

Se somete a informe el Anteproyecto de Ley previamente mencionado. Dicho anteproyecto se ha presentado a esta AEPD para informe junto con su memoria de análisis de impacto normativo (MAIN). Tal y como resulta de dicha MAIN, así como de la Exposición de Motivos del Anteproyecto de Ley presentado (en adelante, APL), su objetivo básico es transponer la 5ª Directiva en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, esto es, la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, que modifica la Directiva (UE) 2015/849 (4ª Directiva), así como incorporar otras novedades aprobadas por la Directiva (UE) 2019/2177 del Parlamento Europeo y del Consejo de 18 de diciembre de 2019; y por último, ya sin venir impuestas por una Directiva, recoger otras modificaciones y mejoras puntuales que resultan de estándares internacionales aprobados por el Grupo de Acción Financiera (GAFI) o son propuestas de la autoridad nacional española encargada de la aplicación de la legislación sectorial en la materia en materia de prevención del blanqueo de capitales y la financiación del terrorismo para tratar de mejorar el funcionamiento del modelo legal establecido en España.

I

El análisis en materia de protección de datos personales de la normativa de prevención de blanqueo de capitales ha de partir de la consideración que realiza la Directiva (UE) 2015/849 en su art. 43 (cuya redacción ha sido modificada por la Directiva (UE) 2018/843 para referirse al RGPD en vez de a la Directiva 95/46) de que *el tratamiento de datos personales en virtud de la presente Directiva a fines de prevención del blanqueo de capitales y la financiación del terrorismo según se contempla en el artículo 1 se considerará de interés público (...)*

El interés público como base jurídica para la licitud del tratamiento de datos personales se contiene en el artículo 6.1, letra e) del RGPD. A su vez, el art. 6.3 RGPD establece la obligación de que dicha base habrá de ser establecida bien por el Derecho de la Unión bien por el Derecho del Estado miembro que se aplique al responsable del tratamiento. Y el segundo párrafo de este último precepto determina que dicha base jurídica “podrá” contener disposiciones específicas para adaptar la aplicación de las normas del RGPD a la materia objeto de regulación por dicha base jurídica, en este caso, la materia de prevención de blanqueo de capitales.

En aplicación de dichas especificidades, entre otras medidas, la Directiva (UE) 2015/849, en su art. 39, establece, una “prohibición de revelación” en virtud de la cual *las entidades obligadas y sus directivos y empleados no revelarán al cliente afectado ni a terceros que se está transmitiendo, se transmitirá o se ha transmitido información de conformidad con los artículos 33 o 34 ni que está realizándose o puede realizarse un análisis sobre blanqueo de capitales o financiación del terrorismo.* Como consecuencia de ello, a su vez, el art. 41.1 de la Directiva 2015/849 (no modificado por la Directiva 2018/843, -lo que sí ha hecho respecto del art. 43- por lo que sigue refiriéndose a la normativa de protección de datos ahora derogada) establece que *la Directiva 95/46/CE, transpuesta a la legislación nacional, será de aplicación al tratamiento de datos personales en virtud de la presente Directiva,* lo que ha de entenderse modificado por la derogación de dicha Directiva 95/46 por el RGPD con efectos desde el 25 de mayo de 2018, y toda referencia a la directiva derogada se entenderá hecha al RGPD (véase art. 94 RGPD). En cualquier caso, el Considerando (38) de la Directiva 2018/843 reconoce expresamente que *el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo se aplica al tratamiento de los datos personales con arreglo a la presente Directiva.*

El art. 41.4 de la Directiva 2015/849 establece que *en aplicación de la prohibición de comunicación de información que figura en el artículo 39, apartado 1, los **Estados miembros** adoptarán **medidas legislativas que restrinjan**, en su totalidad o parcialmente, **el derecho de acceso del interesado** a los datos personales que le conciernan en la medida en que dicha restricción parcial o total constituya una medida necesaria y proporcionada en una sociedad democrática, respetando debidamente los intereses legítimos de la persona afectada, con miras a: a) posibilitar el correcto cumplimiento de las funciones de la entidad obligada o la autoridad nacional competente a efectos de la presente Directiva, o b) evitar la obstrucción de procedimientos de instrucción, análisis, investigaciones o procedimientos judiciales a efectos de la presente Directiva, y a garantizar que no se ponga en peligro la prevención, investigación y detección del blanqueo de capitales y la financiación del terrorismo.*

El art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea -CDFUE- (versión consolidada DOUE 7/6/2016), así como el art. 16 del Tratado de Funcionamiento de la UE -TFUE- (versión consolidada DOUE 7/6/2016) reconocen el derecho fundamental a la protección de datos de las personas físicas. Dicha Carta se aplica, en cuanto que, como establece su art. 51.1, *las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión.*

A su vez, el art. 52.1 de la Carta establece que *cualquier **limitación** del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser **establecida por la ley** y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.*

El art. 23 del RGPD regula la posibilidad de establecer limitaciones al derecho fundamental a la protección de datos personales, siempre que se establezcan mediante “medidas legislativas”, cumpliendo un principio de proporcionalidad, y para la salvaguardia de determinados derechos o intereses de interés público merecedores de dicha protección.

*1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:*

- a) *la seguridad del Estado;*
- b) *la defensa;*
- c) *la seguridad pública;*
- d) *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;*
- e) *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;*
- f) *la protección de la independencia judicial y de los procedimientos judiciales;*
- g) *la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;*
- h) *una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);*
- i) *la protección del interesado o de los derechos y libertades de otros;*
- j) *la ejecución de demandas civiles.*

Pero establece, en su apartado 2, que

*cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:*

- a) *la finalidad del tratamiento o de las categorías de tratamiento;*
- b) *las categorías de datos personales de que se trate;*
- c) *el alcance de las limitaciones establecidas;*
- d) *las garantías para evitar accesos o transferencias ilícitos o abusivos;*
- e) *la determinación del responsable o de categorías de responsables;*
- f) *los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;*
- g) *los riesgos para los derechos y libertades de los interesados, y*
- h) *el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.*

Sentados estos principios generales, cabe decir igualmente que esta AEPD ha tenido ocasión de pronunciarse con anterioridad en varias ocasiones respecto de la normativa de prevención del blanqueo de capitales, entre las que cabe mencionar 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, así como más recientemente el Informe 41/2018, relativo a la trasposición de la Directiva (UE) 2015/849, del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, (4ª Directiva, ya citada), pero que a su vez ya tuvo en cuenta el proceso de revisión parcial que de la misma se estaba llevando a partir de su propuesta de modificación por lo que luego sería la 5ª Directiva, respecto de la que ahora se informa. Igualmente, en este Informe 41/2018 ya se sometían a la AEPD modificaciones de la norma no provenientes de la necesaria trasposición de la Directiva, que afectaban directamente al derecho fundamental a la protección de datos de carácter personal, y sobre las que ya se pronunció esta AEPD, como luego referiremos.

Cabe asimismo mencionar que la trasposición de la Directiva 2015/879 se produjo finalmente por el Real Decreto-ley 11/2018, de 31 de agosto, de transposición de directivas en materia de protección de los compromisos por pensiones con los trabajadores, prevención del blanqueo de capitales y requisitos de entrada y residencia de nacionales de países terceros y por el que se modifica la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En dicho Real Decreto Ley, por su carácter extraordinario, se incluyeron las medidas necesarias para la trasposición de la Directiva, cuyo plazo de trasposición estaba rebasado, pero

no las que no derivaban de esta, por lo que se incluyen ahora en este anteproyecto de ley sometido a informe.

## II

Se incluye un nuevo apartado 5 en el artículo 4 y unos nuevos artículos 4 bis y 4 ter, relativos a la obligación de recabar y conservar información de titularidad real de sus clientes de los sujetos obligados. Esta obligación de identificación del titular real surge del art. 13.1, letra b), de la Directiva 2015/849. El apartado 5 del art. 4 establece que para el cumplimiento de las obligaciones de identificación del titular real, los sujetos obligados recabarán de sus clientes o de las personas que tengan atribuida la representación de la persona jurídica, la información de los titulares reales, *no siendo preciso informar a los afectados* (esto es, a los titulares reales identificados por los clientes de los sujetos obligados) *acerca de la inclusión de sus datos en los ficheros **del sujeto obligado***.

Dado que la ley especifica que la no necesidad de informar al interesado resulta cuando se incluyen los datos del titular en los ficheros **del sujeto obligado**, cuando se trate de datos personales de personas físicas cabe considerar que esta restricción está amparada por la prohibición de revelación del art. 39 de la Directiva y del art. 24 de la LPBC. Pero ello será así tan sólo porque los art. 4 bis y 4 ter establecen que los clientes (sociedades, entidades y fideicomisos) deberán, por su parte, solicitar de los titulares reales dicha información, y que estos, además, tienen la obligación de suministrar dicha información a las entidades de las que son titulares reales. Ello es por tanto un verdadero tratamiento de datos, en el cual los responsables son las entidades que han de recibir dichos datos, que han de mantenerlos siempre actualizados y frente a quienes los interesados que aportan sus datos tendrán todos los derechos previstos en el RGPD (acceso, rectificación, supresión etc.).

En caso contrario, dado que el art. 4.5 se encuentra dentro del capítulo II existiría una diferencia apreciable entre los derechos de dicha persona física-titular real comunicado por los clientes del sujeto obligado, y los derechos de dichos interesados tal y como se establece el art. 32.2 en su nueva redacción. Mientras que en el artículo 32 no se establece ninguna restricción en su derecho fundamental a la protección de datos personales, respecto de las personas físicas identificadas por dichos clientes a los sujetos obligados como titulares reales en virtud de lo establecido en el artículo 4.5, dado que este precepto establece que no se les comunicará su inclusión en los ficheros del sujeto obligado, dichas personas físicas no tendrían conocimiento del tratamiento a que se someten sus datos personales los sujetos obligados. Sin embargo, dado que sí pueden ejercerlos frente a las entidades de las que son titulares reales, la limitación prevista en el art. 4.5 no se considera desproporcionada. Máxime cuando la Disposición Adicional tercera LPBC prevé un Registro de Titularidades Reales, accesible en principio de manera general

(Disposición Adicional Cuarta LPBC y art. 30.5.c) Directiva 2015/849) y que se ha de conservar actualizada (art. 30.4 Directiva 2015/849).

La nueva redacción del art. 15.3 sustituye la referencia anterior que se contenía en la LPBC a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo por la referencia conjunta al RGPD y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) de una manera que se considera correcta, por cuanto la segunda es tan sólo aplicación o especificación de la primera, pero en ningún caso la sustituye, por cuanto el RGPD tiene fuerza vinculante directa.

De igual modo, la referencia que se contiene en el art. 15.4 a que *en todo caso deberán aplicarse las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo* se considera correcta, dado que, como ya se expuso por esta AEPD en su Informe 41/2018: *“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. (...)”*

El art. 24.1 contiene una sutil modificación en cuanto a las exclusiones de reserva que impone el precepto. Frente a la redacción inicial del precepto, que establecía que la prohibición de revelación no incluirá la revelación a las autoridades competentes, incluidos (...) *la revelación por motivos policiales en el marco de una investigación penal*, la nueva redacción especifica que dicha exclusión de la revelación se aplicará cuando se trate de *agentes de la policía judicial en el marco de una investigación judicial penal*. Esta AEPD muestra su conformidad con la precisión, por cuanto que esta redacción contribuye a fortalecer el derecho fundamental de protección de los datos personales de aquellos interesados que hubieran sido comunicados por los sujetos obligados por la LPBC a las autoridades policiales, ya que dichas autoridades policiales habrán de actuar como policía judicial y bajo la dirección de un juez.

### III

Mientras que el art. 32 de la LPBC regulaba en dicho artículo la materia de protección de datos personales respecto de los tratamientos previstos por la LPBC con carácter general, el anteproyecto divide dicha regulación, dedicando el art. 32 en su nueva redacción a la protección de datos en el cumplimiento de las obligaciones de diligencia debida (Capítulo II LPBC) y un nuevo art. 32 ter a la protección de datos personales en el cumplimiento de las obligaciones de información (Capítulo III LPBC). Hay que resaltar que, a diferencia del art. 32 ter de la ley, relacionado con las particularidades de los tratamientos de datos personales resultantes del Capítulo III, la nueva redacción del art. 32, relativo a

los tratamientos resultantes del Capítulo II, no restringe los derechos de los interesados respecto de sus datos personales, por lo que si bien el tratamiento de dichos datos no precisa del consentimiento de los interesados, sus derechos no están restringidos y dichos tratamientos del Capítulo II se rigen por tanto por las reglas generales del RGPD con las especificidades previstas en la propia LPBC.

La Directiva 2018/849, en su art. 43, parte de considerar -como ya se ha mencionado- que el tratamiento de datos personales en virtud de dicha Directiva a fines de prevención del blanqueo de capitales y la financiación del terrorismo según se contempla en el artículo 1 se considerará *de interés público* en virtud del RGPD. A su vez, esta AEPD ya consideró en el Informe 41/2018, con cita del Informe de 24 de julio de 2017, que las obligaciones de previstas en dicho Capítulo II tenían como base jurídica el art. 6.1.c) RGPD, esto es, el cumplimiento de obligaciones legales impuestas a los sujetos obligados en tanto que responsables del tratamiento. Así:

*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.*

En el apartado 1 del art. 32 pues, se considera correcta la mención, como base jurídica del tratamiento, al art. 8.1 de la LOPDGDD; sin embargo no se considera tal que sólo se haga referencia a dicho artículo, por cuanto la verdadera base jurídica se encuentra en el RGPD, art. 6.1.c), ya que es esta norma la que regula el desarrollo del derecho fundamental a la protección de datos personales, máxime en una materia regida por el Derecho de la Unión (recuérdese que la ley es trasposición de la Directiva) -ver art. 51 CDFUE- y además la LOPDGDD tan sólo adapta el RGPD al ordenamiento jurídico español y completa sus disposiciones. Por ello, y tal y como establece el apartado segundo del art. 1.a) LOPDGDD “*El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica*”. En consecuencia, se sugiere introducir una mención en el artículo 32.1 por referencia al artículo 6.1.c) del Reglamento (UE) 2016/679 complementaria a la realizada al artículo

8.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales.

Por otra parte, la mención que se realiza a que los tratamientos que se realicen sobre la base del Capítulo II “no precisan del consentimiento del interesado”, si bien no daña, en realidad es innecesaria por cuanto dado que la base jurídica del tratamiento es la letra c) del art. 6.1 RGPD (cuando el tratamiento necesario para cumplimiento de una obligación legal aplicable al responsable del tratamiento) ello supone per se que no es necesario dicho consentimiento, ya que el consentimiento que es tan solo una de las bases jurídicas posibles para considerar lícito el tratamiento de datos personales, ya que dicho artículo 6.1 RGPD considera suficiente que exista al menos una de dichas bases, no siendo ya el consentimiento la base jurídica predominante o más importante, como lo era en el sistema establecido en la ley orgánica 15/1999, LOPD. Así se pronunció esta AEPD en el citado Informe 41/2018:

*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.*

A continuación el apartado 2 del art. 32 establece una limitación de la finalidad de modo que los datos recogidos por los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida no podrán ser utilizados más que para fines relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo sin el consentimiento del interesado, salvo que el tratamiento de dichos datos fuera necesario para la gestión ordinaria de la relación de negocios. Este apartado se considera correcto y conforme con el artículo 6.3 RGPD, así como con el art. 41 de la Directiva 2015/849

En cuanto a los derechos de los interesados en los tratamientos previstos en el capítulo II de la LPBC, el apartado 3 del artículo 32 requiere que el responsable facilite a los interesados la información prevista en los artículos 13 y 14 RGPD (y 11 LOPDGDD). Dicha información contendrá, adicionalmente y de manera particular, un aviso general sobre las obligaciones legales de los sujetos obligados. Esta regulación no solo se considera correcta, sino acertada por dos razones: la primera porque el derecho de información previsto contiene una circunstancia adicional que permitiría al interesado conocer que la LPBC contiene disposiciones específicas para los sujetos obligados que pueden dar lugar a que, en los casos en que la información del interesado haya de ser tratada a los efectos del capítulo III de la ley (véase art. 32 ter y art. 41.2 de la Directiva 20015/843), su derecho fundamental a la protección de datos personales puede verse limitado o restringido. A este respecto cabe añadir que

esta AEPD considera que el art. 41.3 de la Directiva contiene una obligación específica y particular de informar o avisar a los interesados sobre las obligaciones legales relacionadas con la normativa de protección de datos, sin que pueda entenderse que cupiese cumplir con esta obligación particular mediante la consideración de que una política de privacidad o cláusula de protección de datos hiciera mención genérica al cumplimiento de las obligaciones legales, en general. Por lo tanto, la redacción actual propuesta en el anteproyecto se considera conforme con dicho artículo 41.3 de la Directiva y con la normativa en materia de protección de datos personales.

Y en segundo lugar, precisamente por lo que no dice. Al no establecer este apartado ninguna limitación al derecho fundamental de protección de datos de los interesados respecto de los tratamientos previstos en el Capítulo II, dicho derecho fundamental no se ve restringido o limitado, sino que rigen al respecto las reglas generales establecidas en el RGPD y la LOPDGDD.

Se observa, por otra parte, en relación con el art. 32 que este no recoge expresamente la necesidad de que los responsables de los tratamientos previstos en dicho precepto (esto es, los tratamientos derivados del Capítulo II de la ley, sobre medidas de diligencia debida) lleven a cabo evaluaciones de impacto en la protección de datos (en adelante EIPD), como si se requiere en el anteproyecto con carácter expreso en el art. 32 ter, para los tratamientos del Capítulo III -sobre las obligaciones de información a las autoridades de prevención del blanqueo-, o en el art. 33 -respecto de los tratamientos derivados del intercambio de información entre sujetos obligados y ficheros centralizados de prevención del fraude-. A este respecto, cabe observar que, en opinión de esta AEPD, cuando se trate de tratamientos cuyas bases jurídicas derivan de las letras c) o e) del art. 6.1 RGPD, es decir, por razón de una obligación legal o una misión en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, el RGPD no impide que el Derecho de la Unión o el Derecho del Estado miembro que se aplique al responsable del tratamiento pueda contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras las que se citan -sin carácter exhaustivo- en el art. 6.3 RGPD, que incluye las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, entre las que se puede encontrar la obligación de realizar una EIPD. Pues bien, corresponde al legislador la posibilidad de determinar, en un tratamiento específico sobre la base del art. 6.1 c) o e), si ha de realizarse una EIPD, sin perjuicio de la competencia de la Autoridad de protección de datos prevista en el art. 35 RGPD. Ahora bien, el que para unos determinados tratamientos la norma no recoja la necesidad expresa de que el responsable del tratamiento realice una evaluación de impacto no significa en modo alguno que no debe a realizarla, si serán los supuestos previstos en la normativa reguladora, y que cabe concretar en el artículo 35 ya citado RGPD, que establece una obligación para responsable de realizar dicha evaluación de impacto de las operaciones de tratamiento *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, a lo que hay que añadir que si el tratamiento es de aquellos cuyo contenido o características se incluyen entre los del art. 35.3 RGPD, igualmente será necesaria la realización de una evaluación de impacto. Por último, en virtud del art. 35.4 RGPD, las autoridades de control han establecido publicado una lista de los tipos de operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1 del art RR. 35 RGPD. Dentro de la lista establecida en base a dicho precepto por la AEPD se contienen qué términos tratamientos, de entre los que cabe destacar los siguientes:*

- 1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.*
- 2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.*
- 4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.*
- 8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.*
- 10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.*
- 11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b, c, d) del RGPD.*

Parece claro a la vista de las descripciones que se realizan de estos tratamientos que los tratamientos derivados del capítulo II de la LPBC cabe incluirlos en dos o más de los anteriores ejemplos, por lo que la realización de una evaluación de impacto en materia de protección de datos será necesaria

para el responsable de dichos tratamientos. En consecuencia, el que la norma no recoja de manera expresa la necesidad para los tratamientos derivados del capítulo II de la ley de realizar una evaluación de impacto no significa, en el presente caso concreto, que los responsables no deban de realizarla a la vista de la lista de tratamientos de datos que requieren evaluación de impacto de conformidad con el artículo 35.4 LPBC. Sin embargo, en aras a la seguridad jurídica, y dado que el art. 32 ter y el artículo 33 se contienen la mención expresa de la obligación de realizar una operación de impacto en los tratamientos a que dichos preceptos se refieren, sí se necesitaría que se recogiese expresamente la obligación de realizar dicha evaluación de impacto también en los tratamientos relativos al Capítulo II LPBC.

#### IV

El art. 32 bis establece para los sujetos obligados pertenecientes a una misma categoría la posibilidad de crear sistemas comunes de información almacenamiento y acceso a la información y documentación recopilada al ejercicio de sus obligaciones de diligencia debida establecidas en el Capítulo II.

La redacción del apartado sigue literalmente -con un pequeño matiz- la redacción sugerida por esta AEPD en su Informe 41/2018, ya citado (entonces referido como art. 31 ter), después de una extensa argumentación en los apartados II y III de dicho Informe, que cabe dar por reproducidos pues el anteproyecto ahora presentado a informe sigue expresamente la sugerencia de la AEPD en cuanto a la redacción del precepto.

El único matiz diferente entre la redacción sugerida y la sometida a informe es la referencia al art. 8.1 de la LOPDGDD como base jurídica de los tratamientos. Así, mientras el Informe 41/2018 de esta AEPD mencionaba el art. 6.1.c) del RGPD, el anteproyecto se remite al ya mencionado art. 8.1 LOPDGDD. A este respecto, creemos necesario reiterar lo ya expuesto en el apartado III de este Informe:

*En el apartado 1 del art. 32 pues, se considera correcta la mención, como base jurídica del tratamiento, al art. 8.1 de la LOPDGDD; sin embargo no se considera tal que sólo se haga referencia a dicho artículo, por cuanto la verdadera base jurídica se encuentra en el RGPD, art. 6.1.c), ya que es esta norma la que regula el desarrollo del derecho fundamental a la protección de datos personales, máxime en una materia regida por el Derecho de la Unión (recuérdese que la ley es trasposición de la Directiva) -ver art. 51 CDFUE- y además la LOPDGDD tan sólo adapta el RGPD al ordenamiento jurídico español y completa sus disposiciones. Por ello, y tal y como establece el apartado segundo del art. 1.a) LOPDGDD “El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica”. En consecuencia, se sugiere*

*introducir una mención en el artículo 32.1 por referencia al artículo 6.1.c) del Reglamento (UE) 2016/679 complementaria a la realizada al artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales.*

En relación con este art. 32 bis, se sugiere que su apartado 2, párrafo primero, quede redactado así: *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 y en el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre.*

Cabe añadir que estos sistemas comunes no están exentos del resto de los preceptos del RGPD, y entre ellos de los principios establecidos en el art. 5, y particularmente al de exactitud, de modo que los datos contenidos en estos sistemas habrán de ser exactos y actualizados, debiendo ser adoptadas 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 trata (art. 5.1.d) RGPD). Como puede observarse, la regulación de estos sistemas de información comunes sigue de cerca la regulación prevista en el art. 20.1 LOPDGDD sobre los sistemas comunes de información crediticia. El párrafo final del apartado 2 establece: *Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.* Al igual que se regula en el art. 20.1, en el art. 32 bis propuesto las entidades que mantengan el sistema tendrán la condición de corresponsables, y conforme al art. 26 RGPD, corresponde a estos determinar *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.* Igualmente, en el apartado 2 del art. 26 RGPD. Por tanto, el derecho del Estado miembro aplicable al tratamiento, cuando establezca las características del tratamiento en base al art. 6.1.c), podrá determinar las responsabilidades de los corresponsables. En base a lo anterior, se considera conveniente que el art. 32. bis incluya, en su apartado 5, un párrafo inicial que determine que *Corresponderá al sujeto obligado que hubiera proporcionado los datos al sistema responder de su exactitud y actualización, debiendo cumplir en su caso lo establecido en los artículos 17.2 y 19 del Reglamento (UE) 2016/679. Conforme al art. 26.3 del Reglamento (UE) 2016/679, los interesados podrán ejercer los derechos que les reconoce el citado Reglamento frente a, y en contra de, cada uno de los responsables.* Los dos párrafos siguientes del apartado 5 del art. 32 bis se mantienen.

El art. 32 ter regula la protección de datos personales en el cumplimiento de las obligaciones de información, esto es, en los tratamientos de datos personales derivados de las obligaciones establecidas en el Capítulo III de la LPBC.

En primer lugar, en su apartado 1, primer y segundo párrafo, y al igual que se ha mencionado respecto del art. 32 y 32 bis, se considera conveniente hacer una referencia expresa al art. 6.1.c) del RGPD junto a la mención del art. 8.1 de la LOPDGDD. Del mismo modo, tal y como igualmente se ha referido, y se hizo mención también en el Informe 41/2018 de esta AEPD, siendo la base del tratamiento el art. 6.1.c) RGPD no se requiere del consentimiento de los interesados, no siendo siquiera necesario indicarlo expresamente.

A continuación es de mencionar que el presente artículo 32 ter, en su redacción íntegra actual (salvo el actual apartado 5) es consecuencia del informe 41/2018, de esta AEPD, cuya redacción se sugirió, por modificación del entonces artículo 32 del anteproyecto, que regulaba conjuntamente, como se ha mencionado, la protección de datos tanto en los tratamientos derivados del Capítulo II como del Capítulo III. En dicho Informe esta AEPD expuso lo siguiente:

*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.*

Respecto de la mención a la evaluación de impacto en materia de protección de datos a que este artículo se refiere, ya se hizo mención en el epígrafe III de este Informe que el Derecho del Estado miembro aplicable al responsable del tratamiento puede considerar, en aquellos tratamientos cuya base jurídica sea la letra c) o e) del art. 6.1, la posibilidad, conforme al art. 6.3, de establecer disposiciones específicas para adaptar la aplicación de las normas del RGPD, y entre dichas particularidades podrá considerar entre las medidas a adoptar que los responsables de dichos tratamientos lleven a cabo

la evaluación de impacto en materia de datos personales. Por ello, nada se objeta respecto del deber impuesto legalmente a los responsables de realizar dicha EIPD en los tratamientos del Capítulo III LPBC.

## VI

El art. 33 regula el intercambio de información entre sujetos obligados y ficheros centralizados de prevención del fraude. En este artículo cabe distinguir dos supuestos.

En primer lugar su apartado 1 establece la posibilidad de que (i) cuando se den unas circunstancias excepcionales no previstas en la ley, sino deferidas a su determinación por vía reglamentaria, la Comisión de Prevención del Blanqueo podrá acordar el intercambio entre sujetos obligados de información (esto incluiría un tratamiento de datos personales cuando se refiera a personas físicas) respecto de (ii) operaciones que no se definen o delimitan, o (iii) respecto de clientes sujetos a “determinadas circunstancias” que tampoco se determinan. Su apartado 2 regula la posibilidad para los sujetos obligados de intercambiar información en aquellos supuestos previstos en la ley cuando por las características de la operación de que se trate exista la posibilidad de que una vez rechazada esta puede intentarse ante otros sujetos obligados. A continuación los apartados 3, 4, 5 y 6 regulan conjuntamente aspectos relativos y aplicables tanto a los tratamientos del apartado 1 como a los del apartado 2. En concreto, el apartado 4 exceptúa a los responsables de los tratamientos de proporcionar a los interesados la información prevista en el art. 14 RGPD; y el segundo párrafo de dicho apartado 4 limita los derechos de los interesados previstos en los arts. 15 a 22 RGPD respecto de ambos tipos de tratamientos. Existe sin embargo una diferencia esencial entre los tratamientos previstos en el apartado 1 y los del apartado 2, y es que mientras que los tratamientos del apartado 2 está determinados en la ley, los del apartado 1 no lo están, sino que se remite a un reglamento para determinar dichas “circunstancias excepcionales” que permitirían a la Comisión de Prevención del Blanqueo llevar a cabo tratamiento de datos en los cuales el derecho fundamental a la protección de datos personales de los interesados está limitado.

A su vez, el art. 61.1 del Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (RLPBC) aprobado por Real Decreto 304/2014, de 5 de mayo, establece: *Conforme a lo dispuesto en el artículo 33.1 de la Ley 10/2010, de 28 de abril, cuando concurren riesgos extraordinarios identificados mediante los análisis a que se refiere el artículo 65.1.e), la Comisión, previo dictamen conforme de la Agencia Española de Protección de Datos, podrá autorizar el intercambio de información sobre determinadas categorías de operaciones o clientes.* Y el art. 65.1 RLPBC hace referencia al Comité de Inteligencia Financiera, que será responsable del análisis de riesgo nacional en materia de blanqueo de capitales y de la financiación del terrorismo, y en particular, el apartado e) de dicho art. 65.1 refiere que dicho órgano será responsable de coordinar las

acciones de análisis de riesgos en materia de blanqueo de capitales y financiación del terrorismo.

La MAIN no contiene explicación al respecto, centrándose en otros aspectos del art. 33 LPBC. No obstante, podemos considerar que el art. 33.1 LPBC está tratando de cerrar la puerta, y prever, comportamientos contrarios a la ley mediante el intercambio de información entre sujetos obligados respecto de operaciones y/o clientes que presentan características distintas de las que la ley, en principio, ha previsto como sospechosas. Esta prevención, que se considera razonable, desde el punto de vista de la normativa de protección de datos personales habrá de cumplir con los requisitos de esta regulación, puesto que no es la ley la que regula en el presente caso los supuestos, requisitos y garantías de los tratamientos de datos, sino que remite al reglamento dicha determinación, con el añadido de que dichos tratamientos, además, excluyen los derechos de los interesados en materia de protección de datos (art. 33 apartados 3 y 4).

El Tribunal Constitucional ha tenido ocasión de examinar los requisitos para que las leyes que establecen tratamientos de datos personales, en cuanto que restricciones al derecho fundamental a la protección de datos personales del interesado, puedan considerarse conformes a la Constitución. Así, dicha doctrina constitucional puede resumirse en la sentencia del Tribunal Constitucional (STC) 76/2019, de 22 de mayo. Esta sentencia contiene la doctrina relevante de este sobre el derecho fundamental a la protección de datos personales, y aborda tanto las características como el contenido que ha de tener la normativa que pretenda establecer una injerencia en ese derecho fundamental.

*(...) Por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (artículo 81.1 CE), ora limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). (...) Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, **«no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites»** (STC 292/2000, FJ 15).*

En consecuencia, y tal y como exige el Tribunal Constitucional, la ley que establezca unas determinadas injerencias en el derecho fundamental a la protección de datos personales de los interesados, como es, en el caso presente, la posibilidad de tratar datos personales de los interesados de

categorías especiales, como son datos relativos a su salud, requiere que esta en primer lugar, y para cada tratamiento de datos personales de categorías especiales que contemple:

a) especifique el interés público esencial que fundamenta la restricción del derecho fundamental (FJ 7 de la STC 76/2019).

b) en segundo lugar, la ley habrá de regular pormenorizadamente las injerencias al derecho fundamental estableciendo reglas claras sobre el alcance y contenido de los tratamientos de datos que autoriza. Es decir, habrá de establecer cuáles son los presupuestos y las condiciones del tratamiento de datos personales relativos a las categorías especiales de datos personales que habrán de ser objeto de tratamiento, mediante reglas claras y precisas (STC 76/2019, FJ 7 b)

c) Y por último, la propia ley habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El TC ha sido claro en cuanto a que *[l]a previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata en definitiva, de “garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”.*

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

*“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual*

*eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo, F. 5; 55/1996, de 28 de marzo, FF. 7, 8 y 9; 270/1996, de 16 de diciembre, F.4.e; 37/1998, de 17 de, F. 8; 186/2000, de 10 de julio, F. 6)."*

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, y el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

Pues bien, la STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, (no disponible aún a esta fecha en español), en su apartado 175, recuerda que:

*With regard to the justification for such interference, the requirement, established in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits that interference with those rights must **itself** define the scope of the limitation on the exercise of the right concerned (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).*

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

*Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser **establecida por ley** implica que la base legal que permita la injerencia en dichos derechos debe definir **ella misma** el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: *Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir **ella misma** el alcance de la limitación del ejercicio del derecho de que se trate [Dictamen 1/15 (Acuerdo*

PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos,

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

*176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer **reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas**, de modo que las personas cuyos datos se hayan transferido dispongan de **garantías suficientes** que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].*

La STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las categorías especiales de datos:

*68 (...) Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].*

Resulta pues tanto de la jurisprudencia del Tribunal Constitucional como del Tribunal de la UE que es la propia ley que establece el tratamiento de datos de categorías especiales (esto es, la injerencia en el derecho fundamental) la que ha de establecer, ella misma, (i) la finalidad de interés público esencial que lo justifica, (ii) reglas claras y precisas sobre el alcance y contenido de los tratamientos de datos que autoriza, y (iii) unas exigencias mínimas de modo que las personas cuyos datos se hayan transferido dispongan de garantías

suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso.

En este caso concreto, esta Agencia considera conveniente recordar expresamente las palabras del Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre, que declaró inconstitucionales determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

*De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. **Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse** y, además, es él quien debe hacerlo mediante reglas precisas que **hagan previsible al interesado la imposición de tal limitación y sus consecuencias**. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 C.E., esto es, establecer claramente el límite y su regulación.*

17. *En el caso presente, el empleo por la L.O.P.D. en su art. 24.1 de la expresión «funciones de control y verificación», abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, **al habilitar la L.O.P.D. a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo**. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 L.O.P.D., deja en la más absoluta **incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia** (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales*

*sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.*

Así pues, y a la vista de la jurisprudencia citada, se sugiere que el artículo 33 del anteproyecto (en esto similar al actual art. 33) no contenga tan sólo una remisión a una “circunstancias excepcionales” que se habrán de determinar “reglamentariamente”, sino que la sea la propia ley la que integre y contenga aquellas precisiones que permiten al ciudadano la previsibilidad acerca de cuándo su derecho fundamental a la protección de datos puede va a ser objeto de una injerencia (un tratamiento) o verse limitado.

Así, (1) dichas “circunstancias excepcionales” citadas en la ley se remiten en el RPBC simplemente a unos análisis de riesgo mencionados en el art. 65.1.e) RPBC que en realidad se refiere a su vez a los Informes de inteligencia financiera previstos en el art. 46 LPBC. Sería conveniente que dicha referencia constase en la ley.

(2) Igualmente la ley debe dejar claro que la finalidad del intercambio de información que para estas circunstancias excepcionales prevé la ley será exclusivamente la relativa a la prevención de las actividades de blanqueo de capitales o financiación del terrorismo. Cabe considerar que esta limitación de la finalidad ya se contiene en el apartado 6 de art. 33 del anteproyecto.

(3) En cuanto a quiénes pueden acceder o consultar los datos contenidos en los sistemas que fueren creados a dichos datos, se considera correcto igualmente la relación del apartado 6. Y por último,

(4) respecto de las garantías oportunas, el apartado 5 contiene la obligación de que los sujetos obligados realicen una EIPD de los tratamientos a fin de adaptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. 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. Esta Agencia sugiere que para completar estas garantías se recoja en la ley el requisito previsto tan sólo reglamentariamente (art. 61.1 RLPBC) según el cual, la autorización de intercambio de información (esto es, el tratamiento de datos personales) por la Comisión requiere el dictamen conforme de la AEPD.

De esta manera estos tratamientos se alejan de una determinación meramente reglamentaria para pasar hasta regulados en la propia ley que establece el tratamiento de los datos personales, estableciendo esta ley igualmente los requisitos y características del tratamiento, su finalidad, los destinatarios y finalmente las garantías.

En consecuencia, dicho apartado 33.1 del anteproyecto podría quedar redactado de la siguiente manera:

1. Sin perjuicio de lo establecido en el artículo 24.2, cuando concurren riesgos extraordinarios identificados mediante los análisis de riesgos en materia de blanqueo de capitales y financiación del terrorismo llevados a cabo por los sujetos obligados, o a través de la actividad de análisis e inteligencia financieros del Servicio Ejecutivo de la Comisión, o del análisis de riesgo nacional en materia de blanqueo de capitales y de la financiación del terrorismo, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, previo dictamen conforme de la Agencia Española de Protección de Datos, podrá acordar el intercambio de información referida a determinado tipo de operaciones distintas de las previstas en el artículo 18 y 19 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.*

En cuanto a la mención en el apartado 3 al art. 8.2 de la LOPDGDD (esto es, que la base jurídica dichos tratamientos será el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable), se considera correcta (véase art. 43 de la Directiva 2015/849, modificada por la Directiva 2018/843), pero de la misma manera que se ha hecho referencia respecto del artículo 32, 32 bis y 32 ter, se considera necesario hacer una referencia expresa, en este caso, al art. 6.1.e) RGPD junto a la mención de dicho artículo 8.2 LOPDGDD en dicho apartado 33.3 del anteproyecto, no siendo preciso, como igualmente se ha hecho mención al comentar los artículos anteriormente referidos, el consentimiento de los interesados para el tratamiento, sin que sea necesario indicarlo expresamente en la ley.

## VII

El anteproyecto modifica el art. 43 LPBC, relativo al Fichero de Titularidades Financieras, ya existente en la ley desde su promulgación. La modificación responde a la introducción en la Directiva 2015/849 del art. 32 bis por la Directiva 2018/843, relativo a la necesidad por los Estados miembros de mecanismos centralizados automatizados, como registros 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 y cajas de seguridad en una entidad de crédito. Por ello, se añaden a las entidades de crédito, ya contempladas en dicho art. 43, a las entidades de pago y de dinero electrónico. Pero, sin perjuicio de lo anterior, este art. 43 habrá de recoger las modificaciones llevadas a cabo en la normativa de protección de datos personales, por la entrada en vigor del

RGPD, que es posterior a la redacción inicial de la ley. Y además se han introducido otras modificaciones no derivadas de la Directiva 2018/843.

Así, el apartado 2 del art. 43 en la redacción del anteproyecto establece que del fichero denominado Fichero de Titularidades Financieras será responsable la Secretaría de Estado de Economía y Apoyo a la Empresa, y encargado el Servicio Ejecutivo de la Comisión. El RGPD permite que la determinación del responsable se haga mediante contrato u otro acto jurídico (art. 28.3 RGPD), pero, en ambos casos, deberá dicho contrato u otro acto jurídico -en este caso la propia ley- establecer las determinaciones que señala el apartado 3 de dicho art. 28 RGPD. En la MAIN no se especifica si es la ley el acto jurídico que ha de regir las relaciones entre responsable y encargado o existirá un contrato para ello. Si fuera la ley, esta habrá de contener, como se ha mencionado, todo lo relacionado en dicho apartado 3 del art. 28. Si fuera un contrato, sin perjuicio de que este sería el que ha de contener dichas circunstancias expresamente, sería conveniente que la ley especificara que las relaciones entre encargado y responsable se regirán por un contrato que contendrá todas las circunstancias previstas en el art. 28.3 RGPD.

Por otra parte, ya que se está haciendo referencia en dicho apartado 2 del art. 43 a la normativa de protección de datos, al igual que se ha reiterado ya en ocasiones anteriores en este informe, se considera necesario, y más correcto, que la referencia a la ley orgánica 3/2018 que se realiza en dicho apartado se haga bien a la normativa de protección de datos, en general, bien al RGPD.

El apartado 3 del art. 43 del anteproyecto incorpora una serie de modificaciones que no provienen de la transposición de la Directiva 2018/843. A ello parece referirse el párrafo segundo del epígrafe I de la Exposición de Motivos del anteproyecto cuando refiere que junto a las modificaciones necesarias para trasponer la norma europea *se proponen otras modificaciones y mejoras puntuales que responden a esos mismos objetivos generales de mejora de los instrumentos y mecanismos de prevención, pero que no vienen derivados de la necesaria transposición de normas europeas, sino que se recogen en los estándares internacionales aprobados por el Grupo de Acción Financiera (en adelante, GAFI) o son el resultado del diagnóstico que, sobre el funcionamiento del modelo legal implementado en España y sus posibilidades de mejora, realizan las autoridades encargadas de la aplicación de la legislación en materia de prevención del blanqueo de capitales y la financiación del terrorismo.*

En primer lugar se suprime del texto legal la necesidad de que las Fuerzas y Cuerpos de Seguridad del Estado (y por extensión las Policías Autonómicas) deban acceder a este Fichero de Titularidades Financieras (en adelante FTF) previa autorización judicial o del Ministerio Fiscal. Esta Agencia ya tuvo oportunidad de **informar negativamente** a esta modificación en su Informe 41/2018, porque suponía la desaparición de garantías previas que

justificaban el acceso de las FCSE a dicha información, lo que ahora se reitera expresamente. Dicho **Informe 41/2018** decía a este respecto lo siguiente:

*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. (...)*

*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.***

*(...), 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 -prosigue la sentencia- 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 sean 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, (...)*

**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, (...) 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.***

Existen por otra parte otras modificaciones respecto del texto del art. 43 de la LPBC. Así, si en el texto de la LPBC el art. 43 se refería a la posibilidad de acceso al FTF para investigar delitos relacionados con el blanqueo de capitales o la financiación del terrorismo a los jueces de instrucción. El nuevo texto se refiere simplemente a “los órganos jurisdiccionales”, si bien cabe considerar que dicha modificación es conforme a derecho por cuanto no sólo los “jueces de instrucción” podrían teóricamente llevar a cabo la instrucción de estos delitos (piénsese por ejemplo en los juzgados centrales de instrucción o en aquellos casos en que la instrucción la realiza un miembro de un tribunal superior por estar una persona aforada, etc.). Pero ello habrá de interpretarse de modo que se refiera únicamente a los jueces entre cuyas competencias se incluya la de “investigación de los delitos”, y no cualquier otro órgano jurisdiccional.

Igualmente, el nuevo texto recoge nuevos supuestos de acceso a los datos del Fichero de titularidades Financieras, respecto de las cuales ya se pronunció esta AEPD en el reiterado Informe 41/2018.

*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**, (...), 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 último, hay que mencionar que el actual apartado 4 del art. 43 LPBC -que no ha sido modificado- se ve integrado en el anteproyecto como último párrafo del apartado 3, en lo que más bien parece un error de tipografía, porque no parece haber razón especial para ello. Se considera más conveniente que se mantenga como apartado 4 del art. 43. Y sin perjuicio de ello hay que añadir que dicho apartado no cumpliría los requisitos previstos en la jurisprudencia del TJUE de requerir como garantía para el acceso a los datos del Fichero de Titularidades Financieras, como se ha expuesto, un control judicial o del ministerio fiscal previo.

## VIII

El art. 47, apartado 4, del anteproyecto, tiene la siguiente redacción:

*4. Los sujetos obligados, sus empleados, directivos y agentes, prestarán la máxima colaboración al personal del Servicio Ejecutivo de la Comisión y, en el ámbito de sus competencias, al personal del Banco de España, de la Comisión Nacional del Mercado de Valores y de la Dirección*

*General de Seguros y Fondos de Pensiones, facilitando sin restricción alguna cuanta información o documentación se les requiera, incluidos libros, asientos contables, registros, programas informáticos, archivos en soporte magnético, comunicaciones internas, actas, declaraciones oficiales, y cualesquiera otros relacionados con las materias sujetas a inspección.*

*A efectos de esta ley, las entidades financieras notificarán a sus supervisores prudenciales, con carácter previo, su intención de contratar con proveedores de servicios de almacenamiento o computación de información relacionada con las obligaciones en materia de prevención del blanqueo de capitales y de la financiación del terrorismo. En todo caso, deberá garantizarse el cumplimiento de sus obligaciones en materia de prevención del blanqueo de capitales y la financiación del terrorismo y el acceso por las autoridades a toda la información alojada en estos servidores sin dilación. Los servicios de almacenamiento y tratamiento de datos serán prestados dentro del Espacio Económico Europeo o, en su caso, de un tercer país que según la Comisión Europea ofrezca las garantías necesarias que aseguren un nivel adecuado de protección equivalente al ofrecido en la Unión Europea, y siempre que se cumplan las disposiciones relativas a la transferencia de datos personales a terceros países u organizaciones internacionales establecidas por el Reglamento (UE) 2016/679 del Parlamento 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 la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

Nos encontramos por tanto ante una nueva redacción de este apartado respecto de la establecida en la LPBC que refuerza la obligación que ya existía en la redacción original del precepto de facilitar sin restricción alguna toda información respecto de registros, programas informáticos, archivos en soporte magnético etc. relacionadas con la materia supervisada.

Se añade ahora, en primer lugar, una obligación para las entidades financieras, en tanto que sujetos obligados, de notificar a sus supervisores prudenciales, con carácter previo, su intención de contratar con proveedores de servicios de almacenamiento o computación de información relacionada con las obligaciones en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, así como, a continuación una obligación de garantizar el cumplimiento de sus obligaciones en materia de prevención del blanqueo de capitales y la financiación del terrorismo y el acceso por las autoridades a toda la información alojada en estos servidores sin dilación. Desde el punto de vista de la normativa de protección de datos personales no se formula ninguna objeción a estas obligaciones, sin que tampoco venga impuesta esa obligación por dicha normativa.

A continuación se obliga a las entidades financieras a que (1) los servicios de almacenamiento y tratamiento de datos (sic) habrán de ser prestados (2) dentro del Espacio Económico Europeo o, en su caso, (3) de un tercer país que según la Comisión Europea ofrezca las garantías necesarias que aseguren un nivel adecuado de protección equivalente al ofrecido en la Unión Europea, (4) y (sic) siempre que se cumplan las disposiciones relativas a la transferencia de datos personales a terceros países u organizaciones internacionales establecidas por el RGPD y la LOPDGDD.

El RGPD define (art. 4.2) «tratamiento» como **cualquier** operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, **como** la recogida, registro, organización, estructuración, **conservación**, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. Nos encontramos por tanto ante una definición amplia de tratamiento, y no exhaustiva.

El texto del anteproyecto se refiere a los “servicios” de “almacenamiento” y “tratamientos”. La expresión no es muy afortunada, por cuanto los “servicios de tratamientos” no se sabe muy bien a qué se refiere. En primer lugar, al referirse a “servicios de almacenamiento” parece querer reflejar aquel acuerdo por el cual la entidad financiera confía a otra empresa sus datos para que estos residan, o se alojen, en espacios físicos dentro de un ordenador (servidor) pertenecientes a esa otra empresa. Hoy día suele ser conocido como “hosting”. Como tal, ese servicio de conservación es en sí mismo un tratamiento de datos, de acuerdo con el concepto que maneja el RGPD. Por otro lado, el anteproyecto menciona además lo que denomina “servicios de tratamiento de datos”, que por su propia extensión, vista la definición del RGPD de tratamientos de datos (art. 4.1), hace referencia a todo tipo de tratamientos.

En realidad lo que parece querer prevenir dicho precepto es que la entidad financiera, en tanto que sujeto obligado, no transfiera los datos necesarios para el control de la materia relativa al blanqueo de capitales y financiación del terrorismo (y obsérvese que aquí puede haber tanto datos personales como no personales) a países o lugares que no son considerados por la normativa de protección de datos personales como equivalentes en protección al nivel existente en la UE (extensible a los países del EEE).

La transferencia de datos a terceros países u organizaciones internacionales (fuera de la UE y del EEE) se regula en el Capítulo V del RGPD. El principio general se encuentra en su art. 44, según el cual sólo podrán realizarse transferencias de datos personales (únicos a los que se refiere el RGPD) si el responsable y el encargado del tratamiento cumplen las condiciones establecidas en dicho capítulo. Ahora bien, el RGPD no impone en modo alguna a los responsables del tratamiento una obligación positiva de que sus tratamientos hayan de realizarse dentro del EEE. Ello es ajeno a la

normativa de protección de datos; estas normas simplemente establecen los requisitos para que los tratamientos de datos tengan las mismas garantías para los interesados tanto si se ejecutan en el EEE como fuera de él. Puede entenderse que el RGPD no permite una transferencia de datos a terceros países si no se cumplen los requisitos que el RGPD prevé (que exista una Decisión de adecuación de la Comisión -art. 45 RGPD-; que existan garantías adecuadas conforme al art. 46 RGPD; o haya normas corporativas vinculantes conforme al art. 47; o se den las circunstancias específicas del art. 49 RGPD. Pero cuando dichas circunstancias existen, ni la impone ni la prohíbe. Sentado lo anterior, el que el anteproyecto imponga que determinados tratamientos (al menos, el almacenamiento (o “hosting”) -y quizás también el resto de los posibles tratamientos de datos personales a que parece referirse la expresión “servicios de tratamiento de datos” del art. 43 del anteproyecto-) hayan de ser prestados dentro del EEE no se considera contrario a la normativa de protección de datos personales. Su examen conforme a otros sectores del ordenamiento -pactos comerciales con terceros países, por ejemplo- queda fuera de nuestro informe. Por ello, y por extensión, cuando el anteproyecto regula que dichos servicios de almacenamiento (y otros tratamientos) sólo pueden prestarse en países del EEE o en un tercer país que según la Comisión Europea ofrezca las garantías necesarias que aseguren un nivel adecuado de protección equivalente al ofrecido en la Unión Europea, no sería contrario a la normativa de protección de datos personales, pues conforme al art. 6.3 RGPD, cuando la base jurídica del tratamiento sea la establecida en el art. 6.1.c) o 6.1.e), dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; (...) así como las operaciones y los procedimientos del tratamiento (...).

Obsérvese por otra parte que sería redundante, una vez que se ha establecido por el anteproyecto que sólo será posible -fuera de la EEE- el almacenamiento (y otros tratamientos) en aquellos países para los que la Comisión haya dictado una Decisión de Adecuación, el que se diga que “*y siempre que se cumplan las disposiciones relativas a la transferencia de datos personales a terceros países u organizaciones internacionales establecidas por el Reglamento (UE) 2016/679 del Parlamento 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 la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*”, pues la existencia de una Decisión de Adecuación de la Comisión ya determina que las transferencias de datos a los lugares de almacenamiento de datos cumplen dichos estándares. Salvo que con ello se pretenda por el redactor del anteproyecto diferenciar entre “almacenamiento de datos”, sean o no personales, que siempre habrán de almacenarse en países para los que exista una Decisión de Adecuación, y el “tratamiento de datos personales” en que consiste la transferencia de datos a dichos países, que habrán de cumplir en todo caso con la normativa reguladora de protección de

datos personales. De todos modos, ese precepto no acaba de quedar claro para esta AEPD, y la MAIN no proporciona tampoco explicación sobre la concreta redacción del precepto en este punto.

Esta AEPD recuerda que una normativa análoga, y con la misma finalidad de protección de datos personales -en la que se requiere a los responsables una determinada ubicación de los recursos técnicos necesarios para la prestación de determinados servicios en casos considerados de interés público por el legislador, o respecto de la notificación de sus proyectos en materia de almacenamiento de datos personales etc.- se ha aprobado por **Real Decreto-ley 14/2019, de 31 de octubre**, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

En concreto, en su artículo 5. Cinco se da nueva redacción al apartado 2 del artículo 122 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), que establece (en la parte aplicable al caso):

*Sin perjuicio de lo establecido en el artículo 28.2 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 la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, adicionalmente en el pliego se hará constar:*

- a) La finalidad para la cual se cederán dichos datos.*
- b) La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de lo establecido en el último párrafo del apartado 1 del artículo 202.*
- c) La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto **dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.***
- d) La obligación de **comunicar cualquier cambio que se produzca**, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior.*
- e) La obligación de los licitadores de indicar en su oferta, **si tienen previsto subcontratar los servidores o los servicios asociados** a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.*

*En los pliegos correspondientes a los contratos a que se refiere el párrafo anterior las obligaciones recogidas en las letras a) a e)*

*anteriores en todo caso deberán ser calificadas como esenciales a los efectos de lo previsto en la letra f) del apartado 1 del artículo 211.»*

Pero, **sobre todo**, el art. 3 de dicho Real Decreto Ley 14/2019 ya ha establecido la obligación de ubicar, en determinados casos considerados de interés público, los recursos técnicos necesarios en la UE, o incluso concretamente en España. Así, el art. 3. Uno, y 3. Dos dan nueva redacción a los artículos 9.3 y 10.3 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, de la siguiente manera:

*9.3. En relación con los **sistemas de identificación** previstos en la letra c) del apartado anterior, se establece la **obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea**, y en caso de tratarse de **categorías especiales de datos** a los que se refiere el artículo 9 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, **en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.***

*Los **datos** a que se refiere el párrafo anterior **no podrán ser objeto de transferencia** a un tercer país u organización internacional, con **excepción** de los que hayan sido objeto de una **decisión de adecuación** de la Comisión Europea o cuando así lo exija el cumplimiento de las **obligaciones internacionales** asumidas por el Reino de España.*

El artículo 10.3, referido esta vez a los sistemas de firma (frente a los sistemas de identificación regulados en el art. 9.3 mencionado) tiene similar redacción:

*10.3. En relación con los **sistemas de firma** previstos en la letra c) del apartado anterior, se establece la **obligatoriedad** de que los **recursos técnicos necesarios** para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren **situados en territorio de la Unión Europea**, y en caso de tratarse de **categorías especiales de datos** a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, **en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.***

*Los datos a que se refiere el párrafo anterior **no podrán ser objeto de transferencia a un tercer país u organización internacional**, con excepción de los que hayan sido objeto de una **decisión de adecuación** de la Comisión Europea o cuando así lo exija el cumplimiento de las **obligaciones internacionales** asumidas por el Reino de España.*

El redactor del anteproyecto podría utilizar estas mismas expresiones y principios, sobre todo lo relativo a la ubicación de “*los recursos técnicos necesarios*” para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas, pues parece ser el objetivo que pretende conseguir con el precepto legal de la LPBC ahora comentado en este epígrafe.

## IX

El anteproyecto da una nueva redacción a las letras a), c), d) y f) del apartado 2 del art. 49 de la LPBC. Este precepto trata de las excepciones al carácter reservado de cualesquiera datos e informaciones que obren en poder de la Comisión de Prevención del blanqueo de capitales e infracciones monetarias o de cualquiera de sus órganos.

Llama la atención en primer lugar la disparidad de criterios en cuanto a la solicitud de las autoridades judiciales del orden penal o del ministerio fiscal para requerir información de la que principio tiene carácter reservado, puesto que en estos casos el apartado d) requiere que la autoridad requirente, esto es, el juez o el ministerio fiscal, invoque “expresamente” un precepto legal que habilite a la petición de información. Mientras que respecto de las Fuerzas y Cuerpos de Seguridad del Estado no se establece la necesidad de invocar “expresamente” precepto alguno que le habilite a solicitar dicha información, sino que en este último caso bastará con una solicitud motivada.

Pero además en segundo lugar, y como ya ha tenido ocasión de mencionar esta Agencia respecto del art. 43.3, no se ha contemplado la necesidad de que las Fuerzas y Cuerpos de Seguridad del Estado cuenten previamente con la autorización judicial o del ministerio fiscal para solicitar datos en principio reservados. Obsérvese además que en la posibilidad para las FCSE de solicitar del servicio ejecutivo de la comisión la aportación de información prevista en este precepto depende de que se trate de una investigación por delito grave. Ello abunda aún más en la necesidad de que, como **garantía previa** a los tratamientos de datos personales que puedan resultar de dicha información, **las FCSE obtengan con carácter previo la mencionada autorización judicial o del Ministerio Fiscal**. Se reitera aquí la totalidad de los argumentos expuestos anteriormente respecto del art. 43.3 (véase epígrafe VII de este Informe, y referencia en él al Informe 41/2018 de esta AEPD).

## X

El artículo Único, apartados cuarenta y uno a cuarenta y cinco, del anteproyecto modifica los artículos 56 y 57 de la LPBC para añadir algunas precisiones sobre las sanciones a imponer. En concreto, en los arts. 57.1 y 57.2 se introduce un último párrafo para poder tener en cuenta la posibilidad de que *Cuando se considere que la publicación de la identidad de las personas responsables o los datos personales de dichas personas resulte desproporcionada o ponga en peligro la estabilidad de los mercados financieros o una investigación en curso, se optará por la amonestación privada.* Esta Agencia se muestra de acuerdo con la propuesta.

No obstante, se sugiere que por el redactor del anteproyecto se considere si es conveniente modificar el apartado 5 del art. 57 para añadir como causa de no publicación en los casos ahí previstos, cuando el sancionado sea una persona física, el que la publicación de sus datos personales pueda ser desproporcionada. Es de resaltar que el art. 60.1 de la Directiva 2015/843 no lo impide ni siquiera para el caso de las infracciones muy graves.

De hecho, esta Agencia considera que puede haber una discrepancia entre la legislación española y la Directiva 2015/843, por cuanto el art. 60 de esta establece efectivamente que *toda decisión firme que imponga una sanción o medida administrativa por incumplimiento de las disposiciones nacionales de transposición de la presente Directiva sea publicada por las autoridades competentes.* Ahora bien, igualmente el apartado b) de dicho art. 60 establece sin distinción **para todo tipo de sanciones** que *cuando la autoridad competente considera (sic) que la publicación de la identidad de las personas responsables a que se refiere el párrafo primero o los datos personales de dichas personas resulta desproporcionada, tras una evaluación en cada caso de la proporcionalidad de dicha publicación, (...) dicha autoridad podrá: b) publicar la decisión de imponer una sanción o medida administrativa de manera anónima de conformidad con la legislación nacional, en caso de que dicha publicación anónima garantice una protección efectiva de los datos personales de que se trate; en caso de que se decida publicar una sanción o medida administrativa de manera anónima, la publicación de los datos pertinentes podrá aplazarse por un período razonable de tiempo si se prevé que en el transcurso de ese período dejarán de existir las razones que justifiquen una publicación con protección del anonimato;* Igualmente el apartado c) de dicho art. 60.1 de la Directiva prevé la posibilidad de que no se publique si la publicación es una medida desproporcionada *frente a medidas que se consideran de menor importancia.*

El redactor del anteproyecto no ha considerado la posibilidad de tener en cuenta la posibilidad de no publicar los datos personales de las personas físicas prevista en la norma comunitaria, para las sanciones muy graves del art. 56 ni para las graves en el art. 57.3 ni en el art. 57.3.bis, ni en el art. 57.5, por lo que en estos casos (en tanto sean trasposición de la Directiva) la autoridad

competente también debería poder tener en cuenta la posibilidad de que la publicación de los datos personales del infractor persona física fuese desproporcionada *tras una evaluación en cada caso de la proporcionalidad de dicha publicación* a los efectos de no publicar dicha decisión.

## XI

El artículo 65, sobre Protección de las personas, entronca con el art. 63, relativo a la comunicación de las infracciones por empleados, directivos y agentes de los sujetos obligados que conozcan hechos o situaciones que puedan ser constitutivos de infracciones. El anteproyecto añade un apartado 5 al art. 65 LPBC con la siguiente redacción:

*“5. Las personas expuestas a amenazas, acciones hostiles o medidas laborales adversas por comunicar por vía interna o al Servicio Ejecutivo de la Comisión comunicaciones sobre actividades relacionadas con el blanqueo de capitales o la financiación del terrorismo podrán presentar una **reclamación** ante el Servicio Ejecutivo de la Comisión. Mediante orden del Ministerio de Asuntos Económicos y Transformación Digital se aprobará el modelo de comunicación y el sistema de recepción de comunicaciones para garantizar su confidencialidad y seguridad.”*

Este artículo es la trasposición del art. 38 de la Directiva 2015/849, al que ha dado nueva redacción la Directiva 2018/843. La redacción actual de dicho precepto es:

*1. Los Estados miembros **garantizarán** que las personas, incluidos los empleados y representantes de las entidades obligadas, que comuniquen sospechas de blanqueo de capitales o de financiación del terrorismo, ya sea por vía interna o a la UIF, estén **protegidas legalmente** de toda amenaza, medida de represalia o acción hostil, y en particular de toda medida laboral adversa o discriminatoria.*

*2. Los Estados miembros **garantizarán** que las personas expuestas a amenazas, medidas de represalia o acciones hostiles o medidas laborales adversas o discriminatorias por comunicar por vía interna o a la UIF sospechas de blanqueo de capitales o de financiación del terrorismo tengan derecho a **presentar de forma segura una reclamación ante las autoridades competentes respectivas**. Sin perjuicio de la confidencialidad de la información recopilada por la UIF, los Estados miembros garantizarán asimismo que dichas personas tengan derecho a una **tutela judicial efectiva** a fin de preservar sus derechos en virtud del presente apartado.*

Siendo su redacción originaria la siguiente:

*Los Estados miembros **velarán** por que las personas, incluidos los empleados y representantes de las entidades obligadas, que comuniquen sus sospechas de blanqueo de capitales o de financiación del terrorismo, ya sea por vía interna o a la UIF, estén **protegidas** de toda amenaza o acción hostil, y en particular de toda medida laboral adversa o discriminatoria.*

Como puede verse, entre la primera redacción de la Directiva y la actual, (1) en primer lugar se establece que el Estado miembro ha de “garantizar”, no simplemente “velar” por la protección de las comunicantes -que en última instancia redundaría en beneficio del Estado miembro, pues a mayor seguridad de los comunicantes más comunicaciones habrá-. En segundo lugar (2) se añade que dicha garantía de protección ha de venir establecida “legalmente”. Y (3) se recoge la necesidad de que los Estados miembros acojan en la ley la posibilidad de presentar una reclamación ante la autoridad competente. La modificación de la LPBC tan sólo atiende a esta última circunstancia, como expresamente alude la MAIN al referirse al art. 65.5, sin que exista mención alguna a las otras dos modificaciones que entraña la nueva redacción de la Directiva.

Dado que la protección de los comunicantes redundaría en última instancia no sólo en el sistema de prevención del blanqueo de capitales, sino también en ellos mismos, y por tanto en la protección de los datos personales de los comunicantes esta Agencia considera conveniente sugerir al redactor del anteproyecto la modificación de este artículo 65 LPBC para incluir “garantías efectivas” para el comunicante para prevenir represalias en el ámbito laboral. Así, si bien el art. 65.1 LPBC ya recoge que las comunicaciones realizadas al amparo del artículo 63: a) no constituirán violación o incumplimiento de las restricciones sobre divulgación de información; b) no constituirán infracción de ningún tipo en el ámbito de la normativa laboral por parte de la persona comunicante, ni de ella podrá derivar trato injusto o discriminatorio por parte del empleador; c) no generarán ningún derecho de compensación o indemnización a favor de la empresa, se sugiere que se contemple como **garantía efectiva** la medida de considerar un posible despido o medida disciplinaria por dichas razones como despido nulo, -con las consecuencias que ello conlleva- introduciéndolo como una nueva letra d) en el art. 55.5 del Estatuto de los Trabajadores; o bien, en caso de que no se considere ello oportuno y se considere el despido como improcedente, otorgar a la persona trabajadora (en vez de al empresario) la facultad de optar entre la readmisión del trabajador o el abono de una indemnización prevista en el art. 56.1 del citado Estatuto de los Trabajadores. Estas medidas, si se adoptan, pueden suponer la diferencia entre la redacción original, según la cual al Estado miembro le bastaba con “velar” para que no hubiera represalias laborales, con la obligación actual impuesta por la Directiva de que el Estado habrá de “garantizar” de manera efectiva que no se produzcan dichas represalias.

El anteproyecto añade una nueva Disposición Adicional Tercera (DA 3ª) a la LPBC para recoger la regulación sobre Registro de Titularidades Reales, y una Disposición Adicional Cuarta (DA 4ª) para regular el acceso a dicho Registro, cuyo objeto es la trasposición de los artículos 30 y 31 de la Directiva 2015/843, en su parte correspondiente a este registro único centralizado, modificados por la Directiva 2018/843. El redactor del anteproyecto ha considerado conveniente que las obligaciones de creación de un registro central único que recoja las titularidades reales de las personas jurídicas (art. 30.3 de la Directiva 2015/849) y de los fideicomisos tipo “trust” (art. 31.3 bis de dicha Directiva) se unan en el mismo registro central. Esta opción legislativa es aceptable, pero sin embargo existen diferencias en la regulación en ambos casos, que hace que haya que establecer diferentes reglas, según el caso, sobre todo en cuestión de acceso, que, en opinión de esta Agencia, no han sido satisfactoriamente resueltas.

Desde la perspectiva de la protección de datos personales, el Considerando 38 de la Directiva 2018/843 (Quinta Directiva) establece:

***El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo se aplica al tratamiento de los datos personales con arreglo a la presente Directiva. Como consecuencia de ello, las personas físicas cuyos datos personales se conserven en los registros nacionales en calidad de titulares reales deben ser informadas al respecto. Además, solo deben facilitarse los datos personales que estén actualizados y correspondan a los titulares reales efectivos, y se debe informar a los beneficiarios de sus derechos con arreglo al vigente marco de protección de datos de la Unión, según establecen el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, así como de los procedimientos aplicables al ejercicio de dichos derechos. Además, para evitar el uso indebido de la información contenida en los registros y para equilibrar los derechos de los titulares reales, los Estados miembros pueden considerar la posibilidad de facilitar al titular real los datos relativos a la persona que solicite la información, junto con la base jurídica de su solicitud.***

Que se completa con el Considerando 40: *La presente Directiva se entiende sin perjuicio de la protección de los datos personales tratados por las autoridades competentes de conformidad con la Directiva (UE) 2016/680.*

- En primer lugar, la DA 3ª encarga la “gestión” del Registro central único al Ministerio de Justicia, considerándolo así responsable del tratamiento de los datos personales, y sobre quien recaen por lo tanto las obligaciones que el RGPD establece, entre ellos la llevanza del correspondiente registro de tratamientos, información a los interesados, acceso, rectificación etc. El precepto no menciona esta circunstancia, por lo que debería hacerlo para la completa regulación del tratamiento de los datos personales.

- Del mismo modo, esta Agencia, a la vista de la regulación de la LPBC, que establece limitaciones al derecho fundamental de protección de datos personales de los interesados en diversos casos, pero que no se aplican (véase el considerando 38 de la Directiva recién mencionado) a los titulares reales cuyos datos constan en el Registro, considera necesario, para la efectividad de sus derechos personales, que conste expresamente que las personas físicas cuyos datos personales se conserven en el registro en calidad de titulares reales deben ser informadas al respecto de conformidad con la normativa vigente en materia de protección de datos personales.

- En el apartado 5 de la DA 3ª se establece que las fundaciones, asociaciones y en general todas las personas jurídicas deberán actualizar los datos anualmente. Esta posibilidad de actualización de los datos habrá de ser precisada como “cuando menos anualmente” ya que no sólo por el principio de exactitud del art. 5.1.d) RGPD, sino directamente por la propia Directiva 2015/849, art. 31.5 dice que *Los Estados miembros exigirán que la información conservada en el registro central a que se refiere el apartado 3 bis sea adecuada, exacta y actualizada, y establecerán mecanismos para tal fin*. Para ello establece mecanismos para los sujetos obligados, y en su caso, para las propias autoridades competentes. No se considera que una actualización “anual” cumpla el principio de exactitud, sino que deberán preverse los mecanismos necesarios para que la información esté actualizada **en todo momento**. La actualización “cuando menos anual” puede ser un mecanismo de actualización, pero desde luego no cumple, por sí solo, el principio de exactitud.

- Cabe mencionar que el principio de minimización de datos (art. 5.1c) RGPD) no permitiría hacer constar en este Registro *datos personales* cuya constancia en el mismo no fuere obligatoria por la norma que establece el tratamiento de datos personales.

- Ya en al DA 4ª, su apartado primero regula el acceso “sin restricción” a determinadas autoridades a dicho registro de titularidades reales. El apartado 6 del art. 31 de la Directiva 2015/849 dice así:

*6. Los Estados miembros garantizarán que las autoridades competentes y las UIF tengan acceso oportuno e ilimitado a toda la información conservada en el registro a que se refiere el apartado 3, sin alertar a la entidad de que se trate. Los Estados miembros permitirán también el acceso oportuno a las entidades obligadas que adopten medidas de diligencia debida con respecto al cliente de conformidad con el capítulo II.*

***Las autoridades competentes a las que se concederá acceso al registro central a tenor del apartado 3 serán aquellas con responsabilidades específicas en la lucha contra el blanqueo de capitales o la financiación del terrorismo, así como las autoridades***

*tributarias, los supervisores de las entidades obligadas y las autoridades cuya función sea la investigación o el enjuiciamiento del blanqueo de capitales, los delitos subyacentes conexos y la financiación del terrorismo, el rastreo y la incautación o embargo y el decomiso de activos de origen delictivo.*

El texto del apartado 1 de la DA 4ª dice:

*1. Corresponderá al Ministerio de Justicia garantizar y controlar el acceso a la información contenida en el Registro de Titularidades Reales en las condiciones establecidas en la ley y las que reglamentariamente determine. Esta información será accesible, de forma gratuita y sin restricción, a las autoridades con competencias en la prevención y represión de los delitos de financiación del terrorismo, blanqueo de capitales y sus delitos precedentes, **con inclusión de** la fiscalía, los órganos de poder judicial, los Cuerpos y Fuerzas de Seguridad, Centro Nacional de Inteligencia, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y sus órganos de apoyo, los órganos supervisores en caso de convenio, la Oficina de Recuperación y Gestión de Activos, la Agencia Estatal de Administración Tributaria y aquellas autoridades que reglamentariamente se determinen. Todas estas autoridades, así como los notarios y registradores, podrán acceder no sólo al dato vigente sobre la titularidad real de la persona o entidad, sino también a los datos históricos que hayan quedado registrados, así como a los que, en caso de discrepancia, no hayan sido publicados en el Registro.*

En relación con este listado de posibles accesos hay que reiterar una vez más en este Informe que el acceso de las Fuerzas y Cuerpos de Seguridad del estado y del Centro Nacional de Inteligencia, serán admisibles, como se ha expuesto anteriormente en este informe, **con la necesaria autorización previa del ministerio fiscal o de la autoridad judicial**. Por otro lado, el texto del anteproyecto parece establecer una lista abierta de entidades que pueden tener acceso este registro de titularidades reales, dado que la utilización de la expresión “*con inclusión de*” deja abierta, o parece dejar la abierta, a que las autoridades que pueda tener acceso a este registro de titularidades reales sean más de las que nominativa mente se citan en el precepto. Esta Agencia considera inadecuada dicha redacción, por cuanto todo tratamiento de datos personales supone una injerencia en el derecho fundamental a la protección de datos personales de los interesados, por lo que dicha redacción habría de eliminar dicha expresión “con inclusión de” y limitarla a las autoridades citadas, y siempre con el añadido de la ya mencionada necesidad de autorización judicial en los supuestos que se han reiterado.

- El apartado 4 de la DA 4ª (su primera frase) establece:

4. *El acceso a la información disponible en el Registro requerirá la previa identificación del solicitante, y acreditación de la condición en la que se solicita el acceso, y el interés en su conocimiento, en los términos que se establezcan reglamentariamente. (...)*

Como se ha mencionado anteriormente, existen diferencias en la regulación de la Directiva según que la titularidad real sea de sociedades o de fideicomisos tipo trust. Así, dado que la regulación de la DA 4ª engloba el acceso a las titularidades reales tanto (i) para sociedades o entidades jurídicas como para (ii) fideicomisos tipo trust, hay que recalcar, como se ha hecho al principio de este epígrafe, que la regulación de dicho acceso en la Directiva 2015/849 (modificada por la Directiva 2018/843) es diferente en lo que se refiere, sobre todo, al acceso del público para una y otras clase de información. Así, el art. 30.5 de la Directiva, respecto de la información sobre la titularidad real de sociedades establece:

5. *Los Estados miembros garantizarán que la información sobre la titularidad real esté en todos los casos a disposición de:*

- a) las autoridades competentes y las UIF, sin restricción alguna;*
- b) las entidades obligadas, en el marco de la diligencia debida con respecto al cliente de conformidad con el capítulo II;*
- c) cualquier miembro del público en general.***

*(...)*

Pero el art. 31.4, sobre el acceso a la titularidad real de los fideicomisos tipo trust, establece:

4. *Los Estados miembros garantizarán que la información sobre la titularidad real de un fideicomiso (del tipo «trust») o instrumento jurídico análogo se ponga en todos los casos a disposición de:*

- a) las autoridades competentes y las UIF, sin restricción alguna;*
- b) las entidades obligadas, en el marco de la aplicación de las medidas de diligencia debida de conformidad con el capítulo II;*
- c) toda persona física o jurídica que pueda demostrar un interés legítimo;***
- d) toda persona física o jurídica que presente una solicitud por escrito relativa a un fideicomiso (del tipo «trust») o instrumento jurídico análogo que sea titular o dueño de una participación de control en una sociedad u otra entidad jurídica distinta de las mencionadas en el artículo 30, apartado 1, a través de la propiedad directa o indirecta, incluidas las carteras de acciones al portador, o a través del control por otros medios.*

Como se observa, la necesidad de acreditar un interés legítimo (que es básicamente un nuevo dato personal del solicitante) tan sólo lo requiere la Directiva para la solicitud de información real sobre los fideicomisos de tipo trust, pero no para una solicitud de información sobre la titularidad real respecto de una sociedad o entidad sin personalidad jurídica prevista en el artículo 30 de

la Directiva. En consecuencia, la expresión que consta en el apartado 4 de la Disposición Adicional cuarta del anteproyecto: “(...) y *acreditación de la condición en la que se solicita el acceso, y el interés en su conocimiento (...)*”, en tanto que supone la revelación por el interesado de unos datos personales no requeridos por la Directiva respecto de las solicitudes de acceso al registro de titularidades reales de personas jurídicas (regulada en el art. 30 de la Directiva) se considera **contrario al principio de minimización de datos** previstos en el **art. 5.1.c del RGPD**. Sí sería aceptable respecto de las solicitudes que se realicen de acceso a las titularidades reales de fideicomisos tipo “trust”, por cuanto la Directiva establece en su art. 31, como hemos visto, una más estricta legitimación para acceder a dichos datos.

En cuanto a la expresión “en los términos previstos reglamentariamente”, baste recordar lo ya expuesto de manera extensa en este informe: *cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir **ella misma** el alcance de la limitación del ejercicio del derecho de que se trate.*

O como estableció el Tribunal Constitucional en la STC 292/2000, ya citada:

*Al respecto, ya hemos dicho [STC 127/1994, F.J. 5, con remisión a la STC 83/1984, F.J. 4, y 99/1987, F.J. 3 a)] que incluso en los ámbitos reservados por la Constitución a la regulación por Ley no es imposible una intervención auxiliar o complementaria del Reglamento, pero siempre que estas remisiones restrinjan efectivamente **el ejercicio de esa potestad reglamentaria a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley**. De tal modo que esa remisión no conlleve una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular de la potestad reglamentaria, sin fijar ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino «deferir a la normación del Gobierno el objeto mismo reservado» (STC 227/1993, de 9 de julio, F.J. 4, recogiendo la expresión de la STC 77/1985, de 27 de junio, F.J. 14).*

Por ello, si la remisión al reglamento que realiza dicho precepto va más allá del mero motivo técnico, el legislador estaría haciendo dejación de su obligación de regular en la propia ley que establece el tratamiento de datos personales los límites al derecho fundamental a la protección de datos personales, y dicha norma (la ley, y por supuesto, el reglamento) sería inconstitucional por vulnerar dicho derecho fundamental.

- La segunda frase del apartado 4 de la Disposición Adicional Cuarta dispone:

*Asimismo, será obligatorio el previo pago de una tasa que cubra el coste del Registro y, en su caso, el de las fuentes de los datos incluidos en el mismo, por el sistema que se establezca reglamentariamente. No será exigible el pago de tasas en los accesos realizados por autoridades públicas.*

Los artículos 30.5 bis y 31.4 bis de la Directiva establecen que el pago de dicha tasa *no será superior a los costes administrativos de la puesta a disposición de la información, incluidos los costes de mantenimiento y desarrollo del registro*

No existe una explicación en la MAIN para la distinta redacción entre la normativa comunitaria y la nacional, y por qué unos conceptos son diferentes de otros, por lo que si el importe de la tasa aplicando la normativa nacional resultase superior a la que se obtendría aplicando los conceptos que establece la Directiva, la ley sería contraria a esta última.

- La redacción del apartado 5 de la DA 4ª no es del todo acorde con los arts. 30.9 y 31.7 bis de la Directiva 2015/849. La Directiva establece que podrá exceptuarse el derecho de acceder al registro de titularidades reales en aquellos casos que puedan *exponer al titular real a un riesgo desproporcionado, un riesgo de fraude, secuestro, extorsión, acoso, violencia o intimidación, o si el titular real es un menor o tiene otro tipo de incapacidad jurídica*. Es decir, la Directiva exceptúa dicho acceso tanto (i) en caso de “riesgo desproporcionado” como (ii) en caso de “riesgo de fraude etc.”. El “riesgo de fraude, secuestro, extorsión etc.” no necesita ser “desproporcionado”, basta con su mera existencia apreciada por el encargado del Registro. El “riesgo desproporcionado” es una causa diferente de denegación del acceso al registro del “riesgo de fraude, extorsión etc.”, por lo que habrá que modificar la redacción de la DA 4ª para acomodarla a la Directiva y no dejar fuera dicha limitación de acceso a los datos personales que constan en el Registro.

### XIII

Como hemos visto, el RGPD se aplica al tratamiento de los datos personales con arreglo a la Directiva 2015/849, pero ello es sin perjuicio de la protección de los datos personales tratados por las “autoridades competentes” de conformidad con 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 (Véase Considerando 40 de la Directiva 2018/843).

Dado que dicha Directiva 2016/680 aún no ha sido traspuesta, la LOPDGDD estableció en su Disposición transitoria cuarta que *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*

Dado que en el anteproyecto no se hace mención a la circunstancia de que las “autoridades competentes” (entiende esta Agencia que dicha mención concreta, dada la materia que regula, se refiere estrictamente a la autoridad competente nacional española para la prevención del blanqueo de capitales y financiación del terrorismo, esto es, a la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, y en su caso, sus órganos de apoyo), conforme precisa el considerando 40 de la Directiva 2018/843, pueden tratar datos conforme a la Directiva 2016/680, esta Agencia considera conveniente que se incluya en la ley -quizás en una disposición adicional- una mención a esta circunstancia que refleje igualmente el contenido de la DT cuarta de la LOPDGDD, que podría tener el siguiente contenido:

*La regulación contenida en la presente ley se entiende sin perjuicio de la protección de los datos personales tratados por las autoridades competentes de conformidad con la normativa que trasponga al derecho español 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.*

*En tanto no se trasponga al derecho español dicha Directiva 2016/680, será de aplicación la Disposición Transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*