el 13 de diciembre de 2016, indicando que el mismo no especifica *"los datos exactos que están sujetos a este deber de portabilidad"*, por lo que sería preciso llevar a cabo una delimitación de los mismos, atendiendo a circunstancias tales como su ámbito temporal *"que, en principio, parece referirse a datos actuales del cliente"*, considerando que debe existir una proporcionalidad entre el ejercicio del derecho a la portabilidad y las obligaciones de las entidades de crédito, fundamentalmente teniendo en consideración la diferencia existente entre los derechos de portabilidad y acceso.

En resumen, la consulta plantea, al margen de las consideraciones relacionadas con la normativa de trasposición de la Directiva UE 2015/2366, respecto de las que ya se ha señalado que deberán ser objeto de análisis cuando se valore la conformidad con la Ley Orgánica 15/1999 y el reglamento general de protección de datos de su norma de trasposición al derecho español, que el derecho a la portabilidad sólo podrá ser ejercitado por los

titulares de los productos financieros, y no por los sujetos autorizados en dichos productos, que no exceda de los límites materiales del derecho de acceso y que se refiera a los datos objeto de tratamiento dentro de un límite temporal concreto, que se fija en la consulta en doce meses.

Como cuestión previa, es preciso clarificar que el reglamento configura la portabilidad de los datos como un derecho de los afectados a los que dichos datos se refieren. Ciertamente ello lleva aparejada una obligación para los responsables de los tratamientos de atender el citado derecho, pero dicho deber no es más que la consecuencia del reconocimiento del derecho, por lo que no cabría apreciar en este caso la necesidad de establecer una ponderación, en sentido estricto, entre el derecho a la portabilidad y el deber de atenderla, al ser éste consecuencia de aquél y por tanto tener la extensión y el reconocimiento que se establezca para ese derecho.

En este sentido, 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 *"reforzar 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.

Al propio tiempo, dentro de sus márgenes, el citado considerando 48, haciéndose eco de lo señalado por el artículo 20.4 recuerda que este derecho *"se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento"*.

Finalmente, se recuerda la necesaria compatibilidad de este derecho con los establecidos en el propio texto legal, de modo que, por una parte *"no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento"*, y de otra se recuerda que *"en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato"*.

En este sentido, el derecho a la portabilidad puede considerarse en cierto modo complementario del derecho de acceso reconocido al interesado

por el artículo 15 del Reglamento general de protección de datos, que actuaría como límite máximo al que podría referirse el derecho a la portabilidad. En efecto, el derecho de acceso afecta a la totalidad de datos que estén siendo objeto de tratamiento, sea cual sea además la causa de legitimación que justifique ese tratamiento, a diferencia del derecho a la portabilidad, que se refiere solamente a los tratamientos sometidos, de forma directa o indirecta, a la voluntad o autorización del afectado (basados en el consentimiento o en una relación contractual) y puede verse limitado en cuanto a la extensión de los datos respecto de los que pueda ejercitarse. De este modo, no cabe duda que el derecho a la portabilidad tendrá unos límites más reducidos que el derecho de acceso, cuando menos en lo referente a las causas de legitimación para el tratamiento y en el hecho de que el derecho de acceso podrá referirse a todos los datos objeto de tratamiento salvo cuando resulte de aplicación alguna de las excepciones previstas en el Reglamento o en las normas adoptadas en desarrollo de su artículo 23.

Por otra parte, dado que el derecho a la portabilidad trae su causa de la necesidad de reforzar el control del afectado sobre sus propios datos cuando el tratamiento depende de su voluntad es obvio que dicho derecho sólo podrá ser ejercitado por el afectado que ha prestado su consentimiento al tratamiento o ha suscrito el contrato en cuyo desarrollo se ha producido el tratamiento de los datos y no por terceros que pudieran conocer de la existencia de ese contrato o incluso de los datos que hayan sido tratados. Quiere ello decir que esta Agencia coincide con el criterio de la consultante en que el derecho únicamente podría ser ejercitado por el titular del producto o servicio contratado, que en definitiva ha autorizado el tratamiento, pero no por terceros relacionados con dicho servicio, tales como quienes aparecieran como sujetos autorizados en dichos productos. Lógicamente, y siguiendo lo dispuesto en el Reglamento de desarrollo de la Ley Orgánica 15/1999, el derecho a la portabilidad podría ser ejercitado directamente por el afectado o a través de representante legal o voluntario, dado que esta circunstancia no puede verse afectada por el régimen contenido en el Reglamento general.

Dicho lo anterior, la cuestión a resolver consiste en determinar a qué tipo de datos debería extenderse el derecho a la portabilidad y si podría establecerse algún límite temporal en relación con la antigüedad de tales datos.

Como primera cuestión, debe rechazarse la idea de que el derecho haya de referirse a “datos actuales” si por tales ha de considerarse los relacionados con el momento presente, sin tener en cuenta los que hayan sido facilitados por el interesado u obtenidos por el uso del producto o servicio contratado con anterioridad y que en el momento de ejercicio del derecho estén siendo objeto de tratamiento. Limitar el derecho a “datos actuales”, excluyendo completamente los datos históricos que sigan siendo tratados por el responsable ante el que se ejercita el derecho desnaturalizaría completamente la esencia del derecho a la portabilidad y el control sobre la información

facilitada por el afectado u obtenida directamente del mismo, que como se ha indicado constituye el objeto último del reconocimiento de este derecho.

Por otra parte, debería analizarse las categorías de datos a los que podría referirse este derecho. A tal efecto, resultan sumamente clarificadoras las directrices adoptadas por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE que, a diferencia de lo que parece señalar la consulta, sí se refieren en su apartado III a los datos respecto de los que cabría considerar aplicable el derecho.

Así, el documento señala que el concepto de "datos facilitados por el afectado" debería ser interpretado en un sentido amplio, acorde con la finalidad perseguida por el reconocimiento de este derecho. De este modo, cabría considerar como "facilitados" los datos efectivamente suministrados por el interesado y aquéllos que resultasen del propio "uso" o "desarrollo" del servicio contratado, haciéndose referencia, por ejemplo, a los historiales de búsquedas, datos de tráfico, datos de localización, etc.

Al propio tiempo, el documento excluye del alcance de los datos que puedan ser objeto de portabilidad aquéllos que puedan ser considerados "inferidos" y "derivados", entendidos como los que resulten de la aplicación a la información generada en el desarrollo del servicio de conocimientos o técnicas propias del responsable; es decir, procedentes de la aplicación sobre los datos relacionados con el producto o servicio de técnicas que forman parte del *know how* del responsable; en particular el refiere en este punto a los resultados de la aplicación de técnicas matemáticas sobre esos datos o que resulte de la aplicación de algoritmos sobre aquéllos.

La extrapolación de dichas conclusiones al supuesto de tratamientos llevados a cabo en el ámbito de los productos o servicios contratados con las entidades asociadas a la consultante supone que l derecho a la portabilidad debería comprender, evidentemente, los datos facilitados directamente por el interesado (tales como sus datos identificativos o los relacionados, por ejemplo, con sus domiciliaciones bancarias o sus aportaciones a instrumentos de ahorro o inversión), pero igualmente los que se deriven directamente del desarrollo del servicio (como los movimientos de una cuenta o el historial de pagos en productos de activo). Del mismo modo, quedarían excluidos del derecho aquellos otros datos que se derivase de la aplicación sobre tales datos de las técnicas propias de la entidad, como por ejemplo, los derivados de la calificación del clientes a los que se ha hecho referencia en lugares anteriores de este informe o la realización de perfilados de los clientes sobre la base de la información obtenida de la gestión de los productos o servicios contratados,

La siguiente cuestión a valorar se refiere el límite temporal respecto del que el interesado podría ejercer su derecho. A tal efecto ni el artículo 20 del Reglamento general de protección de datos ni su considerando 68 ni las

directrices del Grupo de Trabajo del artículo 29 establecen ningún criterio especial, dado que parecen partir del hecho de que los datos respecto de los que procederá atender el derecho serán aquéllos que estén siendo objeto de tratamiento por el responsable en el momento en que se ejercite el derecho.

Ciertamente este límite implicaría que la entidad debería facilitar todos los datos que tuviesen una antigüedad igual o inferior a diez años, al ser éste el límite temporal impuesto a las entidades en su condición de sujetos obligados por el artículo 25 de la Ley 10/2010, de 28 de abril, de Prevención del blanqueo de capitales y la financiación del terrorismo. Sin embargo debe tenerse en cuenta que este plazo de conservación guarda relación no tanto con el propio desarrollo de la relación contractual con el cliente, sino con el cumplimiento de la obligación legal impuesta a las entidades; es decir, en la mayor parte de estos supuestos, la conservación de los datos, transcurrido un determinado período de tiempo sólo se lleva a cabo para responder ante las autoridades competentes para la prevención del blanqueo de capitales y la financiación del terrorismo y no para garantizar el adecuado mantenimiento de la relación contractual con el cliente.

Ello conduce a analizar si el plazo de doce meses planteado resultaría congruente con lo previsto en el artículo 20 del reglamento, que como se ha indicado no prevé plazo alguno respecto del que quepa ejercer el derecho y la respuesta a esta cuestión no puede ser la de considerar que este plazo haya de ser tomado como regla para determinar el alcance de este derecho.

En primer lugar, existen determinados productos y servicios, fundamentalmente de activo, en los que las entidades conservan la información relacionada con el producto o servicio contratado durante todo el plazo de vigencia del contrato referido al producto o servicio. Esta conservación no se lleva a cabo en cumplimiento de una obligación legal, sino para el propio desarrollo del contrato. Así sucedería por ejemplo con el historial de pago de los distintos plazos de un crédito hipotecario o de un crédito al consumo. En estos casos, parece razonable que el derecho pueda abarcar tales datos aunque su antigüedad sea superior al año.

En segundo lugar, respecto de productos de pasivo, los propios servicios de banca electrónica de las entidades adheridas a la consultante permiten a los interesados acceder a datos con una antigüedad superior a los doce meses e incluso poder exportar tales datos a hojas de cálculo u otras herramientas. El límite temporal de estos servicios suele encontrarse en el entorno de los dos años anteriores al momento en que se solicita la información. Teniendo en cuenta esta práctica comúnmente aceptada por el sector no parece razonable considerar que no sea posible que respecto de datos que tengan al menos esta antigüedad no sea posible el ejercicio del derecho a la portabilidad y su conversión a un formato interoperables, dado que esta condición se ofrece a los propios afectados que no ejercitan especialmente este derecho.

En todo caso, las conclusiones que se han alcanzado a lo largo de este apartado deben considerarse sin perjuicio de las transmisiones de datos que deban llevarse a cabo conforme a la legislación reguladora de las Instituciones de inversión colectiva y los planes y fondos de pensiones, así como cualquier otra normativa sectorial de aplicación cuando se resuelva por el propio afectado el traspaso del correspondiente producto o servicio.

XI

Finalmente, la consulta plantea una serie de cuestiones relacionadas con la posible complejidad derivada de la aplicación conjunta de las obligaciones impuestas por la normativa de protección de datos de carácter personal y la que establece sus deberes como sujetos obligados por la legislación de prevención del blanqueo de capitales y la financiación del terrorismo.

A tal efecto, la consulta se refiere a la conveniencia de que se adopten medidas legislativas que eximan de la obligación de recabar el consentimiento de los clientes pare el tratamiento y cesión de los datos que resulte necesario a fin de dar adecuado cumplimiento a los deberes de diligencia debida establecidas en dicha legislación, considerando que no operan respecto de estas obligaciones las habilitaciones legales que la Ley sí establece para el supuesto de operaciones sometidas a examen especial o notificación por indicio al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

Como consideración previa, debe señalarse que una interpretación literal de los términos en que se pronuncia la consulta, en que simplemente se realizan propuestas de reforma legislativa en que, como se indica debería constar el dictamen favorable de esta Agencia eximiría de dar respuesta a las mismas en tanto no se desarrolle la correspondiente iniciativa. Ello no obstante, dado que la cuestión planteada ha sido analizada con anterioridad por esta Agencia, se considera oportuno efectuar ciertas consideraciones relacionadas con la misma, a fin de clarificar si los tratamientos o cesiones mencionadas serían admisibles desde el punto de vista de la normativa de protección de datos de carácter personal.

Como es sabido, la Ley 10/2010 y su Reglamento de desarrollo, aprobado por Real Decreto 304/2014, de 5 de mayo, imponen a los sujetos obligados determinadas medidas de diligencia debida. La enumeración más clara de tales medidas aparece recogida en el artículo 13.1 de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el

Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, cuando establece que:

> *"Las medidas de diligencia debida con respecto al cliente comprenderán las actuaciones siguientes:*
>
> *a) la identificación del cliente y la comprobación de su identidad sobre la base de documentos, datos o informaciones obtenidas de fuentes fiables e independientes;*
>
> *b) la identificación del titular real y la adopción de medidas razonables para comprobar su identidad, de modo que la entidad obligada tenga la seguridad de que sabe quién es el titular real; asimismo, en lo que respecta a las personas jurídicas, fideicomisos, sociedades, fundaciones y estructuras jurídicas similares, la adopción de medidas razonables a fin de comprender la estructura de propiedad y control del cliente;*
>
> *c) la evaluación y, en su caso, la obtención de información sobre el propósito y la índole prevista de la relación de negocios;*
>
> *d) la aplicación de medidas de seguimiento continuo de la relación de negocios, en particular mediante el escrutinio de las transacciones efectuadas a lo largo de dicha relación, a fin de garantizar que se ajusten al conocimiento que la entidad obligada tenga del cliente y de su perfil empresarial y de riesgo, incluido, cuando sea necesario, el origen de los fondos, y la adopción de medidas para garantizar que los documentos, datos o informaciones de que se disponga estén actualizados.*
>
> *Cuando las entidades obligadas adopten las medidas mencionadas en las letras a) y b) del párrafo primero, también verificarán que cualquier persona que diga actuar en nombre del cliente esté autorizada a tal fin e identificarán y comprobarán la identidad de dicha persona."*

Las medidas se detallan en el Capítulo II de la Ley 10/2010 y en el Capítulo II de su Reglamento de desarrollo, consistiendo las mismas en la obligación de recabar información de los propios clientes o de terceras fuentes en que dicha información pudiera encontrarse disponible. Dichas obligaciones vienen impuestas de forma claramente imperativa en el texto legal, previéndose específicamente en determinados supuestos la obligación de consultar fuentes disponibles, como sucede en el caso de las personas con relevancia pública (artículo 15). Del mismo modo, el artículo 8 de la Ley se refiere a la aplicación por terceros de estas obligaciones.

De este modo, la legislación de prevención de blanqueo de capitales impone a los sujetos obligados, de forma clara, precisa e incondicional, una

serie de obligaciones legales de obtención de información, bien directamente de los clientes, bien de terceros cuando así lo prevé. Ello implicaría que el tratamiento de los datos, así como la cesión de los mismos cuando se refiera a la obtención de la información de dichas fuentes, e incluso la obtención de los datos de otras entidades pertenecientes al mismo Grupo, se encontraría amparada, siempre que resulte proporcional al cumplimiento de las obligaciones legales impuestas, por el artículo 6.1 c) del Reglamento general de protección de datos, que habilita el tratamiento de los mismos cuando sea necesario para el cumplimiento de una obligación legal impuesta al responsable del tratamiento.

Esta cuestión ya fue analizada por esta Agencia Española de Protección de Datos en un supuesto particular que afectaba a la asociación consultante, dado que se refería a la celebración por la misma de un Convenio con el Consejo General del Notariado para habilitar a los sujetos obligados asociados a la misma el acceso a la Base de Datos de Titularidad real del citado Consejo. Así, en informe de 15 de enero de 2015 consideraba que el citado acceso, y la consiguiente cesión de datos por el Consejo general del Notariado se encontraba habilitado por el artículo 11.2 a) de la Ley Orgánica 15/1999, como consecuencia de la obligación legal impuesta a los sujetos obligados de dar cumplimiento a las obligaciones de diligencia debida establecidas en la Ley 10/2010, entre las que se encuentra la de identificación del titular real. Conforme a su artículo 4.

El mencionado informe señalaba en particular lo siguiente:

"(…) el apartado a) del artículo 11.2 de la Ley Orgánica 15/1999 dispone que no será preciso el consentimiento del interesado, al que acaba de hacerse referencia, cuando la cesión se encuentre amparada por una norma con rango de Ley.

En cuanto al alcance de esta causa de legitimación para el tratamiento debe traerse a colación lo establecido por el artículo 10.2 a) del Reglamento de desarrollo de la Ley Orgánica, cuya conformidad a derecho fue expresamente declarada por la sentencia del Tribunal Supremo de 8 de febrero de 2012, que clarifica que la cesión será posible cuando lo autorice una norma con rango de Ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

- El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

- El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

De este modo, la habilitación establecida por el artículo 11.2 a) de la Ley Orgánica 15/1999 debe considerarse producida no sólo cuando una norma con rango de Ley se refiera expresamente a una determinada cesión de datos (como sucedería, por ejemplo, en lo referente a la comunicación de los datos a los órganos competentes en materia de prevención del blanqueo de capitales y de la financiación del terrorismo a los que se refiere la propia Ley 10/2010 y cuyas transmisiones se prevén expresamente en la norma de creación del fichero al que se está haciendo referencia), sino también en los supuestos en los que la norma con rango de Ley establezca una obligación legal que implique necesariamente el acceso a los datos o cuando dicho acceso deba producirse para garantizar un derecho o interés legítimo del responsable que accede a dichos datos (si bien en este caso con el requisito adicional de que no prevalezcan sobre aquel derecho o interés los derechos del interesado).

Dicho lo anterior, el artículo 4.1 de la Ley 10/2010 establece que "los sujetos obligados identificarán al titular real y adoptarán medidas adecuadas a fin de comprobar su identidad con carácter previo al establecimiento de relaciones de negocio o a la ejecución de cualesquiera operaciones", imponiendo asimismo el artículo 4.4 de la Ley a los sujetos obligados la obligación de adoptar "medidas adecuadas al efecto de determinar la estructura de propiedad o de control de las personas jurídicas".

Por otra parte, el artículo 9.1 del Reglamento de desarrollo de la Ley 10/2010, tras establecer en su párrafo primero el deber de identificación del titular real y señalar en su párrafo segundo que dicha identificación y comprobación de la identidad podrá realizarse, con carácter general, mediante una declaración responsable del cliente o de la persona que tenga atribuida la representación de la persona jurídica, concluye en su párrafo tercero que "no obstante lo dispuesto en el párrafo anterior, será preceptiva la obtención por el sujeto obligado de documentación adicional o de información de fuentes fiables independientes cuando el cliente, el titular real, la relación de negocios o la operación presenten riesgos superiores al promedio". Además, el artículo 9.2 establece una serie de supuestos en los que procederá en todo caso la acreditación de la titularidad real mediante la obtención de información documental o de fuentes fiables independientes.

Para la obtención de dicha información, y como ya se ha indicado con anterioridad, el artículo 8 de la Ley, al que ya hizo referencia esta Agencia en su informe de 23 de febrero de 2012 como fundamento legal de la cesión que ahora viene analizándose, establece que "los sujetos obligados podrán recurrir a terceros sometidos a la presente Ley para la aplicación de las medidas de diligencia debida previstas en esta Sección, con excepción del seguimiento continuo de la relación de negocios".

Al propio tiempo, el artículo 9.6 del Reglamento de desarrollo de dicha Ley prescribe expresamente que "para el cumplimiento de la obligación de identificación y comprobación de la identidad del titular real establecida en este artículo, los sujetos obligados podrán acceder a la base de datos de titularidad real del Consejo General del Notariado previa celebración del correspondiente acuerdo de formalización, en los términos previstos en el artículo 8 de la Ley 10/2010, de 28 de abril".

Este precepto, como puede comprobarse, únicamente sujeta la viabilidad de la cesión de datos a la celebración del Acuerdo cuyo borrador es sometido al parecer de la Agencia por cuanto, dada la naturaleza de la información facilitada, las medidas de seguridad exigibles al tratamiento de la misma y la exigencia de que los datos únicamente sean tratados por quienes en el seno del sujeto obligado tienen encomendada la función de velar por el cumplimiento de la legislación de prevención del blanqueo de capitales, será preciso el establecimiento de especiales garantías y salvaguardas en materia de seguridad y acceso a la información. Estas medidas se contienen en las cláusulas tercera, quinta y sexta del borrado objeto de informe.

Quiere todo ello decir que la Ley 10/2010 establece de forma indubitada una obligación de identificación del titular real, debiendo los sujetos obligados adoptar las medidas que resulte procedentes para el cumplimiento de tal fin, incluyendo, según el artículo 8 de la Ley y el artículo 9 del Reglamento, la obtención de información obrante en los ficheros de terceros, que además será obligatoria cuando la operación revista, por cualquiera de los motivos que se exponen en el segundo de los preceptos un riesgo superior al promedio.

De este modo, existe una obligación legalmente impuesta a los sujetos obligados a la que únicamente será posible dar cumplimiento mediante el acceso a los datos a los que se refiere la consulta, hasta el extremo de que el artículo 9.6 del reglamento de la Ley 10/2010 se refiere expresamente a la base de datos de titularidad real del Consejo General del Notariado como fuente de las citadas informaciones a cuya obtención está obligado el sujeto obligado.

De este modo, no cabe duda de que la cesión de los datos por parte de la consultante a otros sujetos obligados encuentra su cobertura en los artículos 4 y 8 de la Ley 2010, lo que implica asimismo que, por aplicación del artículo 11.2 a) de la Ley Orgánica 15/1999 no será necesario el consentimiento del afectado para que la comunicación de datos pueda tener lugar. Por ello, el Acuerdo remitido resulta conforme a lo dispuesto en la mencionada Ley Orgánica."

Las conclusiones alcanzadas en el citado informe son igualmente extrapolables a los supuestos en que haya de procederse al tratamiento de datos para el cumplimiento de las restantes obligaciones de diligencia debida, no siendo preciso obtener el consentimiento de los clientes para el tratamiento de los datos cuando la Ley imponga la obligación de recabar de los mismos la citada información ni exigiéndose el consentimiento en los supuestos en que la propia Ley habilite la obtención de dichos datos como consecuencia de la consulta de los sistemas de información de terceros. Esta misma regla operará al amparo del Reglamento general de protección de datos, conforme a su artículo 6.1 c).

A la vista de todo ello, y sin perjuicio de las medidas legislativas que pudieran adoptarse en el futuro y que deberán someterse al informe de esta Agencia, el tratamiento de los datos necesario para el cumplimiento de las medidas de diligencia debida establecidas en la legislación de prevención del blanqueo de capitales y la financiación del terrorismo no exige en el presente momento recabar el consentimiento de los interesados.