



Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley por la que se modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo, solicitado de esta Agencia Española de Protección de Datos de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica, de 13 de diciembre, de Protección de datos de Carácter Personal, y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, cúmpleme informarle lo siguiente:

I

Tal y como indica su Exposición de Motivos, el objetivo del Anteproyecto sometido a informe consiste en lograr la plena trasposición 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, conocida como IV Directiva de prevención de blanqueo de capitales, teniendo igualmente en cuenta los proceso de revisión parcial que de la misma se está llevando a cabo a partir de la propuesta de modificación, respecto de la que consta la existencia de un texto de compromiso de fecha 19 de diciembre de 2017. Igualmente, se prevé como objetivo de la norma el ajuste y mejora de alguna de las disposiciones de la vigente Ley, entre las que podría hacerse referencia a las previstas en los artículos 32, 33 y 43 de la Ley 10/2010, que afectan directamente al derecho fundamental a la protección de datos de carácter personal.

Por otra parte, y como es suficientemente sabido, el marco regulador del derecho a la protección de datos de carácter personal ha sido objeto de una profunda modificación como consecuencia de la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dicha norma se encuentra en vigor desde el 25 de mayo de 2016, si bien no será

plenamente aplicable hasta el 25 de mayo de 2018, tal y como establece su artículo 99.

En todo caso, dada la proximidad de la plena aplicación de la norma de la Unión, resultará imprescindible en el análisis que se lleve a cabo en el presente informe atender a su contenido, toda vez que será la disposición plenamente aplicable en el momento en que el Anteproyecto ahora objeto de informe sea finalmente aprobado, en su caso.

Al propio tiempo, debe señalarse que el 10 de noviembre de 2017 el Consejo de Ministros aprobó y acordó la remisión a las Cortes Generales del Proyecto de Ley Orgánica de Protección de Datos, por la que el ordenamiento jurídico español se adapta al citado Reglamento, norma ésta de aplicación directa, como se ha indicado, a partir del 25 de mayo de 2017. El citado Proyecto de Ley Orgánica resulta especialmente relevante en lo que atañe a alguna de las disposiciones contenidas en el Anteproyecto ahora informado, al referirse ambas normas, al menos parcialmente, a cuestiones similares. Así sucede, por ejemplo, en lo que respecta a los sistemas de denuncias recogidos en el artículo 26 bis de la Ley 10/2010 cuya inclusión pretende el Anteproyecto.

Por último, y en lo que respecta a las actuaciones relacionadas con la detección, prevención, investigación y enjuiciamiento de delitos, debe igualmente traerse a colación la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Dicha norma debería ser traspuesta por los Estados Miembros antes de 6 de mayo de 2018, tal y como prevé su artículo 63.1, sin que por el momento conste la adopción de dicha norma de trasposición en nuestro país. No obstante, y sin perjuicio de la necesidad de atender a lo dispuesto en la Directiva, debe señalarse que en tanto no se produjera dicha trasposición sería de aplicación a los tratamientos sometidos a su ámbito de aplicación lo dispuesto en la vigente Ley Orgánica 15/1999 en lo que no se oponga a ella y, particularmente, lo establecido en los artículos 22 a 24 de dicha Ley Orgánica.



Así se establece igualmente para el supuesto de que dicha norma de trasposición no se adoptase en el momento de aprobación de la nueva Ley Orgánica de Protección de Datos su disposición transitoria quinta, según la cual “Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva”

Por último, debe tenerse en cuenta que esta Agencia Española de Protección de Datos ha participado activamente en la redacción de las disposiciones contenidas en la vigente Ley 10/2010 en aquellas materias que afectan al objeto de sus competencias, debiendo traerse a colación los informes de 3 de abril y 16 de noviembre de 2009 en relación con la Ley 10/2010, así como el de 18 de febrero de 2014, referido al entonces Proyecto de Reglamento de desarrollo de la Ley 10/2010, aprobado por Real Decreto 304/2014, de 5 de mayo.

Igualmente, deben tenerse en cuenta los diversos informes emitidos en cumplimiento de lo dispuesto en el artículo 61.2 del citado Reglamento de desarrollo, así como la activa participación de la Agencia como miembro de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

II

Entrando ya en el análisis del contenido del Anteproyecto sometido a informe, y aun a costa de no seguir la estructura sistemática del texto, se va a hacer referencia en primer lugar a las disposiciones que directamente podrían considerarse relacionadas con el derecho fundamental a la protección de datos de carácter personal, contenidas en los artículos 32 y 33 del Anteproyecto.

Dentro de las citadas disposiciones debe especialmente tenerse en cuenta la propuesta de un nuevo apartado 6 del artículo 33 de la Ley 10/2010 según la cual “Los sujetos obligados, previa autorización de la Comisión, podrán crear sistemas comunes de almacenamiento de la información y documentos recopilados en ejecución de las obligaciones de diligencia debida, y sus actualizaciones. Sin perjuicio de la puesta en común de los procesos de actualización, las restantes medidas de seguimiento continuo de la relación de



negocios serán desarrolladas de manera individualizada por cada entidad. La información solamente será accesible a aquellos sujetos obligados que tengan a la persona física o jurídica como cliente, o aquellas que estén en proceso de su captación como cliente, debiendo las entidades informar al cliente del acceso que se va a llevar a cabo”.

De este modo, el Anteproyecto prevé que la creación de sistemas de información comunes, ya existentes en relación con los supuestos de análisis especial y comunicación por indicio, cuente igualmente con amparo legal cuando se trate del cumplimiento de las obligaciones de diligencia debida establecidas en el Capítulo II de la Ley 10/2010.

Ello conduce a la necesidad de traer a colación la consulta planteada a la Agencia Española de Protección de Datos por la Asociación española de Banca, a la que se dio respuesta en informe de 24 de julio de 2017. La última de las cuestiones que se planteaban en dicha consulta se refería a la procedencia de modificar la Ley 10/2010 a fin de excluir el consentimiento del interesado para el tratamiento de los datos de carácter personal necesarios para el cumplimiento por los sujetos obligados de sus obligaciones de diligencia debida, concluyendo el informe que “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”.

Esta conclusión se razonaba, teniendo ya en cuenta las previsiones del reglamento General de Protección de Datos, en los siguientes términos:

“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.”

Del mismo modo, se recordaba en el citado informe que la cesión entre sujetos obligados de los datos necesarios para el cumplimiento de las obligaciones de diligencia debida ya había sido analizada en términos favorables por la Agencia cuando se valoró la conformidad a la Ley Orgánica 15/1999 del acceso por los sujetos asociados a la consultante a la Base de Datos de Titularidad real del Consejo General del Notariado. 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.

Quiere todo ello decir que esta Agencia ya se ha pronunciado en el sentido de considerar que tanto el tratamiento de datos necesario para el cumplimiento de las obligaciones de diligencia debida como el acceso a información de terceros para lograr dicho cumplimiento se encuentran amparados en la existencia de una obligación legal de tratamiento prevista en la normativa reguladora de la prevención de blanqueo de capitales y financiación del terrorismo, sin que sea preciso en ninguno de los dos casos recabar el consentimiento de los afectados.



Teniendo en cuenta estos antecedentes podría ser conveniente que el Anteproyecto recogiese ambos supuestos de forma específica, a fin de garantizar la seguridad jurídica, máxime teniendo en cuenta la reforma del marco regulador de la protección de datos de carácter personal.

Por otra parte, la ubicación sistemática de la norma propuesta, como apartado adicional del artículo 33 de la Ley 10/2010 podría generar o plantear problemas interpretativos, toda vez que dicho precepto se refiere en el resto de su texto al intercambio de información relacionada con el examen especial de operaciones y la comunicación al Servicio Ejecutivo de la Comisión, es decir, obligaciones contenidas en el Capítulo II de la Ley, al que también se remite el artículo 32 del texto.

Por este motivo, podría ser aconsejable que las disposiciones relacionadas con la aplicación de las normas de protección de datos en lo que respecta al cumplimiento de las obligaciones de diligencia debida se recogiesen de forma independiente a las establecidas en los artículos 32 y 33, introduciendo un precepto, que por su ubicación sistemática podría ser un nuevo artículo 31 bis, en que apareciesen dichas previsiones.

El precepto debería, a juicio de esta Agencia contar con dos apartados diferenciados: el primero con la única finalidad de clarificar, de conformidad con lo indicado anteriormente que el tratamiento de datos necesario para el cumplimiento de los deberes de diligencia debida del Capítulo II de la Ley se encontrará fundado en el cumplimiento de una obligación legal, de conformidad con lo dispuesto en el artículo 6.1 c) del Reglamento General de Protección de Datos; y el segundo para regular lo que actualmente el Anteproyecto establece en el nuevo apartado 6 del artículo 33. Será en este punto donde deba proceder nuestro estudio.

Como ya se ha señalado, siendo el sistema común que se describe en el artículo 33.6 incluido en el Anteproyecto un sistema auxiliar de los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida, debe considerarse que su base legal es coincidente con la relacionada con el cumplimiento de estas obligaciones. Por este motivo, debe, como punto de partida, considerarse que la propuesta es conforme al Reglamento General de protección de datos, al ser estos sistemas necesarios para el cumplimiento de las obligaciones legales impuestas a los sujetos obligados por la propia Ley 10/2010.

Ahora bien, a nuestro juicio sería necesario completar el precepto a fin de establecer un régimen más completo de derechos y obligaciones en relación con los mencionados sistemas, resolviendo igualmente algunas cuestiones que se derivarían de lo establecido en la propia normativa de protección de datos de carácter personal.



La primera de las cuestiones a resolver es la de si los sistemas deberían permitir la puesta en común de la información por todos los sujetos obligados independientemente de las categorías en que se incardinan conforme al artículo 2 de la Ley o si su ámbito de participación debería ser más reducido.

A nuestro juicio, la respuesta a esta cuestión debería ser restrictiva de las categorías de sujetos obligados que pudieran intercambiar la información, dentro siempre de la enumeración establecida por el artículo 2. De este modo, cuando los sujetos pudieran incardinarse en la misma letra del precepto (lo que en ocasiones no supone que se dediquen en todo caso a una misma actividad) sería posible la creación de este tipo de sistemas sin ningún tipo de limitación. Por el contrario, en caso de no existir dicha identidad sería posible la creación de los sistemas, si bien sometiéndola a la previa autorización de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, en términos similares a los previstos en el artículo 33.1 de la Ley 10/2010, de forma que la Comisión resuelva qué tipos de sujetos obligados podrán constituir estos sistemas y qué información necesaria para el cumplimiento de las obligaciones de diligencia debida podrán intercambiar.

La segunda cuestión sería la referida a la información que, como máximo, podría incorporar el sistema, pareciendo ajustado a la finalidad de cumplimiento de las obligaciones de diligencia debida que sea, en todo caso, la relacionada con la identificación del interesado, así como en su caso de su condición de persona de relevancia pública. Igualmente, sería posible compartir la información disponible acerca de la titularidad real.

También sería posible la inclusión en los sistemas de la información referida al propósito o índole de la relación de negocios cuando dicha información pudiese tener un carácter objetivo, si bien en estos supuestos será necesario que cada sujeto obligado realice las actuaciones tendentes al cumplimiento de esta obligación respecto de su relación particular con el interesado. Finalmente, por motivos obvios, no debería incorporarse a los sistemas la información referida al seguimiento de la relación de negocios, que deberá ser llevada a cabo por cada sujeto obligado de forma evidentemente diferenciada.

Una tercera cuestión que deberá resolverse es la referida a la responsabilidad del tratamiento. A tal efecto, debe recordarse que el artículo 26.1 del Reglamento general de Protección de Datos dispone que “Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en



que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados”.

Añade el apartado 2 del mismo artículo 26 que “El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo”.

A nuestro juicio, teniendo en cuenta el modo en que se configurarían estos sistemas, los sujetos obligados adheridos a los mismos deberían tener la condición de corresponsables, de modo que cada uno de ellos responderá de la información que incorpore al sistema.

En todo caso, es preciso tener en cuenta que la responsabilidad a la que se está haciendo referencia es la relacionada con la normativa de protección de datos de carácter personal. Quiere ello decir que los sujetos obligados deberían en todo caso verificar el cumplimiento de sus obligaciones de diligencia debida, siendo la información accedida únicamente un elemento que facilita el cumplimiento de sus obligaciones en materia de prevención, pero que no excluye la necesidad de adoptar las que resulten necesarias a tales efectos.

Los sujetos obligados podrían encomendar el mantenimiento de los sistemas a un tercero, incluso aunque no tuviera la condición de sujeto obligado. El indicar esta circunstancia permitiría amparar estos sistemas en la Ley incluso en los supuestos en que quien gestionase el sistema de información no pudiese considerarse incluido dentro de los sujetos a los que se refiere el artículo 8 de la Ley 10/2010.

Por otra parte, sería necesario establecer determinadas garantías que garanticen el cumplimiento de los principios de protección de datos y al propio tiempo eviten el acceso indebido a la información del sistema.

Así, en primer lugar, los accesos a la información contenida en el sistema deberían quedar limitados a quienes ya fuesen clientes del sujeto obligado que lo solicitase o a quienes pretendiesen iniciar con él una relación de negocio. No obstante, en este último supuesto la documentación accesible debería ser únicamente la necesaria para dar cumplimiento a las obligaciones establecidas a tal efecto por el artículo 3 de la Ley 10/2010.

Por otra parte, sería necesaria la intervención del órgano de prevención del sujeto obligado, tanto para la incorporación de la información al sistema como para canalizar las solicitudes de información, garantizando así el establecimiento de un filtro que permita detectar posibles supuestos en que se pretenda un acceso indebido a la información.



Además en garantía del principio de limitación de finalidad, contemplado por el artículo 5.1 b) del reglamento General de Protección de Datos, los datos obtenidos deberán ser tratados únicamente para finalidades relacionadas con el cumplimiento de los deberes de diligencia debida, previstas en la normativa de prevención del blanqueo de capitales y la financiación del terrorismo.

Igualmente, sería necesario que los datos del sistema respetasen el principio de exactitud al que se refiere el artículo 5.1 d) del reglamento, de forma que los mismos sean “exactos y, si fuera necesario, actualizados” y que se adopten “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”. Por este motivo, si un sujeto obligado detectase la inexactitud de la información o que la misma no está actualizada debería ponerlo de inmediato en conocimiento del sistema para que se proceda a su actualización o rectificación.

Finalmente, deberían implantarse en el sistema, en cumplimiento de las medidas de responsabilidad activa establecidas en el Capítulo IV del Reglamento General de Protección de Datos, medidas técnicas y organizativas que garanticen la integridad, disponibilidad y seguridad de la información contenida en aquél. En particular, será necesario que se garantice la trazabilidad de los accesos producidos, a fin de poder verificar que los mismos se llevaron a cabo para el cumplimiento de las obligaciones de diligencia debida y no para otros fines distintos.

A la vista de todo lo que se ha venido indicando, se propone la inclusión de dos nuevos artículos 31 bis y 31 ter con el siguiente tenor literal.

“Artículo 31 bis. Protección de datos en el cumplimiento de las obligaciones de diligencia debida

El tratamiento de datos de carácter personal que resulte necesario para el cumplimiento de las obligaciones establecidas en el Capítulo II de esta Ley se encuentra amparado por lo supuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos no precisando del consentimiento del interesado.

Artículo 31 ter. Sistemas comunes de información para el cumplimiento de las obligaciones de diligencia debida

1. Los sujetos obligados pertenecientes a una misma categoría de las establecidas en el artículo 2 de esta Ley podrán crear sistemas comunes de información, almacenamiento y, en su caso, acceso a



la información y documentación recopilada para el cumplimiento de las obligaciones de diligencia debida establecidas en el Capítulo II, con excepción de la relacionadas con el seguimiento continuo de la relación de negocios, recogida en el artículo 8.

Los sujetos adheridos al sistema tendrán la condición de corresponsables del tratamiento a los efectos previstos en el artículo 26 del reglamento (UE) 2016/679.

El mantenimiento de estos sistemas podrá encomendarse a un tercero, aun cuando no tenga la condición de sujeto obligado.

Los sujetos obligados corresponsables deberán comunicar a la Comisión de Prevención del Blanqueo de Capitales e infracciones monetarias la intención de constituir estos sistemas al menos sesenta días antes de su puesta en funcionamiento.

2. La comunicación de datos a los sistemas así como el acceso a los datos incorporados a los mismos se encuentran amparados en lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

Los sujetos obligados sólo podrán acceder a la información facilitada por otro sujeto obligado en los supuestos en que la persona a la que se refieran los datos sea su cliente o el acceso a la información sea necesario para el cumplimiento de las obligaciones de identificación previas al establecimiento de la relación de negocios previstas en el artículo 3. En este supuesto, sólo se accederá a los datos necesarios a tal efecto.

3. Los datos serán facilitados al sistema por los órganos de control interno previstos en el artículo 26 ter. Estos órganos canalizarán asimismo las solicitudes de acceso a los datos contenidos en el sistema.

En todo caso, los interesados deberán ser informados acerca de la comunicación de los datos al sistema así como del acceso que pretendiese llevarse a cabo con carácter previo a que el mismo se produzca.

4. Los datos obtenidos como consecuencia del acceso al sistema únicamente podrán ser empleados para el cumplimiento por los sujetos obligados de lo dispuesto en el Capítulo II de esta Ley.

5. Cuando el sujeto obligado compruebe, a la vista de la información que él mismo hubiese recabado en cumplimiento de sus deberes de diligencia debida, que los datos a los que hubiese



accedido son incorrectos o no están actualizados, lo comunicará al sistema a fin de que los datos sean objeto de actualización o rectificación en su caso.

Del mismo modo deberá proceder cuando aprecie que un documento incorporado al sistema deba ser sustituido por otro más reciente.

6. Sin perjuicio de las restantes medidas que deban adoptarse en cumplimiento de lo dispuesto en el Capítulo IV del Reglamento (UE) 2016/679, el sistema de información incorporará medidas que garanticen la trazabilidad de los accesos al mismo.

6. La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias podrá autorizar el establecimiento de sistemas comunes en que participen varias categorías de sujetos obligados, delimitando dichas categorías y la información que podrá ser compartida.”

IV

En cuanto a las previsiones de reforma del artículo 32 de la Ley 10/2010, incluidas en el apartado ocho de su artículo cuarto.

Como cuestión previa, debe indicarse que los supuestos contemplados en las letras b) y c) del apartado 2 de este precepto, que se añadirían como consecuencia de la reforma proyectada, no serían necesarias siempre y cuando se tuviera en consideración lo indicado en el apartado anterior de este informe.

En efecto, como se indica en el artículo 31 bis propuesto, el tratamiento de los datos para el cumplimiento de los deberes impuestos a los sujetos obligados por el Capítulo I está amparado por lo establecido en el artículo 6.1 c) del Reglamento general de Protección de Datos, teniendo en cuenta las obligaciones impuestas a los citados sujetos no sólo por la normativa interna, sino por la IV Directiva, por lo que no sería preciso amparar dichos tratamientos en el consentimiento de los interesados. De este modo, tanto el acceso a la información obtenida por el grupo para el cumplimiento de tales fines como el de los datos referidos a la titularidad real se encontrarían amparados por el citado artículo 31 bis propuesto en conexión con el mencionado artículo 6.1 c), sin que fuera ya necesario indicarlo expresamente, siendo la redacción propuesta mucho más amplia que la que se derivaría de las dos letras citadas.

Habiendo establecido en dos preceptos diferenciados los tratamientos referidos al cumplimiento de las obligaciones previstas en los Capítulos II y III de la Ley, y en cuanto a la base legal del tratamiento que se lleve a cabo para



el cumplimiento de las disposiciones del Capítulo III, cabe considerar que sería, al igual que en lo que afecta a las disposiciones del Capítulo II el cumplimiento de las obligaciones legalmente impuestas a los sujetos obligados por la normativa interna y de la Unión. El propio texto propuesto lo dejaría claro en la letra a) del artículo 33.2, dado que se refiere expresamente al “cumplimiento de las obligaciones de información a que se refiere el Capítulo III”. Por ello, sería necesario modificar el apartado 1 proyectado, dado que la base legal se encontraría en el apartado c) y no en el e) del artículo 6.1 del Reglamento, sin perjuicio de que el tratamiento llevado a cabo por las autoridades competentes sí lo sea en cumplimiento de una misión de interés público, lo que sin embargo no necesita precisarse, en aplicación del artículo 87 de la Directiva (UE) 2016/680.

En cuanto a la limitación del derecho de información al interesado, así como de los restantes derechos establecidos en la normativa de protección de datos, conforme parece desprenderse del artículo 32.3, sería preciso en primer lugar que se hiciese referencia expresa de los citados derechos, toda vez que parece que se ha omitido el primer inciso del párrafo segundo actual artículo 32.3 de la Ley 10/2010.

Por lo que respecta a la exclusión a la que acaba de hacerse referencia, debe recordarse que el artículo 14.5 del Reglamento General de Protección de Datos establece que “Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que (...) c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria”.

En cuanto al ejercicio de los restantes derechos, debe recordarse que el artículo 23.1 del Reglamento establece los supuestos en los que el derecho de la Unión o el de los Estados miembros podrá establecer excepciones y limitaciones al ejercicio de los derechos contemplados en los artículos 15 a 22 cuando ello sea necesario para “la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención” (apartado d) o por “otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social” (apartado e), siempre que establezca ciertas especificaciones a las que se refiere el apartado 2 del artículo 23 del Reglamento general de Protección de Datos, siendo así que la normativa de la



Unión en materia de prevención del blanqueo de capitales y la financiación del terrorismo, así como su norma de transposición al derecho español, tanto actualmente a través de la Ley 10/2010 como en lo que corresponde completarla con el Anteproyecto sometido a informe, establecen esas garantías requeridas por el artículo 23.2 del Reglamento.

No obstante, sería necesario que el responsable, dentro del nuevo enfoque derivado del establecimiento del principio de responsabilidad activa, regulado por el Capítulo IV del Reglamento, adopte las medidas necesarias para garantizar el derecho de los afectados a los que pudieran referirse los datos en estos supuestos, teniendo en cuenta la minoración de ese derecho que representa la no aplicación de las previsiones referidas a los derechos de los afectados.

En particular, debe recordarse que el artículo 35 del reglamento general de Protección de Datos impone a los responsables la obligación de llevar a cabo una evaluación de impacto en la protección de datos “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas”.

El artículo 35.10 del Reglamento no obstante dispone que “cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento”. No obstante, no consta que la evaluación se llevase a cabo al adoptarse la IV Directiva de prevención el Blanqueo de capitales.

En definitiva, de lo que se trata es de reemplazar la referencia actual a las medidas de seguridad de nivel alto contempladas en el Título VIII del reglamento de desarrollo de la Ley Orgánica 15/1999, dado que la plena aplicación del Reglamento supone la derogación tácita de dicho Título, por cuanto será el responsable quien deba adoptar las medidas técnicas y organizativas necesarias para preservar los derechos de los afectados. En este sentido, el Anteproyecto sometido a informe se refiere a la adopción de “medidas de seguridad y control reforzadas”.

Debe finalmente hacerse referencia a la condición de encargados del tratamiento de los órganos centralizados de prevención.



En este punto, no debe olvidarse que el artículo 44.6 del reglamento de la Ley 10/2010 establece lo siguiente respecto de los órganos centralizados de prevención de incorporación obligatoria; es decir los referidos a los sujetos obligados a que se refiere el artículo 2.1.n) de la Ley 10/2010:

“Sin perjuicio de lo dispuesto en el artículo 32.4 de la Ley 10/2010, los órganos centralizados de prevención a los que se refiere este artículo tendrán la condición de responsables de los tratamientos que lleven a cabo por propia iniciativa o a requerimiento de la Comisión o de sus órganos de apoyo, o de cualquier otra autoridad pública legalmente habilitada, con la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo.

Igualmente serán responsables de los tratamientos efectuados en el marco de sus funciones de análisis de riesgo y de supervisión establecidos en la normativa de prevención del blanqueo de capitales y la financiación del terrorismo, así como de los que se deriven directamente del acceso y tratamiento de la información de los datos contenidos en los ficheros de los que los propios órganos fueran responsables, tanto en el marco de las obligaciones de diligencia debida como en las de examen especial e información establecidas en la normativa de prevención del blanqueo de capitales.

En los supuestos a los que se refiere el apartado anterior, no será de aplicación a la actividad de los órganos centralizados de prevención lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre.

Este precepto fue introducido como consecuencia de la propuesta efectuada por esta Agencia española de Protección de Datos, teniendo en cuenta lo señalado por la misma en su informe al Acuerdo del Consejo general del Notariado de creación del fichero Base de datos de titularidad real”, de fecha 23 de febrero de 2012, en que se señalaba lo siguiente:

“(…) en cuanto a la delimitación del responsable del tratamiento el Acuerdo se limita a indicar que el mismo será “el órgano correspondiente dentro del Consejo General del Notariado”.

No deben en este punto olvidarse las funciones atribuidas por la Orden ECO/2693/2005 al Órgano Centralizado de Prevención creado por la misma, tanto en lo relativo al análisis especial de operaciones como en la comunicación de operaciones sospechosas al Servicio Ejecutivo. En este marco, el artículo 1 de la citada Orden encomienda a ese órgano “el reforzamiento, intensificación y canalización en la colaboración del notariado con las autoridades judiciales, policiales y administrativas responsables de la lucha contra el blanqueo de capitales”.



En este mismo sentido, la Orden EHA/114/2008, de 29 de enero, por la que se Regula el cumplimiento de determinadas obligaciones de los notarios en el ámbito de la prevención del blanqueo de capitales crea en su Anexo II del fichero de Cumplimiento de las obligaciones de tratamiento y comunicación de datos derivadas de lo dispuesto en los artículos 17 y 24 de la Ley del Notariado, con la finalidad de garantizar el “cumplimiento por el Consejo General del Notariado de las obligaciones de tratamiento y comunicación de datos derivadas de lo dispuesto en los artículos 17 y 24 de la Ley del Notariado” y recabando datos a partir de la “remisión de comunicaciones de los notarios y del índice único informatizado”. De dicho fichero es directamente responsable el mencionado Órgano Centralizado de Prevención.

Pues bien, el fichero ahora objeto de creación tiene por finalidad el “cumplimiento por el notario y por OCP de sus deberes de diligencia debida, examen especial e información a las autoridades competentes previstos en la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales”, recabando la información de idénticas fuentes a las anteriormente citadas.

Ciertamente el Consejo será el titular y responsable del índice único informatizado del que se obtendrá la información contenida en el fichero objeto ahora de creación, dado que el artículo 17.2 de la Ley del Notariado, en la redacción dada al mismo por la [Ley 36/2006, de 29 de noviembre, de medidas para la prevención del fraude fiscal](#), dispone en su párrafo segundo que “el Consejo General del Notariado formará un índice único informatizado con la agregación de los índices informatizados que los notarios deben remitir a los Colegios Notariales. A estos efectos, con la periodicidad y en los plazos reglamentariamente establecidos, los notarios remitirán los índices telemáticamente a través de su red corporativa y con las garantías debidas de confidencialidad a los Colegios Notariales, que los remitirán, por idéntico medio, al Consejo General del Notariado”.

Sin embargo, ello no empece que el fichero ahora analizado pueda ser responsabilidad del Órgano Centralizado de Prevención, al que corresponde precisamente la función de garantizar el efectivo cumplimiento por los notarios de las obligaciones establecidas en la Ley 10/2010.

Al propio tiempo, debe recordarse que, conforme a lo dispuesto en el artículo 5.1 q) del Reglamento de desarrollo de la Ley Orgánica 15/1999 el responsable del fichero podrá ser “persona física o jurídica, de naturaleza pública o privada, u órgano administrativo”, por lo que nada impide que un órgano creado con tal naturaleza en el seno del Consejo General del Notariado ostente la condición de responsable del fichero.



Por último, la atribución de la responsabilidad del fichero al Órgano Centralizado de Prevención garantiza que se dé pleno cumplimiento a los deberes establecidos en la Ley 10/2010 y, particularmente, a la prohibición de revelación prevista en su artículo 22, dado que el Consejo, en sí mismo, no tiene la condición de sujeto obligado de la Ley 10/2010.

Por este motivo, se propone que el apartado g) sea modificado, en el sentido de indicar que el órgano responsable del fichero será el Órgano Centralizado de Prevención del Blanqueo de Capitales del Consejo General del Notariado.”

Pues bien, a nuestro juicio, la posibilidad de que los órganos centralizados de prevención de incorporación obligatoria puedan ostentar la condición de responsable del tratamiento en determinadas circunstancias debería consagrarse en el texto del Anteproyecto, a fin de evitar la aparente contradicción que podría producirse entre el citado artículo 32.4 y el artículo 44.6 del Reglamento de desarrollo de la Ley.

Por último, y dado que el párrafo segundo del artículo 32.1 excluye el consentimiento del interesado en los supuestos establecidos en el artículo 24.2, es preciso indicar que, efectivamente, el intercambio de información previsto en dichos preceptos se produciría en cumplimiento de una obligación legal, y por tanto amparado en el artículo 6.1 c) del Reglamento general de Protección de Datos, toda vez que los apartados 3 a 5 del artículo 39 de la Directiva 2015/849 exceptúan la prohibición de revelación prevista en su apartado 1 en los siguientes términos:

“3. La prohibición establecida en el apartado 1 no impedirá la comunicación de información entre las entidades financieras y de crédito, o entre estas entidades y sus sucursales y filiales en las que tengan participación mayoritaria situadas en terceros países, a condición de que las sucursales y las filiales con participación mayoritaria cumplan plenamente las políticas y procedimientos a nivel de grupo con arreglo al artículo 45, incluidos los procedimientos de intercambio de información dentro del grupo, y de que las políticas y procedimientos a nivel de grupo cumplan los requisitos establecidos en la presente Directiva.

4. La prohibición establecida en el apartado 1 no impedirá la comunicación de información entre las entidades obligadas a que se refiere el artículo 2, apartado 1, punto 3, letras a) y b), o entidades de terceros países que impongan requisitos equivalentes a los enunciados en la presente Directiva, que ejerzan sus actividades profesionales, ya sea como empleados o de otro modo, dentro de una misma entidad jurídica o en una estructura más amplia a la que pertenece la persona y



que comporta una propiedad, una gestión o una supervisión del cumplimiento comunes.

5. Cuando se trate de las entidades obligadas a que se refiere el artículo 2, apartado 1, puntos 1 y 2, y punto 3, letras a) y b), en los casos que se refieran a un mismo cliente y a una misma transacción en la que intervengan dos o más entidades obligadas, la prohibición establecida en el apartado 1 del presente artículo no impedirá la comunicación de información entre las entidades obligadas pertinentes, siempre que sean entidades de un Estado miembro o entidades de un tercer país que imponga requisitos equivalentes a los establecidos por la presente Directiva, pertenezcan a la misma categoría profesional y estén sujetas a obligaciones en lo relativo al secreto profesional y la protección de los datos personales.”

Tomado en consideración todo lo que ha venido indicándose se propone la siguiente redacción del artículo 32 de la Ley 10/2010 para su inclusión en el Anteproyecto sometido a informe:

“Artículo 32. Protección de datos en el cumplimiento de las obligaciones de información.

1. El tratamiento de datos de carácter personal que resulte necesario para el cumplimiento de las obligaciones establecidas en el Capítulo III de esta Ley **se encuentra amparado por lo supuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679, no precisando del consentimiento del interesado.**

Tampoco será necesario el consentimiento para las comunicaciones de datos previstas en el citado Capítulo y, en particular, para las previstas en el artículo 24.2, **quedando igualmente amparadas por el artículo 6.1 c) del Reglamento (UE) 6179/2016.**

2. En virtud de lo dispuesto en el artículo 24.1, **y de conformidad con el artículo 14.5 del Reglamento (UE) 2016/679**, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo **14 en relación con los tratamientos a los que se refiere el apartado anterior**

Asimismo, **de conformidad con el artículo 23 del Reglamento (UE) 679/2016, no procederá la atención de los derechos establecidos en los artículos 15 a 22 del Reglamento en relación con los citados tratamientos.** En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.



Lo dispuesto en el presente apartado será igualmente aplicable a los **tratamientos llevados a cabo** por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta Ley.

3. Los órganos centralizados de prevención a los que se refiere el artículo 27 tendrán la condición de encargados del tratamiento a los efectos previstos en la normativa de protección de datos de carácter personal.

Se exceptúan de lo señalado en el párrafo anterior los tratamientos que llevasen a cabo los órganos centralizados de prevención de incorporación obligatoria en el ámbito de las funciones que se le atribuyan reglamentariamente. La norma reglamentaria especificará los supuestos en que estos órganos tengan la condición de responsables del tratamiento

4. Los sujetos obligados deberán realizar una evaluación de impacto en la protección de datos de los tratamientos a los que se refiere este artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos de carácter personal. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos.

En todo caso, el tratamiento deberá llevarse únicamente a cabo por los órganos a los que se refiere el artículo 26 ter de esta Ley.”

V

Las conclusiones alcanzadas en apartados anteriores de este informe deberán igualmente tenerse en consideración en la redacción del artículo 33 del Anteproyecto sometido a informe, que regula los sistemas comunes de información para el cumplimiento de las obligaciones establecidas en el Capítulo III de la Ley.

De este modo, debería excluirse de la reforma de dicho artículo el proyectado apartado 6, que ahora sería reemplazado por el artículo 32 ter. Igualmente, los apartados 4 y 5 proyectados deberían ajustarse en su redacción a las redacciones propuestas en este informe para los apartados 2 y 4 del artículo 32 de la Ley 10/2010.

Junto con lo antedicho, sería precisa la modificación del apartado 2, a fin de evitar la confusión producida por la remisión que el mismo efectuaba al artículo 19 de la Ley. En efecto, tal y como se desprende de los informes emitidos por esta Agencia en relación con los sistemas creados al amparo del



vigente artículo 33 de la Ley, así como de las autorizaciones emitidas por la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, la garantía de la exactitud de los datos contenidos en los sistemas y su posible vinculación con el blanqueo de capitales o la financiación del terrorismo exige que la información incorporada a estos sistemas se refiera únicamente a la que ha sido objeto de comunicación por indicio al Servicios Ejecutivo y que además no ha sido objeto de devolución por éste, conforme le habilita el penúltimo párrafo del artículo 18.2.

De este modo, el precepto debería incorporar ambas circunstancias en su apartado 2.

Al propio tiempo, debería suprimirse la referencia a “ficheros”, toda vez que el reglamento General de Protección de Datos ya sólo tiene en consideración este concepto jurídico para los supuestos de tratamientos no automatizados, lo que no sucederá en este supuesto. Así, habrá de centrarse la redacción en los términos “tratamiento” y “sistema de información”, rechazándose la referencia a “ficheros”.

A la vista de todo ello, se propone la siguiente redacción del artículo 33, para su inclusión en el Anteproyecto sometido a informe:

“Artículo 33. *Intercambio de información entre sujetos obligados y ficheros centralizados de prevención del fraude.*

1. Sin perjuicio de lo establecido en el artículo 24.2, cuando concurren las circunstancias excepcionales que se determinen reglamentariamente, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias podrá acordar el intercambio de información referida a determinado tipo de operaciones distintas de las previstas en el artículo 18 o a clientes sujetos a determinadas circunstancias siempre que el mismo se produzca entre sujetos obligados que se encuentren en una o varias de las categorías previstas en el artículo 2.

El Acuerdo determinará en todo caso el tipo de operación o la categoría de cliente respecto de la que se autoriza el intercambio de información, así como las categorías de sujetos obligados que podrán intercambiar la información.

2. Asimismo, los sujetos obligados podrán intercambiar información relativa a las operaciones a las que se **refiere el artículo 18** con la única finalidad de prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla.



Quedarán excluidas aquéllas operaciones que hayan sido objeto de devolución por el Servicio Ejecutivo de la Comisión, conforme al artículo 18.2 de esta Ley.

3. El tratamiento de los datos de carácter personal al que se refieren los dos apartados anteriores, cuando proceda, se encontrará amparado en lo dispuesto en el artículo 6.1 e) del Reglamento (UE) 679/2016, no siendo preciso contar con el consentimiento del interesado.

4. En virtud de lo dispuesto en el artículo 24.1, y de conformidad con el artículo 14.5 del Reglamento (UE) 2016/679, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 14 en relación con los tratamientos a los que se refieren los apartados 1 y 2.

Asimismo, de conformidad con el artículo 23 del Reglamento (UE) 679/2016, no procederá la atención de los derechos establecidos en los artículos 15 a 22 del Reglamento en relación con los citados tratamientos. En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

5. Los sujetos obligados o quienes desarrollen los sistemas que sirvan de soporte al intercambio de información al que se refieren los apartados 1 y 2 deberán realizar una evaluación de impacto en la protección de datos de los citados tratamientos a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos de carácter personal. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos.

El acceso a los datos quedará limitado a los órganos de control interno previstos en el artículo 26 ter, con inclusión de las unidades técnicas que constituyan los sujetos obligados.”

6. Los sujetos obligados y las autoridades judiciales, policiales y administrativas competentes en materia de prevención o represión del blanqueo de capitales o de la financiación del terrorismo podrán consultar la información contenida en los **sistemas que fueren creados, de acuerdo con lo previsto en la normativa vigente en materia de protección de datos de carácter personal, por entidades privadas con la finalidad de prevención del fraude en el sistema financiero, siempre que el acceso a dicha información fuere necesario para las finalidades descritas en los apartados anteriores.”**



VI

Debe ahora hacerse referencia a los sistemas de denuncia regulados por el artículo 26 bis propuesto por el apartado dos del artículo 4 del Anteproyecto sometido a informe bajo la denominación de “procedimientos internos de comunicación de potenciales incumplimientos”.

A tal efecto, el Anteproyecto se refiere a la obligación de los sujetos obligados que no se encontrasen excluidos de ello por previsión reglamentaria de establecer procedimientos para que sus empleados, directivos o agentes pedan denunciar el posible incumplimiento de la Ley 10/2010 y su normativa de desarrollo por dichos sujetos obligados, indicando el apartado 2 que dichos canales de denuncia deberán ser “independientes y anónimos”, si bien podrán coincidir con los que tuviera implantados la entidad para la recepción de otro tipo de denuncias.

En relación con esta cuestión debe indicarse que el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, actualmente en tramitación parlamentaria, regula en su artículo 24 lo que denomina “Sistemas de información de denuncias internas en el sector privado”, dentro de los cuales encajarían los que se recogerían en el artículo 26 bis de la Ley 10/2010 que ahora se propone, estableciendo, en su redacción conforme al Proyecto remitido a las Cortes, lo siguiente:

“1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento. Sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.



4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias. Si fuera necesaria su conservación para continuar la investigación, podrán seguir siendo tratados en un entorno distinto por el órgano de la entidad al que compete dicha investigación.

No será de aplicación a estos sistemas la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.”

El apartado XII del informe emitido por esta Agencia el 11 de julio de 2017 al Anteproyecto de Ley Orgánica se refiere a estos sistemas, su fundamento y la justificación de las garantías especiales previstas en el texto, señalando lo siguiente:

“El artículo 17 del Anteproyecto regula los sistemas de información de denuncias internas en el sector privado, siendo ésta una materia que no había sido objeto de regulación específica con anterioridad, sin perjuicio de la existencia de diversos dictámenes de la Agencia Española de Protección de Datos, así como del Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE que se referían a este tipo de tratamientos.

En cuanto a la necesidad de regular dichos sistemas, debe recordarse que el artículo 31 bis del Código Penal en la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo regula el régimen de responsabilidad penal de las personas jurídicas. Así, su apartado 1 señala que “En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión,



vigilancia y control de su actividad atendidas las concretas circunstancias del caso.”

No obstante, el apartado 2 del artículo establece una serie de condiciones acumulativas para que pueda eximirse de responsabilidad a la persona jurídica, entre los que la condición 1ª se refiere a que “el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión”.

Estos sistemas deberán cumplir los requisitos establecidos en el apartado 5 del artículo 31 bis, exigiéndose en el párrafo 4º de dicho apartado que los sistemas “Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención”.

La Circular 1/2016, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del código penal efectuada por Ley Orgánica 1/2015, al analizar los requisitos establecidos en el citado artículo 31 bis.5 4ª indica en su apartado 5.3 (bajo la rúbrica “condiciones y requisitos de los modelos de organización y gestión”) lo siguiente:

“Si bien esta primera condición del apartado 2 no lo menciona expresamente, un modelo de organización y gestión, además de tener eficacia preventiva debe posibilitar la detección de conductas criminales. Lo sugiere el cuarto requisito del apartado 5, cuando impone “la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y la observancia del modelo de prevención.” La existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención. Ahora bien, para que la obligación impuesta pueda ser exigida a los empleados resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (whistleblower), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos...) sin riesgo a sufrir represalias.”

Todo ello hace necesario el establecimiento de un régimen que regule los sistemas de denuncia interna de estos ilícitos en que se recojan las garantías esenciales del derecho fundamental a la protección de datos, permitiendo a las entidades el cumplimiento de los requisitos legalmente exigidos para asegurar sus exención de la responsabilidad penal.



En relación con estos sistemas, el apartado 1 del citado artículo 17 prevé que a través de los mismos podrán “ponerse en conocimiento de una entidad privada, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable”.

De este modo, frente al criterio tradicionalmente sostenido por esta Agencia Española de Protección de Datos, en que se propugnaba el carácter confidencial y no anónimo de estos sistemas, se establece la posibilidad de que las denuncias sean comunicadas al sistema “incluso anónimamente”. Esta previsión, no obstante, trae causa de la fundamentación jurídica de dichos sistemas, que acaba de ser descrita, por cuanto su existencia resulta vital para la posible exención de la responsabilidad penal de la persona jurídica. Por este motivo, y aun considerándose excepcional la inclusión de estos datos, cabe concluir, de conformidad con lo señalado en la Circular 1/2016 de la Fiscalía General del Estado, que estos sistemas podrán tener el mencionado carácter.

Ello no obstante exige reforzar las garantías de exactitud y acceso a la información obrante en esos sistemas. Por este motivo, el artículo 17 establece un sistema en que se determinan claramente las garantías que deberán implantarse en los mismos a fin de poder hacer ponderar a favor del interés legítimo de la entidad responsable la legitimación para el tratamiento de los datos.

De este modo, y además de ser exigible la previa información a quienes pudieran ser objeto de denuncia de la existencia de los sistemas y d la obligación de preservar la identidad del denunciante, cuando el mismo hubiera facilitado este dato, el artículo 17 impone dos exigencias adicionales:

Por una parte, el apartado 2 limita al máximo el acceso a los datos, dado que el mismo únicamente podrá llevarse a cabo por el personal que lleve a cabo las funciones de control interno y de cumplimiento de la entidad y, sólo cuando procediera la adopción de medidas disciplinarias contra un trabajador, al personal con funciones de gestión y control de recursos humanos.

Por otra, se limita la conservación de los datos en el sistema a un período de tres meses, sin que opere en este caso la obligación de bloqueo que será objeto de análisis con posterioridad. Ello no implica que en caso de que la denuncia pueda considerarse fundada y dé lugar a una concreta investigación los datos deban suprimirse de los sistemas de la entidad, sino que únicamente procederá su supresión del concreto



sistema de información de denuncias internas, pasando a integrarse en los sistemas propios del órgano de cumplimiento o, en su caso, del que tenga a su cargo la gestión de recursos humanos.

Las garantías citadas permiten aplicar en favor del responsable la regla de ponderación del interés legítimo establecida en el artículo 6.1 f) del Reglamento General de Protección de datos, procediendo así informar favorablemente este artículo.

En todo caso, debe clarificarse que los sistemas descritos en el precepto únicamente se refieren a las denuncias internas formuladas en el sector privado y ninguna relación guardan con el tratamiento de las denuncias que se formularan, cualquiera que sea su naturaleza, ante el sector público, en que el órgano administrativo receptos de las mismas habrá de estar a lo dispuesto en su normativa específica y en la Ley 39/2015, de 1 de octubre."

Debe igualmente indicarse que con la única excepción de una enmienda de supresión propuesta por un Grupo Parlamentario, únicamente se han planteado enmiendas tendentes a la mejora técnica del apartado 4 del precepto, por lo que es probable que, con esa mejora técnica que no afecta al contenido del precepto, el precepto se incorpore finalmente al texto legal, al existir una apoyo mayoritario a su mantenimiento.

Si bien podría aparentemente considerarse que la finalidad que justifica la creación de los sistemas a los que se refiere el Anteproyecto sometido a informe no coincide plenamente con la derivada de la aplicación del artículo 31 bis del Código Penal, debe recordarse que el artículo 302.2 del citado Código reconoce expresamente la responsabilidad de la persona jurídica en los delitos de blanqueo de capitales, por lo que sí cabe apreciar una identidad de razón entre ambos sistemas de denuncia, sin perjuicio de la finalidad de prevención que puede llevar aparejada la creación de estos sistemas en el ámbito sometido al Anteproyecto ahora informado.

Teniendo en cuenta lo anterior, se informa favorablemente la creación de estos sistemas de denuncia. No obstante, se considera que sería precisa una mayor correlación de los mismos con el régimen general establecido en la normativa de protección de datos, lo que afectaría esencialmente a los dos primeros apartados del precepto contenido en el Anteproyecto.

En primer lugar, si bien, como se ha indicado al hacer referencia al informe de esta Agencia, no es preciso que los sistemas se basen en la confidencialidad de los datos del denunciante, pudiendo admitir denuncias anónimas, no termina de comprenderse por qué motivo el precepto sometido a informe excluye en todo caso la confidencialidad, imponiendo el anonimato en las comunicaciones. Por este motivo, se considera que sería posible indicar que el sistema podría recibir denuncias anónimas, en términos similares a los



previstos en el Proyecto de Ley Orgánica de Protección de Datos, sin excluir necesariamente la posibilidad de que el comunicante opte por su identificación.

Por otra parte, la redacción del apartado 2 podría simplificarse, limitándose a señalar que los sistemas podrían ser compatibles con otros sistemas de denuncias internas, sin que se haga referencia a la independencia para posteriormente excepcionarla, como hace el Anteproyecto.

Finalmente, sería preciso que se indicase que estos sistemas estarán sujetos a las garantías establecidas en la normativa de protección de datos y que contrarrestan el efecto que la información pudiera producir en el derecho del afectado. En este sentido, sería conveniente que se clarificase que el órgano de control del cumplimiento previsto en el Proyecto de Ley Orgánica será el regulado por el artículo 26 ter del Anteproyecto.

A la vista de todo ello, se propone la siguiente redacción del artículo 26 bis:

1. Los sujetos obligados, con las excepciones que se determinen reglamentariamente, establecerán procedimientos internos para que sus empleados, directivos o agentes puedan comunicar, **incluso anónimamente**, información relevante sobre posibles incumplimientos de esta Ley, su normativa de desarrollo o las políticas y procedimientos implantados para darles cumplimiento, cometidas en el seno del sujeto obligado.

Estos procedimientos podrán integrarse en los sistemas que hubiera podido establecer el sujeto obligado para la comunicación de informaciones relativas a la comisión de actos o conductas que pudieran resultar contrarios a la restante normativa general o sectorial que les fuera aplicable.

2. **Será de aplicación a estos sistemas y procedimientos lo dispuesto en la normativa de protección de datos de carácter personal para los sistemas de información de denuncias internas.**

A estos efectos, se considerarán como órganos de control interno y cumplimiento exclusivamente los regulados en el artículo 26 ter.

3. Los sujetos obligados adoptarán medidas para garantizar que los empleados, directivos o agentes que informen de las infracciones cometidas en la entidad sean protegidos frente a represalias, discriminaciones y cualquier otro tipo de trato injusto.

4. La obligación de establecimiento del **procedimiento** de comunicación descrito en los párrafos anteriores, no sustituye la necesaria existencia



de mecanismos específicos e independientes de comunicación interna de operaciones sospechosas de estar vinculadas con el blanqueo de capitales o la financiación del terrorismo por parte de empleados a las que se refiere el artículo 18.”

VII

El artículo 48 bis de la Ley 10/2010, en la redacción propuesta por el apartado cinco del artículo séptimo del Anteproyecto sometido a informe regula el régimen de cooperación internacional de la Comisión y el Servicio Ejecutivo para la prevención del blanqueo de capitales y la financiación del terrorismo. A tales efectos, es preciso diferenciar dos supuestos en virtud del Estado con el que se lleve a cabo la cooperación.

Respecto de los Estados Miembros de la Unión Europea, el apartado 1 del artículo 48 bis dispone que “La Secretaría de la Comisión, el Servicio Ejecutivo de la Comisión o los órganos supervisores a que se refiere el artículo 44, cooperarán por propia iniciativa o previa solicitud, con otras autoridades competentes de la Unión Europea siempre que sea necesario para llevar a cabo las funciones establecidas en esta Ley, haciendo uso, a tal fin, de todas las facultades que la misma les atribuye”. A su vez, el artículo 48 bis.3 establece que “El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de Estados de la Unión Europea se realizará de conformidad con lo dispuesto en los artículos 51 a 57 de la Directiva 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 la prevención del blanqueo de capitales o la financiación del terrorismo”.

De este modo, la transmisión de datos entre los Estados Miembros, como tratamiento no constitutivo de transferencia internacional de datos, al no referirse a Estados terceros, debe considerarse amparado en lo dispuesto en la propia Directiva 2015/849, siendo necesario para el cumplimiento de una misión de interés público establecida en dicha Directiva. Por ello, encontraría su amparo legal en el artículo 6.1 e) del Reglamento General de Protección de Datos.

En cuanto a la colaboración con terceros Estados, dispone el apartado 2 del precepto que “En el caso de autoridades competentes de terceros países no miembros de la Unión Europea, la cooperación e intercambio de información se condicionará a lo dispuesto en los Convenios y Tratados Internacionales o, en su caso, al principio general de reciprocidad, así como al sometimiento de dichas autoridades extranjeras a las mismas obligaciones de secreto profesional que rigen para las españolas”, añadiendo el apartado 4 que “El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de terceros países no miembros de la Unión Europea se realizará de acuerdo con los principios del Grupo Egmont o en los términos



del correspondiente memorando de entendimiento. Los memorandos de entendimiento con Unidades de Inteligencia Financiera serán suscritos por el Director del Servicio Ejecutivo, previa autorización de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias”.

En relación con este punto, debe tenerse en cuenta que el artículo 42.1 b) del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, en una redacción que no ha sido objeto de enmienda alguna por parte de los Grupos Parlamentarios en el Congreso de los Diputados, dispone que “Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos (...) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento”.

De este modo, cuando la colaboración se fundamente en un acuerdo no normativo, como sucede en el caso de los memorandos de entendimiento será precisa, además de la autorización de la Comisión de Prevención del Blanqueo de Capitales e infracciones Monetarias, la autorización de esta Agencia Española de Protección de Datos.

Ciertamente, el sometimiento del memorando a un doble procedimiento de autorización podría resultar complejo. No obstante, la opinión favorable de la Agencia resulta imprescindible, conforme al citado precepto, para que proceda el intercambio de la información.

Por este motivo, se propone modificar el apartado 4 del artículo 48 bis, pasando a tener el siguiente tenor literal:

“El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de terceros países no miembros de la Unión Europea se realizará de acuerdo con los principios del Grupo Egmont o en los términos del correspondiente memorando de entendimiento. Los memorandos de entendimiento con Unidades de Inteligencia Financiera serán suscritos por el Director del Servicio Ejecutivo, previa autorización de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, **debiendo contar con el previo informe favorable de la Agencia Española de Protección de Datos.**”



VIII

Debe finalmente hacerse referencia a la reforma que se plantea en el Anteproyecto del denominado “fichero de titularidades financieras”, regulado por el artículo 43, cuya reforma plantea el apartado tres del artículo quinto del texto sometido a informe.

En relación con este punto debe señalarse que esta Agencia ya informó favorablemente, con las modificaciones posteriormente incorporadas al texto, el régimen jurídico del fichero de titularidades financieras contenido en la vigente Ley 10/2010 y su Reglamento de desarrollo.

Por otra parte, la legitimación para el establecimiento de una base de datos como la que se está analizando se verá además reforzada por la aprobación en el futuro de la V Directiva de prevención de blanqueo de capitales y la financiación del terrorismo, dado que el texto de compromiso de la citada norma, al que ya se ha hecho referencia en un lugar anterior de este informe, incorpora la adición a la Directiva 2015/849 de un nuevo artículo 32 bis, en que se establecerá lo siguiente:

“1. Los Estados miembros implantarán mecanismos centralizados automatizados, como registros centrales o sistemas centrales electrónicos de consulta de datos, que permitan la identificación, en tiempo oportuno, de cualquier persona física o jurídica que posea o controle cuentas de pago y cuentas bancarias identificadas con un número IBAN y cajas de seguridad tal y como se definen en el Reglamento (UE) n.º 260/2012 del Parlamento Europeo y el Consejo, en una entidad de crédito en su territorio. Los Estados miembros notificarán a la Comisión las características de estos mecanismos nacionales.

2. Los Estados miembros se asegurarán de que la información conservada en los mecanismos centralizados contemplados en el apartado 1 del presente artículo sea directamente accesible, de forma inmediata y no filtrada, por las UIF. La información también será accesible por las autoridades competentes, con miras al cumplimiento de las obligaciones que les impone la presente Directiva. Los Estados miembros se asegurarán de que cualquier UIF esté en condiciones de facilitar a cualquier otra UIF, en tiempo oportuno y conforme a lo establecido en el artículo 53, la información conservada en los mecanismos centralizados contemplados en el apartado 1 del presente artículo.

3. Estará accesible y será consultable, gracias a los mecanismos centralizados contemplados en el apartado 1, la información siguiente:



- *respecto del cliente-titular de la cuenta y de cualquier persona que pretenda actuar en nombre del cliente: el nombre y los apellidos, complementados con los demás datos de identificación requeridos por las disposiciones nacionales que incorporen el artículo 13, apartado 1, letra a), o con un número de identificación único;*
- *respecto del titular real del cliente-titular de la cuenta: el nombre y los apellidos, complementados con los demás datos de identificación requeridos por las disposiciones nacionales que incorporen el artículo 13, apartado 1, letra b), o con un número de identificación único;*
- *respecto de la cuenta bancaria o la cuenta de pago: el número IBAN y la fecha de apertura y cierre;*
- *respecto de la caja de seguridad: el nombre y los apellidos del arrendatario, complementados con los demás datos de identificación requeridos por las disposiciones nacionales que incorporen el artículo 13, apartado 1, o con un número de identificación único y la duración del período de arrendamiento.*

4. *Los Estados miembros podrán considerar la posibilidad de exigir que esté accesible y sea consultable, gracias a los mecanismos centralizados, cuanta información se considere esencial para las UIF y las autoridades competentes con miras al cumplimiento de las obligaciones que les impone la presente Directiva.*

5. *A más tardar el 26 de junio de 2020, la Comisión presentará al Parlamento Europeo y al Consejo un informe en el que evalúe las condiciones y las especificaciones y procedimientos técnicos que permitan garantizar la interconexión segura y eficiente de los mecanismos centralizados automatizados. Cuando proceda, ese informe irá acompañado de una propuesta legislativa.”*

Dicho lo anterior, el Anteproyecto ahora sometido a informe introduce algunas modificaciones relevantes en relación con el artículo 43 de la Ley 10/2010 y el régimen del fichero de titularidades financieras.

Así, en primer lugar, se modifica la finalidad del fichero, que sería la de prevenir, impedir y perseguir la financiación del terrorismo, el blanqueo de capitales y sus delitos precedentes”. Se amplía así la finalidad inicial del fichero desde la persecución de dos tipos penales concretos a la totalidad de los delitos en que pueda producirse una conducta posterior constitutiva de los mismos, sin excluir, según parece deducirse del texto la necesaria imputación de un delito de blanqueo de capitales o financiación del terrorismo, por cuanto no se prevé que el acceso sea complementario a la persecución del delito



precedente cuando existan indicios de la posible comisión del delito de blanqueo o del de financiación del terrorismo.

Por otra parte, se produce una modificación sustancial del apartado 3, por cuanto se suprime la necesaria autorización judicial o del Ministerio Fiscal para el acceso al fichero por parte de las Fuerzas y Cuerpos de Seguridad, lo que a su vez puede incidir en las funciones de control que, con independencia de las que corresponden a esta Agencia, se prevén en el apartado 4 del artículo 43.

Finalmente, se amplían los supuestos de acceso a los datos del fichero, que ahora se extienden a la Oficina de Gestión y Recuperación de Activos, el Centro de Inteligencia contra el terrorismo y el Crimen Organizado, la Comisión Nacional del Mercado de Valores y el Centro Nacional de Inteligencia. Además, se suprime la referencia a la Ley General Tributaria como fundamento legal del acceso por parte de la Agencia Estatal de la Administración Tributaria.

Consecuencia de los tres cambios anteriormente señalados es la de que se modifica tanto la finalidad del tratamiento de los datos como las categorías de destinatarios de los datos como, finalmente las garantías previas que justifican el acceso en el caso de las Fuerzas y Cuerpos de Seguridad. Todo ello lleva aparejadas importantes consecuencias en materia de protección de datos de carácter personal, teniendo en cuenta la naturaleza del sistema de información al que se está haciendo referencia, en que se incorporarán la totalidad de los datos sobre titularidades y cajas de seguridad de todas las entidades de crédito sujetas al derecho español, lo que implica un tratamiento masivo de datos de la práctica totalidad de la población de nuestro país y de cualquier otra persona que fuese titular de un producto de pasivo en el mismo.

A mayor abundamiento, las reformas propuestas no guardan relación con lo establecido en el Proyecto artículo 32 bis de la Directiva 2015/849, sino que se refieren a cuestiones que escapan de la regulación contenida en ese precepto.

Ello plantea importantes problemas desde el punto de vista de la aplicación de la normativa de protección de datos de carácter personal, teniendo en cuenta la doctrina sentada por el Tribunal de Justicia de la Unión Europea en relación con el posible tratamiento masivo de datos para su puesta a disposición de las autoridades competentes para la prevención, investigación, averiguamiento y enjuiciamiento de delitos.

En efecto, el Tribunal ha tenido la ocasión de pronunciarse acerca de la conformidad con el Derecho de la Unión, y particularmente con los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea de una norma de derecho derivado de la Unión, la Directiva 2006/24/CE, que permitía la conservación por los operadores de los datos de tráfico generados por los abonados y usuarios de comunicaciones electrónicas para su comunicación a



las autoridades competentes para la detección, prevención, investigación y enjuiciamiento de delitos graves, considerando que dicha medida vulnera dichos preceptos, por lo que la declara inválida (sentencia de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y otros).

Posteriormente, en su sentencia de 21 de diciembre de 2016 (Asuntos acumulados C-2013/15 y C-698/15, Tele2 Sverige AB y otros) el Tribunal analizó si las normas nacionales de trasposición de la mencionada Directiva 2006/24/CE podían considerarse conformes al Derecho de la Unión, apreciando que no existía dicha conformidad en una norma que previera la recogida generalizada e indiscriminada de los datos y no sometiera el acceso a los mismos al previo control administrativo y judicial.

En relación con la primera de las cuestiones mencionadas, el apartado 94 de la sentencia recordaba que “con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley y respetar su contenido esencial”, añadiendo el apartado 96 que “el respeto del principio de proporcionalidad se desprende igualmente de la reiterada jurisprudencia del Tribunal de Justicia según la cual la protección del derecho fundamental al respeto de la vida privada a nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencias de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 56; de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 77; Digital Rights, apartado 52, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 92)”.

Dicho lo anterior, conforme al apartado 100, “la injerencia que supone una normativa de este tipo en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta tiene una gran magnitud y debe considerarse especialmente grave”. Y añade el apartado 103 que “si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 51)”.

Se concluye así que “una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario



y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta (apartado 107), siendo sin embargo conforme al Derecho de la Unión “una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido” (apartado 108), para lo que la norma nacional “debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso. Debe indicar, en particular, en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, garantizando que tal medida se limite a lo estrictamente necesario (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 54 y jurisprudencia citada)” (apartado 109). El apartado 11 señala que la delimitación del colectivo afectado “puede garantizarse mediante un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos, que existe un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas”.

Por su parte, en cuanto a la segunda de las cuestiones señaladas; esto es, la relativa al control judicial o administrativo independiente y previo, el Tribunal señala en su apartado 116 que “en relación con el respeto del principio de proporcionalidad, una normativa nacional que regula los requisitos con arreglo a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos conservados debe garantizar, conforme a lo expresado en los apartados 95 y 96 de la presente sentencia, que tal acceso sólo se produzca dentro de los límites de lo estrictamente necesario”.

Será a juicio del Tribunal “el Derecho nacional en que debe determinar los requisitos conforme a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder dicho acceso. No obstante, la normativa nacional de que se trata no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, ni siquiera el de la lucha contra la delincuencia grave. En efecto, tal normativa nacional debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 61)” (apartado 118).



El apartado 120 concluye que “Para garantizar en la práctica el pleno cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 62; véanse igualmente, por analogía, en relación con el artículo 8 del CEDH, TEDH, 12 de enero de 2016, Szabó y Vissy c. Hungría, CE:ECHR:2016:0112JUD003713814, §§ 77 y 80)”.

IX

La doctrina que acaba de ponerse de manifiesto exige que el tratamiento masivo de datos para la persecución del delito se delimite claramente desde un triple punto de vista: por una parte se minimicen los datos objeto de tratamiento; por otra, se limiten los supuestos en que el acceso a los datos pueda llevarse, especificando por ejemplo la naturaleza de los delitos cuya gravedad justifica ese acceso; y por último, que exista un control, que en el caso de España debería ser judicial, previo al efectivo acceso a la información.

El texto ahora objeto de análisis sí cumpliría el primero de los requisitos mencionados, al minimizar, en correlación con el proyectado artículo 32 bis de la Directiva, la cantidad de datos que se incorporará al fichero de titularidades financieras.

Al propio tiempo, en su redacción actualmente vigente, la norma analizada, el artículo 43 de la Ley 10/2010 también daría cumplimiento a los restantes requisitos exigidos por la jurisprudencia, por cuanto el acceso queda limitado en principio a la prevención, investigación y enjuiciamiento del blanqueo de capitales y la financiación del terrorismo y se prevé la autorización judicial o del Ministerio Fiscal para que los datos sea accesibles por las Fuerzas y Cuerpos de Seguridad.

Sin embargo, el texto ahora sometido a informe altera las dos garantías que acaban de mencionarse.

Así, en primer lugar, se prevé una ampliación de la finalidad del fichero a la persecución de los delitos precedentes al blanqueo o la financiación del terrorismo, sin especificar si la investigación llevada a cabo por estos delitos precedentes es independiente de la que es realmente objeto de la Ley y



constituía la finalidad inicial del tratamiento. De este modo, se podría en la práctica producir el acceso al fichero en cualesquiera supuestos de investigación de delitos con contenido económico, con independencia de que existiese o no una investigación acerca de la prevención del blanqueo de capitales y la financiación del terrorismo, dado que en caso de existir esta vinculada a los delitos precedentes no sería preciso llevar a cabo una ampliación de la finalidad del fichero en el texto legal.

Del mismo modo, y de manera aún más evidente, desaparece del apartado 3 del texto toda referencia al control judicial o fiscal previo al acceso al fichero y ni siquiera se indica que las Fuerzas y Cuerpos de Seguridad que accedan a los datos lo harán en su condición de policía judicial.

Ello conduce a dos consecuencias necesarias para garantizar la conformidad del precepto con la jurisprudencia que se ha analizado anteriormente: por una parte, deberá suprimirse la referencia a los delitos precedentes, manteniendo el texto actualmente vigente y, por otra, deberá añadirse al apartado 3 el control judicial o fiscal previo al acceso, en los términos en que actualmente se recoge en la Ley 10/2010.

X

Junto con las cuestiones que acaban de añadirse, ya se inició que el texto sometido a informe incluye igualmente nuevos supuestos de acceso a los datos contenidos en el fichero de titularidades financieras, siendo preciso valorar si todas ellas pueden considerarse adecuadas a la finalidad de dicho fichero y si las mismas encuentran cobertura legal

En relación con el acceso por la Oficina de Gestión y Recuperación de Activos, el artículo 1 del Real decreto 948/2015, de 23 de octubre aclara que la Oficina de Recuperación y Gestión de Activos “se configura como un órgano de la Administración General del Estado y auxiliar de la Administración de Justicia, al que corresponden las competencias de localización, recuperación, conservación, administración y realización de los efectos, bienes, instrumentos y ganancias procedentes de actividades delictivas cometidas en el marco de una organización criminal y de cualesquiera otras que se le atribuyan, en los términos previstos en la legislación penal y procesal” y añade que la misma “actuará cuando se lo encomiende el juez o tribunal competente, de oficio o a instancia del Ministerio Fiscal o de la propia Oficina”.

La Oficina de Recuperación y Gestión de Activos se encuentra regulada por la Disposición adicional sexta de la Ley de Enjuiciamiento Criminal, introducida por el apartado dieciocho del artículo único de la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales.



El apartado 1 de la citada disposición señala en su primer párrafo que “la Oficina de Recuperación y Gestión de Activos es el órgano administrativo al que corresponden las funciones de localización, recuperación, conservación, administración y realización de efectos procedentes de actividades delictivas en los términos previstos en la legislación penal y procesal”. El párrafo segundo de dicho apartado 1 añade que “cuando sea necesario para el desempeño de sus funciones y realización de sus fines, la Oficina de Recuperación y Gestión de Activos podrá recabar la colaboración de cualesquiera entidades públicas y privadas, que estarán obligadas a prestarla de conformidad con su normativa específica”.

De este modo, la actuación de la Oficina se llevará siempre a cabo en virtud de un mandato judicial o como consecuencia de éste, por lo que el acceso a los datos para la averiguación de los productos financieros de los que pueda ser titular un determinado sujeto se encontraría amparado en las funciones que le atribuye la Ley de Enjuiciamiento Criminal.

Del mismo modo, puede considerarse conforme a la doctrina derivada de la jurisprudencia que se ha analizado el acceso por el Centro Nacional de Inteligencia, siempre que se suprima la referencia a los delitos precedentes, en los términos que ya se han indicado con anterioridad y se someta el acceso al control judicial previo.

En cuanto al acceso por el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, el texto sometido a informe lo vincula con las funciones que al mismo atribuye la Ley 12/2003, de 21 de mayo. EN este sentido, el artículo 3 del Real Decreto 413/2015, de 29 de mayo, por el que se aprueba el Reglamento de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, creado por el artículo 9 de la citada Ley, dispone que “La Secretaría de la Comisión, prevista en el artículo 9 de la Ley 12/2003, de 21 de mayo, será ejercida por el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), dependiente de la Secretaría de Estado de Seguridad”, al que corresponde, conforme a su apartado 2:

“a) Instruir los procedimientos sancionadores a que hubiere lugar por las infracciones a la Ley 12/2003, de 21 de mayo, incluyendo la formulación de propuesta de resolución para la Comisión.

b) Recibir de las Administraciones Públicas y personas obligadas la información relacionada con el bloqueo de la financiación de actividades del terrorismo a que se refiere el artículo 4 de la Ley 12/2003, de 21 de mayo.



c) Recibir y tramitar, conforme a las normas de este Reglamento, las solicitudes de autorización de liberación o puesta a disposición de fondos o recursos económicos bloqueados en ejecución de un acuerdo de la Comisión.

d) Recibir y tramitar las peticiones de supresión de personas y entidades de las listas de terroristas elaboradas por la Unión Europea y Naciones Unidas.

e) Elaborar informes que permitan a la Comisión decidir sobre las solicitudes de verificación de identidad a que se refiere el artículo 12.

f) Cualesquiera otras tareas que le encomiende la Comisión.”

Por ello, este acceso, basado en la condición del Centro de Secretaría de la Comisión de Prevención y Bloqueo de la Financiación del Terrorismo, se encontrará amparado en las competencias atribuidas a la Comisión por el artículo 9 y a las que dentro de la misma le otorga a la Secretaría el artículo 3 del Reglamento de Funcionamiento de dicha Comisión.

En relación con los accesos por parte de la Administración Tributaria, ya aparecen actualmente recogidos en la Ley 10/2010. Sin embargo, a juicio de esta Agencia, debería mantenerse la referencia a la Ley General Tributaria como norma que ampara el acceso, especialmente a los efectos previstos en sus artículos 93 y 94.

Por el contrario, y a diferencia de los supuestos anteriormente indicados, relacionados todos ellos con la prevención, enjuiciamiento e investigación de los delitos de blanqueo y financiación del terrorismo, el acceso a los datos por parte de la Comisión Nacional del Mercado de Valores se llevaría a cabo en el marco de sus competencias para la persecución e investigación de conductas constitutivas de abuso de mercado en los mercados de valores, tratándose así de un acceso basado en competencias administrativas y no de naturaleza judicial o vinculadas a ellas, lo que podría resultar excesivo a los efectos analizados en la jurisprudencia del Tribunal de Justicia de la Unión a menos que existiese una norma de Derecho de la Unión o de derecho interno que otorgase a la Comisión, en su condición de supervisor del mercado de Valores la competencia que justificase la proporcionalidad del acceso a los datos del fichero de titularidades financieras. Sólo en ese supuesto sería posible considerar amparado en los principios de minimización y proporcionalidad el mencionado acceso.

A la vista de todo ello, y con la salvedad que acaba de indicarse en relación con el acceso a los datos del fichero por la Comisión Nacional del Mercado de Valores (que se mantiene entre paréntesis a resultas de la existencia, en su caso, de una fundamentación suficiente para el acceso), se propone la siguiente redacción para el artículo 43 de la Ley 10/2010:



“1. Con la finalidad de prevenir, impedir **y perseguir** la financiación del terrorismo y el blanqueo de capitales, las entidades de crédito deberán declarar al Servicio Ejecutivo de la Comisión, con la periodicidad que reglamentariamente se determine, la apertura o cancelación de cuentas corrientes, cuentas de ahorro, **cuentas de pago**, cuentas de valores depósitos a plazo **y cajas de seguridad**.

La declaración contendrá, en todo caso, los datos identificativos de los titulares, representantes o autorizados, así como de cualesquiera otras personas con poderes de disposición, la fecha de apertura o cancelación, el tipo de cuenta o depósito y los datos identificativos de la entidad de crédito declarante.

2. Los datos declarados serán incluidos en **el** Fichero de Titularidades Financieras, del cual será responsable la Secretaría de Estado de Economía **y Apoyo a la Empresa**.

El Servicio Ejecutivo de la Comisión, como encargado del tratamiento, determinará, con arreglo a lo establecido en la **normativa vigente en materia de protección de datos**, las características técnicas del fichero, pudiendo aprobar las instrucciones pertinentes.

3. Con ocasión de la investigación **o persecución** de delitos relacionados con la financiación del terrorismo o el blanqueo de capitales, los **órganos jurisdiccionales**, el Ministerio Fiscal y, previa autorización judicial o del Ministerio Fiscal, las Fuerzas y Cuerpos de Seguridad, podrán obtener los datos declarados en el Fichero de Titularidades Financieras.

La Oficina de Gestión y Recuperación de Activos del Ministerio de Justicia podrá acceder al Fichero cuando exista una previa asignación de funciones por parte de un órgano jurisdiccional.

El Centro de Inteligencia contra el Terrorismo y el Crimen Organizado podrá acceder al Fichero en el marco de las competencias que tiene atribuidas en su condición de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo creada por la Ley 12/2003, de 21 de mayo, de bloqueo de la financiación del terrorismo.

El Servicio Ejecutivo de la Comisión podrá obtener los referidos datos para el ejercicio de sus competencias.



La Agencia Estatal de Administración Tributaria podrá obtener los referidos datos en los términos previstos en la Ley 58/2003, de 17 de diciembre, General Tributaria.

(La Comisión Nacional del Mercado de Valores podrá obtener los datos mencionados para la investigación y persecución del abuso de mercado en los mercados de valores.)

Toda petición de acceso a los datos del Fichero de Titularidades Financieras habrá de ser adecuadamente motivada por el órgano requirente, que será responsable de la regularidad del requerimiento. En ningún caso podrá requerirse el acceso al Fichero para finalidades distintas de la prevención, **investigación** o represión de la financiación del terrorismo o el blanqueo de capitales.

4. Sin perjuicio de las competencias que correspondan a la Agencia Española de Protección de Datos, un miembro del Ministerio Fiscal designado por el Fiscal General del Estado de conformidad con los trámites previstos en el Estatuto Orgánico del Ministerio Fiscal y que durante el ejercicio de esta actividad no se encuentre desarrollando su función en alguno de los órganos del Ministerio Fiscal encargados de la persecución de los delitos de blanqueo de capitales o financiación del terrorismo velará por el uso adecuado del fichero, a cuyos efectos podrá requerir justificación completa de los motivos de cualquier acceso.”