

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

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

I

Tal y como indica su el artículo 1 del Reglamento cuya aprobación se pretende a través del Proyecto sometido a informe, su objeto es el desarrollo de la Ley 10/2010, en particular en lo referido a las obligaciones de los sujetos obligados y a la organización institucional en materia de prevención del blanqueo de capitales y la financiación del terrorismo.

A tal efecto, el Proyecto (al que nos referiremos en los sucesivo cuando pretendamos hacer referencia al Reglamento que el mismo contiene) desarrolla y detalla las distintas obligaciones contenidas en la citada Ley 10/2010, y derivadas a su vez de lo dispuesto en la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo.

De este modo, se detallan las obligaciones relacionadas con el cumplimiento del deber de diligencia debida y con el de examen especial y comunicación de operaciones, así como las obligaciones accesorias a aquéllas y la organización institucional de prevención del blanqueo de capitales.

Como punto de partida a lo que se razonará a lo largo del presente informe debe tenerse en cuenta la relevancia que en lo que respecta al cumplimiento de las obligaciones previstas en la normativa sectorial que regula el Proyecto sometido a informe ostenta el respeto a las garantías esenciales del derecho fundamental a la protección de datos de carácter personal. Esta interrelación generó, entre otras cosas, que la Ley 10/2010 estableciese una



serie de normas específicas en materia de tratamiento de datos de carácter personal, fundamentalmente contenidas en los artículos 15, 32 y 33 de la Ley, así como que el Director de la Agencia Española de Protección de Datos forme parte de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. Para tomar en consideración la interrelación entre el derecho fundamental a la protección de datos y las obligaciones derivadas de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo puede analizarse lo señalado por esta Agencia en el informe emitido en fecha 3 de abril de 2009 al entonces Anteproyecto de Ley de Integridad del Sistema Financiero, que culminó con la aprobación de la vigente Ley 10/2010.

El citado informe ya analizaba con detenimiento la existencia de legitimación para la realización de los diversos tratamientos establecidos en la Ley, así como para la cesión de datos a la Comisión de Prevención del blanqueo de capitales e infracciones monetarias y sus órganos de apoyo, en particular el Servicio Ejecutivo de aquélla, así como el cumplimiento en los citados tratamientos del principio de proporcionalidad en el tratamiento de los datos.

Quiere ello decir, que en el presente informe no se hará nuevamente referencia a la legitimación para los distintos tratamientos y cesiones de datos, así como a la obligación de conservación de información establecida en la Ley 10/2010, en términos que el Reglamento al que se refiere el Proyecto objeto de informe no hace sino clarificar.

De este modo, el tratamiento de datos necesario para el cumplimiento de las obligaciones de identificación formal de los clientes (artículo 5), del titular real (artículo 8), del propósito o índole de los negocios (artículo 9) y del seguimiento continuo de la relación comercial (artículo 10) traerían su causa de las obligaciones establecidas expresamente en el Capítulo II de la Ley 10/2010 y, en última instancia, de la Directiva 2005/60/CE, por lo que a su vez se encuentran amparados por el artículo 6.1 de la Ley Orgánica 15/1999.

Asimismo, las previsiones que se refieren a la recogida y tratamiento de los datos por parte de terceros sujetos obligados a los que otros sujetos encomienden estas actuaciones trae su causa de lo establecido en el artículo 8 de la Ley 10/2010. Del mismo modo, el tratamiento de los datos de personas con responsabilidad pública, ya sean las contenidas en la redacción originaria de la Ley 10/2010 ya se trate de las incorporadas con la reforma operada por la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno, se encuentran amparadas por lo establecido en el artículo 15 de la Ley 10/2010, que igualmente permite la obtención de esta información de terceros distintos de los sujetos obligados que proceda al tratamiento de datos identificativos de quienes tengan la condición de personas con responsabilidad pública con la exclusiva finalidad de colaborar con los sujetos obligados en el cumplimiento de las medidas reforzadas de diligencia debida.

Del mismo modo, las obligaciones de tratamiento de datos en la realización del examen especial de operaciones, del artículo 22 y para la comunicación de las operaciones al Servicio ejecutivo de la Comisión, tanto cuando se trata de comunicación por indicio (artículo 23) como de comunicación sistemática (artículo 24), traerían su causa de lo establecido en el Capítulo III de la Ley 10/2010, debiendo en relación con dichos tratamientos tenerse particularmente en cuenta lo establecido para estos tratamientos y para el intercambio de información asociada a las operaciones a las que estas obligaciones se refieren las previsiones establecidas en los artículos 32 y 33.

Las obligaciones de conservación de documentos previstas en los artículos 26 y 27 del Proyecto se encontrarían a su vez amparadas por el artículo 25 de la Ley 10/2010.

Por último, la existencia del fichero de titularidades financieras, regulado por la Sección 3ª del Capítulo V del Proyecto traería su causa de lo dispuesto en el artículo 43 de la Ley 10/2010, si bien debe ponerse de manifiesto el parecer de esta Agencia no completamente conforme al tenor de dicho precepto, manifestado en su informe de 16 de noviembre de 2009.

Del escueto resumen que acaba de indicarse no debe deducirse que el parecer de esta Agencia sea íntegramente favorable al contenido del Reglamento sometido a informe sin más matización, sino simplemente que los criterios generales de legitimación para el tratamiento y cesión de los datos necesarios para el cumplimiento de las obligaciones de prevención del blanqueo de capitales y la financiación del terrorismo ya fueron objeto de análisis y ponderación en los informes emitidos por la Agencia en relación al entonces Anteproyecto de Ley y que la inclusión de estas previsiones, informadas en la mayor parte de los casos favorablemente por esta Agencia, en el texto final de la Ley, permite amparar los tratamientos y cesiones, sin perjuicio de otras posibles matizaciones, en los artículos 6.1 y 11.2 a) de la Ley Orgánica 15/1999.

II

Hecha la anterior consideración general, no obstante esta Agencia considera necesario efectuar determinadas consideraciones en relación con el Proyecto sometido a informe, referidas a dos bloques de cuestiones principales:

En primer lugar, como ya se ha dicho, existen determinados preceptos de la Ley 10/2010 específicamente referidos a la aplicación de las normas de protección de datos en la recogida, tratamiento y cesión de los datos necesarios para el cumplimiento de las obligaciones contenidas en la Ley



10/2010 y, por ende, en el reglamento. Se trata, en resumen, de los artículos 15, 32 y 33 de la Ley.

Desde la entrada en vigor del citado texto legal se han planteado a esta Agencia diversas cuestiones relacionadas con la aplicación de los citados preceptos que, a nuestro juicio, podrían ser objeto de clarificación en el Proyecto ahora informado, a fin de facilitar el cumplimiento por los sujetos obligados no sólo de las disposiciones contenidas en la normativa de prevención, sino también en la de protección de datos, a la que están en todo caso sujetos, tal y como establece expresamente el artículo 32.1 de la Ley 10/2010.

De este modo, sería necesario que el Reglamento incorporase determinadas previsiones encaminadas a clarificar el contenido y alcance de los artículos 15, 32 y 33 y también en su caso, a delimitar los supuestos en los que esta Agencia ha considerado que dichos preceptos pueden servir de base legal para la realización de determinados tratamientos no previstos expresamente en la Ley 10/2010.

En particular, podría hacerse referencia, dentro de este bloque de cuestiones, a la delimitación del papel de responsable o encargado del tratamiento de los órganos centralizados de prevención, particularmente de los creados con carácter obligatorio por la Ley 10/2010, el nivel de seguridad exigible a los distintos tratamientos de datos realizados al amparo de la Ley 10/2010 y la procedencia o improcedencia de diferenciar los ficheros vinculados con el cumplimiento de las obligaciones de diligencia debida y de examen especial y comunicación, así como la posible creación de ficheros comunes de intercambio de información entre sujetos obligados al amparo de lo dispuesto en el artículo 33.2 de la Ley 10/2010.

El Proyecto, en este punto, no contiene ningún tipo de previsión clarificadora de las citadas previsiones, limitándose a hacer referencia en el artículo 25 a la exigencia de implantación de las medidas de seguridad de nivel alto “a los ficheros establecidos para el cumplimiento de las obligaciones de comunicación”

Dentro de esta primera categoría también habría de hacerse referencia al régimen aplicable al Fichero de Titularidades Financieras. No obstante, en este caso, a diferencia de los citados anteriormente, el análisis llevado a cabo por el presente informe partirá del estudio de las disposiciones contenidas en el propio Proyecto y no de la mera consideración de esta Agencia.

Junto a las citadas aclaraciones el presente informe incluirá otras relacionadas con el tenor de algunos de los preceptos contenidos en el Proyecto, sin perjuicio de que, como se ha dicho, nos remitamos al informe de esta Agencia de 3 de abril de 2009 en cuanto a la valoración de la legitimación para la recogida, tratamiento y cesión de los datos.



III

De las diversas cuestiones a las que hemos hecho referencia con anterioridad, en relación con el desarrollo de los artículos 32 y 33 de la Ley 10/2010 debe hacerse en primer lugar referencia a las relacionadas con la aplicación de lo establecido por el artículo 32.4, según el cual “Los órganos centralizados de prevención a los que se refiere el artículo 27 tendrán la condición de encargados del tratamiento a los efectos previstos en la normativa de protección de datos de carácter personal”.

Los citados órganos centralizados aparecen regulados, como se indica en el precepto, por el artículo 27 de la Ley, cuyo apartado 1 señala en el párrafo segundo que los mismos “tendrán por función la intensificación y canalización de la colaboración de las profesiones colegiadas con las autoridades judiciales, policiales y administrativas responsables de la prevención y represión del blanqueo de capitales y de la financiación del terrorismo, sin perjuicio de la responsabilidad directa de los profesionales incorporados como sujetos obligados. El representante del órgano centralizado de prevención tendrá la condición de representante de los profesionales incorporados a efectos de lo dispuesto en el artículo 26.2”.

No obstante, el artículo 27.1 parece ampliar ese ámbito competencial, dado que prevé que el análisis de las operaciones a las que se refiere el artículo 17 de la Ley, es decir, las sometidas a examen especial podrá llevarse a cabo “por propia iniciativa o a petición de los profesionales incorporados”, previéndose igualmente que los órganos comunicarán dichas operaciones al Servicio Ejecutivo de la Comisión “cuando concurren las circunstancias establecidas en el artículo 18”.

Además, el propio precepto prevé que “los profesionales incorporados deberán facilitar al órgano centralizado de prevención toda la información que éste les requiera para el ejercicio de sus funciones” y que aquéllos “facilitarán toda la documentación e información que la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias o sus órganos de apoyo les requieran, directamente o por intermedio del órgano centralizado de prevención, para el ejercicio de sus competencias”.

Además, debe tenerse en cuenta que el precepto establece una distinción entre los órganos centralizados de prevención de incorporación voluntaria y los de incorporación obligatoria, al indicar en el artículo 27.3 que “con excepción de los funcionarios a que se refiere el artículo 2.1.n), la incorporación de los sujetos obligados a los órganos centralizados de prevención será voluntaria”.



Este régimen se desarrolla por los artículos 42 y 43 del Reglamento sometido a informe, referidos respectivamente a los órganos de incorporación obligatoria y voluntaria y siendo más detallado el régimen de los primeros que el de los segundos, respecto de los que el Reglamento se limita a establecer que “ejercerán, en los términos que se determinen en la Orden de autorización, funciones de asesoramiento y formación de los profesionales incorporados”.

Respecto de los órganos centralizados de prevención de incorporación obligatoria ya se ha señalado que la Ley 10/2010 diferencia entre las operaciones que son llevadas a cabo por cuenta de los profesionales incorporados de aquéllas que se llevan a cabo a iniciativa propia, pudiendo el órgano centralizado de prevención proceder al análisis de determinadas operativas incluso sin conocimiento de los fedatarios públicos integrados en la profesión colegiada; es decir, los notarios y registradores, de conformidad con lo establecido en el artículo 27.3 de la Ley.

Esta diferenciación se plasma igualmente en el Proyecto sometido a informe, dado que el artículo 42.2, al enumerar las funciones de los órganos centralizados de prevención en los dos supuestos indicados hace mención no sólo de las que se llevan a cabo por cuenta de los funcionarios incorporados a los colegios, sino también de las que se realizan a iniciativa propia e incluso a requerimiento específico del Servicio Ejecutivo.

A tal efecto, el Proyecto otorga a los órganos centralizados de prevención la función de averiguación de la titularidad real derivada de los actos en que intervengan los notarios o registradores (apartado c), la atención de los requerimientos de información de los órganos competentes en materia de prevención, sin que la misma se lleve a cabo en su condición de mandatario de los colegiados (apartado e), el análisis del riesgo de la actividad desarrollada por los colegiados en atención a diversos criterios citados por el apartado f) o la supervisión del cumplimiento de los procedimientos de control interno por parte de los colegiados, cuyos resultados serán asimismo transmitidos al Servicio Ejecutivo (apartado i).

En particular, e incluso en relación con la comunicación por cuenta de los funcionarios de las operaciones al Servicio Ejecutivo, a la que se refiere el apartado b) del artículo 42.2 del proyecto, se señala expresamente que “excepcionalmente, el órgano centralizado de prevención podrá abstenerse de informar al funcionario interviniente cuando así sea solicitado por el Servicio Ejecutivo o cuando estime que ello pudiera poner en riesgo la investigación”. Además, como se establece en el propio artículo 27.2 de la Ley, conforme al artículo 42.3, párrafo primero “los órganos centralizados podrán requerir de los funcionarios incorporados cualquier información o documentación necesaria para el desarrollo de sus funciones”.

En este sentido, cabe hacer referencia al Acuerdo del Consejo General del Notariado, de 24 de marzo de 2012, por el que se aprueba la creación del



fichero de datos de carácter personal "Base de Datos de Titular Real" en cumplimiento de los trámites previstos en los artículos 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos, y 52 y ss. y 130 y ss. de su Reglamento aprobado por Real Decreto 1720/2007, de 21 de diciembre, en cuya Exposición de Motivos se señala que "El sistema notarial de prevención de blanqueo de capitales se basa en una compartimentación de las obligaciones que aquella LPBC impone al notario entre éste y el Órgano Centralizado de Prevención de Blanqueo creado por la Orden ECO/2963/2005, de 20 de septiembre (en adelante, OCP). Tal división de funciones no impide que el notario siga siendo sujeto obligado a todos los efectos (artículos 26 y 27 de la LPBC), si bien que tal condición lo es siempre desde la perspectiva global de la citada normativa, pues es evidente que determinadas obligaciones son intrasladables y, por tanto, ejercidas indefectiblemente por el notario (así, las de diligencia debida [artículos 3 y ss de la LPBC], de abstención [artículo 20 de la LPBC]) o de conservación [artículo 25 de la LPBC]), mientras que otras se ejercen de modo compartido (examen especial de operaciones [artículo 17 de la LPBC]) o en exclusividad por el OCP (sin ánimo exhaustivo, comunicación tras el examen especial de operaciones [artículo 18 de la LPBC], elaboración del Manual donde se incluyen las políticas y procedimientos que obligatoriamente han de ser cumplidas por los notarios [artículo 26.1 párr. tercero y ap. 3 de la LPBC] o formación de empleados [artículo 29 de la LPBC])".

El citado Acuerdo procedió a la creación del fichero "Base de Datos de Titular Real", atribuyéndose la responsabilidad del mismo, en lo que a la aplicación de la normativa de protección de datos se refiere, al propio Órgano Centralizado de Prevención del Consejo General del Notariado. En relación con dicha atribución, el informe emitido por esta Agencia a la Propuesta del mencionado Acuerdo en fecha 23 de febrero de 2012 analizaba esta cuestión en los siguientes términos:

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

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

En este mismo sentido, la Orden EHA/114/2008, de 29 de enero, por la que se Regula el cumplimiento de determinadas obligaciones de los notarios en el ámbito de la prevención del blanqueo de capitales crea en



su Anexo II del fichero de Cumplimiento de las obligaciones de tratamiento y comunicación de datos derivadas de lo dispuesto en los artículos 17 y 24 de la Ley del Notariado, con la finalidad de garantizar el “cumplimiento por el Consejo General del Notariado de las obligaciones de tratamiento y comunicación de datos derivadas de lo dispuesto en los artículos 17 y 24 de la Ley del Notariado” y recabando datos a partir de la “remisión de comunicaciones de los notarios y del índice único informatizado”. De dicho fichero es directamente responsable el mencionado Órgano Centralizado de Prevención.

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

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

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

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

Por último, la atribución de la responsabilidad del fichero al Órgano Centralizado de Prevención garantiza que se dé pleno cumplimiento a los deberes establecidos en la Ley 10/2010 y, particularmente, a la



prohibición de revelación prevista en su artículo 22, dado que el Consejo, en sí mismo, no tiene la condición de sujeto obligado de la Ley 10/2010.

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

Es decir, esta Agencia ha venido entendiendo que, sin perjuicio de que los órganos centralizados de prevención tengan, cuando actúan por cuenta de los sujetos obligados integrados en la correspondiente organización colegial, la condición de encargados del tratamiento, dichos órganos podrán, en los supuestos de órganos de integración obligatoria, como sucede en el caso del Consejo general del Notariado, decidir en determinados supuestos sobre la finalidad, contenido y uso del tratamiento llevado a cabo para el cumplimiento de determinadas obligaciones que les impone la normativa de prevención del blanqueo de capitales y la financiación del terrorismo, lo que les convertirá en esos supuestos en responsables del tratamiento.

Por este motivo, se hace necesario clarificar el tenor del artículo 27.4 de la Ley 10/2010 a través del Reglamento sometido a informe, previendo expresamente que en los supuestos de órganos centralizados de prevención de incorporación obligatoria determinadas funciones que atribuyen a los mismos tanto la citada Ley como el Proyecto sometido a informe, en desarrollo de la misma, implican la asunción por aquellos órganos de la condición de responsable del tratamiento.

Por ello, se propone la inclusión de un nuevo apartado 6 en el artículo 42 del Proyecto sometido a informe, que establezca lo siguiente:

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

Igualmente serán responsables de los tratamientos efectuados en el marco de sus funciones de análisis de riesgo y de supervisión establecidos en la normativa de prevención del blanqueo de capitales y la financiación del terrorismo, así como de los que se deriven directamente del acceso y tratamiento de la información de los datos contenidos en los ficheros de los que los propios órganos



fueran responsables, tanto en el marco de las obligaciones de diligencia debida como en las de examen especial e información establecidas en la normativa de prevención del blanqueo de capitales

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

IV

Como ya se anticipó, la segunda cuestión que a juicio de esta Agencia debería resolverse en el Reglamento cuyo Proyecto se somete a informe es la relativa al nivel de seguridad exigible a los tratamientos llevados a cabo para el cumplimiento de las obligaciones impuestas por la Ley 10/2010.

En este punto, el artículo 32.5 de la Ley dispone que “Serán de aplicación a los ficheros a los que se refiere este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal”

La aplicación de este precepto ha planteado dudas interpretativas a los distintos sujetos obligados, por cuanto si bien el deber de implantación de medidas de seguridad de nivel alto aparece referido a los “ficheros a los que se refiere este artículo”, es cierto que el artículo 32 se refiere en determinados lugares a cualesquiera ficheros creados para el cumplimiento de las disposiciones de la Ley, como sucede en el apartado 1, al someter todos los ficheros a lo dispuesto en la Ley Orgánica 15/1999 y sus disposiciones de desarrollo, mientras que en otros se refiere exclusivamente a los tratamientos relacionados con el cumplimiento de los deberes de información; es decir, los ficheros creados en el ámbito de las obligaciones impuestas en el Capítulo III de la Ley, como sucede en los apartados 2 y 3 al establecer determinadas excepciones al cumplimiento de las obligaciones impuestas por la Ley Orgánica.

De este modo, sería conveniente que el Proyecto sometido ahora a informe clarificase si el deber de implantación de las medidas de seguridad de nivel alto ha de exigirse a la totalidad de los tratamientos vinculados con el cumplimiento de las obligaciones previstas en la Ley 10/2010 o si dicho nivel es únicamente exigible de los tratamientos efectuados para el cumplimiento de las obligaciones de examen especial y comunicación, bien sistemática bien por indicio, al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.



La respuesta a la citada cuestión podría tomar como punto de partida lo que ya señalaba esta Agencia en su informe de 3 de abril de 2009, relacionado con lo dispuesto en el entonces Anteproyecto de Ley, en que se incorporaba una disposición literalmente reproducida por el artículo 32.5 en su redacción final. Dicho informe vinculaba la exigencia de implantación de las medidas de nivel alto a las excepciones del deber de información y del ejercicio por el interesado de sus derechos en relación con los tratamientos que se efectuasen en el marco del examen especial y de la comunicación al Servicio Ejecutivo. Así, el informe, en su apartado VIII señalaba lo siguiente:

“(...) el artículo 31.6 (...) dispone que “Serán de aplicación a los ficheros a los que se refiere este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal”.

En relación con esta previsión, debe tenerse en cuenta que la obligación de implantar las medidas de seguridad trae su causa del artículo 9 de la Ley Orgánica 15/1999, a cuyo tenor “El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural”.

En consecuencia, el deber de seguridad tiene por objeto primordial evitar la pérdida, alteración y, en particular, el acceso no autorizado a la información sometida a tratamiento.

Este objetivo debe ponerse en conexión con la fundamentación legal de los tratamientos a los que ahora se está haciendo referencia, relacionados con las operaciones que han de ser objeto de un análisis singular por los sujetos obligados y de la comunicación de éstas o de las que sean objeto de comunicación sistemática al Servicio Ejecutivo, existiendo además, como se ha venido reiterando una prohibición específica de revelación de la información a terceros e incluso al propio interesado.

De este modo, las cautelas tendentes a evitar el acceso no autorizado a la información contenida en los ficheros resulta esencial para el adecuado cumplimiento de los deberes derivados del propio Anteproyecto.

La evitación de estas situaciones se logrará esencialmente a través de dos medidas concretas: por una parte el control de todos los accesos que se realicen a la información, de forma que dicho acceso quede limitado a quienes forme parte de los órganos creados en el ámbito de la



estructura de la organización del sujeto obligado a los que se refiere el propio texto sometido a informe y, por otra, el cifrado de las comunicaciones de dicha información que impidan su interceptación por terceros.

Ambas medidas aparecen expresamente recogidas entre las de nivel alto previstas en el Reglamento de desarrollo de la Ley Orgánica 15/1999, lo que justifica que la norma ahora informada prevea expresamente la exigencia de este nivel de seguridad cuando se trate de ficheros relacionados con las obligaciones previstas en la Ley en cuanto al examen de operaciones y su comunicación al Servicio Ejecutivo, así como a los creados por éste último.

Por tanto, el artículo 31 del Anteproyecto, con la salvedad ya señalada en relación con los ficheros del Servicio Ejecutivo, resulta plenamente conforme a la Ley Orgánica 15/1999.”

Es decir, en el informe emitido por esta Agencia al proyecto normativo en el que se incorporó la exigencia de implantación de las medidas de nivel alto, ya se indicaba por la Agencia que tal exigencia debía considerarse aplicable a los ficheros creados en cumplimiento de lo establecido en el Capítulo III de la Ley 10/2010, sin perjuicio de que el apartado 1 del artículo 32 establezca una obligación general de sometimiento de cualesquiera ficheros vinculados con el cumplimiento de las obligaciones prevista en la Ley a la legislación vigente en materia de protección de datos de carácter personal.

En particular, y en relación con las obligaciones referidas al cumplimiento por los abogados como sujetos obligados de las obligaciones de diligencia debida establecidas en el Capítulo II de la Ley 10/2010, el informe de esta Agencia de 18 de junio de 2013 recordaba que “el cumplimiento de los deberes de diligencia debida y la averiguación de información acerca del cliente y del titular real de la actividad respecto de la cual, en definitiva, se solicitan los servicios del abogado no sólo forma parte de las obligaciones impuestas por la Ley 10/2010, sino que se encuentra igualmente vinculada con la actividad ordinaria del letrado, por cuanto la averiguación de las circunstancias relativas al cliente y a la operación respecto de la que se solicita asesoría jurídica o el procedimiento en que se presta la asistencia letrada. Por el contrario, los tratamientos llevados a cabo en cumplimiento de lo establecido en el Capítulo III tienen una finalidad directamente vinculada a la prevención del blanqueo de capitales y la financiación del terrorismo”.

El citado informe, en que se resolvía la consulta formulada por un despacho de abogados en relación con el nivel de seguridad exigible a los ficheros creados para el cumplimiento de las obligaciones de la Ley 10/2010, diferenciando entre los tratamientos referidos al cumplimiento de las obligaciones de diligencia debida y los vinculados con los supuestos de examen especial e información, añadía lo siguiente:



“Como señala la consulta, una interpretación literal del precepto parece implicar que el nivel de seguridad exigible será aplicable a cualesquiera ficheros o tratamientos se encuentran previstos en el artículo 32; es decir, todos los “creados para el cumplimiento de las disposiciones” de la Ley, como establece su apartado 1. De este modo, la exigibilidad del nivel de seguridad alto sería aplicable tanto a los ficheros creados para el cumplimiento de los deberes de diligencia debida como para los que fueran establecidos para cumplir las obligaciones de información previstas en el Capítulo III de la Ley. No obstante, podría hacerse referencia a varios argumentos que exigirían revisar si la interpretación literal de la norma es la única que ha de prevalecer en este caso.

Una primera aproximación podría partir igualmente de una interpretación literal y estricta de la norma, toda vez que el artículo 32.1 de la Ley 10/2010 se refiere a los ficheros “creados para el cumplimiento de las disposiciones de esta Ley”, siendo a los mismos a los que se refiere la aplicación del artículo 32 en su totalidad. De este modo si la información tratada por el sujeto obligado en cumplimiento del deber de diligencia debida no se incorpora a un fichero “creado” con la finalidad de dar cumplimiento a las obligaciones establecidas en la norma cabría considerar que el artículo 32 no resulta de aplicación.

Sin embargo esta interpretación debe ser considerada extremadamente rigorista, toda vez que en la práctica vaciaría de sentido el apartado 1 del artículo 32 de la Ley 10/2010, dado que los ficheros que incorporasen datos obtenidos en cumplimiento del deber de diligencia debida, aun en el supuesto de no estar incluidos en el artículo 32.1 sí estarían sometidos a la Ley Orgánica 15/1999, que resulta de aplicación según su artículo 2.1, párrafo primero a “La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.”, siendo datos de carácter personal conforme al artículo 3 a) “Cualquier información concerniente a personas físicas identificadas o identificables”. No obstante, esta interpretación permitiría considerar aplicables a los ficheros “no creados” exclusivamente para el cumplimiento de la Ley 10/2010 las medidas de seguridad que correspondieran conforme al artículo 81 del Reglamento de desarrollo de la Ley Orgánica y no las de nivel alto a las que se refiere el artículo 32.5.

En todo caso, esta interpretación dejaría en manos del sujeto obligado la imposición o no de las medidas de seguridad, según procediera o no a la creación de ficheros específicos para el cumplimiento del deber de diligencia debida, lo que tampoco resulta coherente ni con el espíritu de la Ley 10/2010 ni con la adecuada garantía del derecho fundamental a la protección de datos de carácter personal.



No obstante existe otro argumento, a juicio de esta Agencia de mayor calado, que permite efectuar una interpretación del artículo 32.5 de la Ley 10/2010 similar a la contenida en el apartado (ii) de la consulta formulada a esta Agencia, esto es, de considerar que la referencia efectuada por el artículo 32.5 de la Ley ha de entenderse realizada a los ficheros creados para el cumplimiento de los deberes de información regulados en el Capítulo III de la Ley 10/2010.

En este sentido, debe partirse de que el tenor del artículo 32.5 de la Ley 10/2010 impone al responsable de los ficheros a los que el mismo se refiere la obligación de implantar un nivel de seguridad que no se desprende de la normativa general de protección de datos, dado que la referencia a las finalidades vinculadas a la prevención del blanqueo de capitales y la financiación del terrorismo no aparece recogida en el artículo 81 del Reglamento de desarrollo de la Ley Orgánica 15/1999, que es el que delimita, dentro de la normativa general de protección de datos, los niveles de seguridad que resultan aplicables a los ficheros. Ello conduce a la necesidad de determinar cuál ha podido ser la razón que ha motivado al legislador la imposición de este nivel reforzado de medidas de seguridad no contenido en la normativa de protección de datos.

A tal efecto, debe tenerse en cuenta la diferenciación que se ha llevado a cabo en un lugar anterior entre los tratamientos realizados al amparo, respectivamente, de los Capítulos II y III de la Ley 10/2010, particularmente en lo que se refiere a la aplicación a los mismos de lo que puede ser considerado contenido esencial del derecho fundamental a la protección de datos.

Así, como se vio, los ficheros creados al amparo de lo dispuesto en el Capítulo III quedan exceptuados de la aplicación de la exigencia de consentimiento para el tratamiento, como consecuencia de una exclusión legal expresa, contenida en el artículo 32.2, así como del deber del responsable de informar al interesado acerca del tratamiento y de la obligación de este de atender los derechos consagrados por la legislación de protección de datos.

Estas limitaciones, sin embargo, no serán predicables de los ficheros y tratamientos llevados a cabo en cumplimiento de los deberes de diligencia debida a los que se refiere el Capítulo II de la Ley 10/2010. Ciertamente, la obtención por el abogado de los datos de su cliente dentro del marco de estos deberes se encontrará excluida de la exigencia del consentimiento del interesado, pero ello se fundará bien en la propia relación jurídica que vincula al abogado con el cliente, bien a la adecuada garantía del derecho a la defensa de éste, como parte del derecho fundamental a la tutela judicial efectiva, consagrado por el



artículo 24 de la Constitución. En todo caso, sí procederá la información al afectado y la atención de sus derechos de acceso, rectificación, cancelación u oposición, siendo igualmente preciso tener en cuenta el deber de secreto profesional impuesto al abogado por la normativa reguladora de su profesión, al que se ha hecho referencia en un lugar anterior.

A la vista de estos precedentes, y teniendo en cuenta que las limitaciones al derecho a la protección de datos únicamente se recogen en relación con los ficheros vinculados al cumplimiento de las obligaciones impuestas por el Capítulo III de la Ley 10/2010, puede considerarse que la exigencia de un nivel reforzado de seguridad, como el establecido en el artículo 32.5 tiene por objeto el establecimiento de una salvaguarda o garantía adicional que pueda servir de contrapeso a la limitación establecida por los apartados 2 y 3 del precepto.

De este modo, aun cuando se prevén limitaciones de los derechos de los interesados, el precepto exigiría que en estos supuestos se establezcan garantías reforzadas para evitar que quienes no hayan de acceder a la información puedan hacerlo, quedando así garantizado el control de quienes acceden a la información, a través de la figura del registro de accesos o exigiendo el cifrado de los datos en caso de uso de redes públicas de comunicaciones electrónicas. Del mismo modo, debería, entre otras cosas, procederse a la designación de un responsable de seguridad o a la realización de una auditoría específica sobre esos ficheros, tal y como exige el Reglamento para las medidas de seguridad de nivel medio, también aplicables a estos ficheros.

En consecuencia, la interpretación de que el nivel de seguridad alto es al que se refiere el artículo 32.5 de la Ley 10/2010 es únicamente exigible en relación con los ficheros creados para el cumplimiento de las obligaciones establecidas en el Capítulo III de la citada Ley ha de considerarse congruente con el hecho de que la propia Ley establece determinadas limitaciones al afectado en relación únicamente con dichos ficheros, siendo ese nivel exigible una garantía adicional establecida como contrapeso de las citadas limitaciones.”

El Proyecto sometido a informe establece en su artículo 25 que “los sujetos obligados aplicarán medidas de seguridad de nivel alto a los ficheros establecidos para el cumplimiento de las obligaciones de comunicación”.

Esta disposición encaja con la interpretación que esta Agencia ha venido realizando de lo dispuesto en el artículo 32.5 de la Ley 10/2010. Sin embargo, el hecho de que la misma aparezca exclusivamente referida a los ficheros creados al amparo de lo dispuesto en el Capítulo III de la Ley 10/2010 puede dar lugar a que se mantengan las dudas interpretativas que genera el citado artículo en cuanto al nivel de seguridad exigible a los tratamientos vinculados al



cumplimiento de las obligaciones de diligencia debida. Por este motivo, sería conveniente, garantizando en mayor medida el principio de seguridad jurídica, que el precepto se refiriese expresamente a los restantes tratamientos de datos, incluidos los vinculados al cumplimiento de las obligaciones de diligencia debida, y que por esta razón el precepto se ubique en un lugar distinto del Reglamento, probablemente dentro de las disposiciones establecidas en el Capítulo V.

Por todo ello, **se propone la supresión del artículo 25 del Proyecto sometido a informe, siendo reemplazado por otro precepto distinto con el siguiente tenor:**

“Artículo nn. Nivel de seguridad en los tratamientos de datos de carácter personal.

Los sujetos obligados aplicarán medidas de seguridad de nivel alto a los tratamientos llevados a cabo para el cumplimiento de las obligaciones de comunicación a las que se refiere el Capítulo III del presente Reglamento.

Será exigible a los tratamientos efectuados en el cumplimiento del deber de diligencia debida el nivel de seguridad que corresponda conforme a lo previsto en la normativa vigente de protección de datos de carácter personal.”

V

La última de las cuestiones en que el Proyecto sometido a informe podría clarificar el régimen establecido en la Ley 10/2010 en lo relacionado con el tratamiento de datos de carácter personal sería la relativa al modo en que será posible el intercambio entre sujetos obligados de la información a la que se refiere el artículo 33.2 de la Ley.

Según prevé el citado precepto “los sujetos obligados podrán intercambiar información relativa a las operaciones a las que se refieren los artículos 18 y 19 con la única finalidad de prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla”.

Si bien esta previsión permite el intercambio de información entre sujetos obligados, se ha planteado a esta Agencia si la misma podría legitimar la creación de sistemas comunes de información en que tales sujetos incorporasen información relacionada con las citadas operaciones, de forma que dicha inclusión permitiese a los restantes sujetos obligados asociados al



sistema acceder a los datos relacionados con las operaciones mencionadas en el artículo 33.2, de modo que el sistema de información reemplazase a las cesiones bilaterales de datos que el artículo legitima expresamente, teniendo en cuenta la redacción final del precepto fue precisamente propuesta por esta Agencia en su informe de 3 de abril de 2009.

En este ámbito debe traerse a colación lo analizado por esta Agencia en informe de 2 de agosto de 2011, en respuesta a la consulta planteada por la Asociación Nacional de Entidades de Pago (ANAED), referida a si resulta conforme a lo dispuesto en las normas de Protección de datos la creación y mantenimiento del denominado “Registro de agentes de alto riesgo”, con la finalidad de “impedir que los agentes de alto riesgo, cuyos datos figuren en el Registro, puedan desarrollar actividades relacionadas con el blanqueo de capitales o la financiación del terrorismo a través de las compañías adheridas al registro”, siendo agentes de alto riesgo “los agentes cuyas actividades u operaciones hayan sido puestas en conocimiento del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) por parte de una de las entidades adheridas, por su aparente vinculación con el blanqueo de capitales o la financiación del terrorismo, en cumplimiento de la exigencia prevista en el artículo 18 de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo”.

El citado informe analizaba, en primer lugar, el alcance de la habilitación establecida en el artículo 33.2 de la Ley 10/2010, señalando, como primera consideración, que dicha norma establece tres límites esenciales en cuanto al alcance de la cesión que implican los intercambios de información:

- En primer lugar, deberá tratarse, en todo caso, de operaciones que hayan sido objeto de comunicación al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, al amparo de la obligación impuesta en el artículo 18.1 de la Ley 10/2010.
- En segundo lugar, la comunicación únicamente podrá referirse, de entre las operaciones descritas anteriormente, a aquéllas respecto de las que pueda ser previsible el intento de comisión reiterada ante otro sujeto obligado, coincidiendo la operativa llevada a cabo por el presunto infractor en ambos casos.
- En todo caso, el intercambio de información podrá llevarse a cabo entre sujetos obligados.

El citado informe planteaba si resultaba posible la creación de un fichero de carácter sectorial y cuyo responsable fuera la asociación representativa de los sujetos obligados que procedían al intercambio de información señalando, en cuanto a la posibilidad de que tal asociación fuera responsable, lo siguiente:

“(...) ya se apuntó que el intercambio de información debería producirse entre sujetos obligados, conforme establece el artículo 33.2 de la Ley 10/2010, de constante cita, planteándose aquí el problema de que dicho intercambio se producirá no directamente entre entidades, sino a través de la asociación consultante, que por sí misma no tiene la condición de sujeto obligado.

No obstante, tal y como se indica en la consulta, la citada asociación es representativa de los sujetos obligados respecto de los que se prevé el intercambio de información pudiendo en tal caso considerarse que su actuación, de intermediación entre las entidades adheridas a la misma no violenta la letra de lo dispuesto en la Ley 10/2010.

En este sentido, la posición de la consultante en el supuesto planteado podría asimilarse a la de otras asociaciones representativas de entidades integradas en determinados sectores económicos respecto de las que previendo una norma con rango de Ley la posibilidad de intercambio de información entre las entidades pertenecientes a la asociación, esta Agencia ha considerado posible entender respetada la previsión legal cuando la propia asociación ha constituido un fichero que permita el intercambio de la información, teniendo la asociación la consideración de responsable del mencionado fichero.

Así, por ejemplo, cabe hacer referencia al Fichero Histórico de Seguros del Automóvil, del que es responsable la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA) y cuya existencia se funda en lo dispuesto en el artículo 25.4 del Texto Refundido de la Ley de Ordenación y Supervisión de los Seguros Privados, aprobada por Real Decreto Legislativo 6/2004, que expresa: “Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora (...)”. Dicho fichero se rige por un código tipo que fue objeto de aprobación por parte de la Agencia Española de Protección de Datos, de conformidad con lo establecido en el artículo 32 de la Ley Orgánica 15/1999 y en el Título VII de su Reglamento de desarrollo.

La Agencia consideró en relación con el citado fichero la posibilidad de que la organización que engloba a la mayoría de las entidades del sector pudiese actuar en este caso como responsable del fichero, pese a que del tenor literal del precepto se desprendería que sólo las entidades aseguradoras podrían generar el fichero e intercambiar entre sí la información, habida cuenta de la naturaleza y representatividad de dicha asociación.



Este mismo criterio permitiría entender en este caso cumplido el requisito de que la información sea intercambiada entre sujetos obligados, dado que será la asociación representativa de aquellos sujetos respecto de los que la información a intercambiar resulta relevante la que actuaría como responsable del fichero común que serviría de plataforma al intercambio de la información.”

Igualmente, ha de tenerse en cuenta lo señalado por esta Agencia en informe de 12 de marzo de 2012, referido a la consulta formulada por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) relacionada con la creación de un “Repositorio del Servicio de Información de los Sujetos Obligados”.

En este supuesto, el sistema de información objeto de creación se diferenciaba del mencionado en el informe de 2 de agosto de 2011 al implicar un ámbito más amplio de operaciones que podrían ser incorporadas al fichero, pudiendo producirse además un número más amplio de accesos por parte de categorías distintas de sujetos obligados. No obstante, el sistema permitía una compartimentación de la información, de forma que la misma sólo fuese compartida por sujetos obligados de la misma naturaleza que el informante; es decir, aquéllos en los que la operativa denunciada al Servicio Ejecutivo era realmente susceptible de reproducirse. Además, el sistema introducía una serie de garantías adicionales en el tratamiento de datos de carácter personal.

Tomando en cuenta tales consideraciones, y dada la amplitud del sistema de información creado, la Agencia hubo de analizar si la legitimación para su creación encontraba amparo en lo dispuesto en el artículo 7 f) de la Directiva, cuyo efecto directo había sido expresamente declarado por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 y que dispone que “los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva”.

El informe analizó la procedencia o improcedencia de la creación de este sistema a la luz de las garantías adicionales propuestas por la consultante, concluyendo lo siguiente:

“(...) esos criterios tendentes a garantizar adecuadamente el derecho a la protección de datos de las personas cuyos datos sean incluidos en el fichero común y, en consecuencia, objeto de consulta por los sujetos obligados, se ven además reforzados por otra serie de garantías adicionales que las normas de funcionamiento sometidas a informe vienen a establecer, y que pueden resumirse en las siguientes:



- *El establecimiento de compartimentos diferenciados atendiendo a la distinta naturaleza de los sujetos obligados intervinientes, lo que supone una limitación adicional de los supuestos de acceso a los datos, limitados a los órganos de control de los sujetos obligados de la misma naturaleza que el informante.*
- *El establecimiento de plazos sumamente reducidos, prácticamente de inmediatez, para la inclusión y baja de los datos en el sistema en caso de apreciarse, en cuanto a esta última acción, la existencia de un error en la información aportada o, en particular, de producirse la devolución de la operación por parte del Servicio Ejecutivo.*
- *La clarificación de que la información contenida en el fichero no puede determinar por sí sola la negativa a la operación solicitada, sino que deberá suponer la realización del examen especial al que se refiere el artículo 17 de la Ley 10/2010, en conexión con la prohibición de decisiones personales automatizadas establecida en el artículo 13 de la Ley Orgánica 15/1999.*
- *La existencia de los denominados coordinadores, cuya designación será obligatoria para los intervinientes, encargados expresamente del control de los accesos y consultas al fichero, a fin de que sólo puedan acceder a los datos las personas integrantes del órgano de control y únicamente para la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo.*
- *El establecimiento de un procedimiento de contestación a las solicitudes de ejercicio de los derechos previstos en la normativa de protección de datos en que se clarifique a los solicitantes la base legal que determina su denegación, al amparo del artículo 33.5 de la Ley 10/2010 y se haga constar el derecho de los afectados de solicitar la tutela de esta Agencia.*
- *La creación de un órgano específico encargado de velar por el efectivo cumplimiento de las normas de funcionamiento, del que formarán parte, en representación de los intervinientes, personas integradas en su órgano de control creado conforme al artículo 26 de la Ley 10/2010.*



- *El establecimiento de un régimen de infracciones y sanciones como consecuencia del incumplimiento de las reglas establecidas por las normas de funcionamiento que pueden implicar la exclusión e la participación en el sistema de quienes lleven a cabo incumplimientos de extrema gravedad como los descritos en el texto.*

En consecuencia, el sistema introduce una serie de medidas y garantías que permiten entender minimizado el riesgo que el tratamiento pudiera conllevar en los derechos y libertades del interesado, y en particular en su derecho fundamental a la protección de datos de carácter personal, lo que permite concluir que la creación del sistema y los tratamientos derivados del mismo se encuentran amparados por la normativa vigente en materia de protección de datos de carácter personal.”

Quiere todo ello decir que esta Agencia ha venido considerando amparada en la Ley 10/2010 la creación de sistemas comunes de información que permitan el intercambio de información al que se refiere el artículo 33.2 siempre que sean responsables de los tratamientos llevados a cabo en dichos sistemas los propios sujetos obligados o sus asociaciones representativas.

Por este motivo, sería conveniente que el Proyecto incorporase un precepto dentro del Capítulo V que hiciese expresamente referencia a la posible existencia de estos ficheros comunes, clarificando el alcance de los mismos y sus elementos esenciales. A tal efecto, se propone la inclusión de un nuevo precepto con el siguiente tenor:

“Artículo nn. Ficheros comunes para el cumplimiento de las obligaciones en materia de prevención.

Los sujetos obligados podrán, directamente o por medio de las asociaciones a la que pertenecieran, establecer sistemas ficheros comunes para el intercambio de los datos a los que se refiere el apartado 2 del artículo 33 de la Ley 10/2010. Dichos sistemas deberán, al menos, cumplir los siguientes requisitos:

- a) **Sólo podrá incorporarse al fichero información relacionada con operaciones que**
 - **Hubieran sido previamente objeto de comunicación por indicio al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, sin haber sido objeto de devolución por éste último.**
 - **Una vez rechazadas por el sujeto obligado que comunicase los datos fueran susceptibles de intentarse ante otros sujetos obligados.**



b) El tratamiento de los datos contenidos en el fichero únicamente podrá llevarse a cabo con la finalidad de prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo. En particular, los datos contenidos en el fichero no podrán incorporarse a otros sistemas de detección y prevención del fraude que no se encuentren relacionados con las materias indicadas.

c) El acceso a los datos contenidos en los ficheros quedará exclusivamente limitado a aquéllos sujetos obligados ante los que pudiera reiterarse la operativa a la que se refiera la información.

d) Únicamente podrán tener acceso al fichero quienes integren los órganos de control interno a los que se refiere el artículo 33 de este Reglamento.

En todo caso serán de aplicación a estos ficheros las exenciones y obligaciones a las que se refiere el artículo 33.5 de la Ley 10/2010.”

VI

Debe ahora procederse al análisis de las disposiciones contenidas en la Sección 3ª del Capítulo V del Proyecto de Reglamento, que tienen por objeto el desarrollo del denominado Fichero de Titularidades Financieras, regulado por el artículo 43 de la Ley 10/2010. A efectos de llevar a cabo la valoración de lo dispuesto en esta Sección resulta relevante recordar lo establecido en el citado artículo 43:

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

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

2. Los datos declarados serán incluidos en un fichero de titularidad pública, denominado Fichero de Titularidades Financieras, del cual será responsable la Secretaría de Estado de Economía.



El Servicio Ejecutivo de la Comisión, como encargado del tratamiento, determinará, con arreglo a lo establecido en la Ley Orgánica 15/1999, las características técnicas del fichero, pudiendo aprobar las instrucciones pertinentes.

3. Con ocasión de la investigación de delitos relacionados con el blanqueo de capitales o la financiación del terrorismo, los jueces de instrucción, el Ministerio Fiscal y, previa autorización judicial o del Ministerio Fiscal, las Fuerzas y Cuerpos de Seguridad, podrán obtener los datos declarados en el Fichero de Titularidades Financieras. El Servicio Ejecutivo de la Comisión podrá obtener los referidos datos para el ejercicio de sus competencias. La Agencia Estatal de Administración Tributaria podrá obtener los referidos datos en los términos previstos en la Ley 58/2003, de 17 de diciembre, General Tributaria.

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

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

Debe igualmente recordarse que el citado precepto hubo de ser objeto de un informe específico por parte de esta Agencia Española de Protección de Datos, a instancia del Consejo de Estado, habida cuenta de que su inclusión en el entonces Anteproyecto de Ley había sido posterior al informe de 3 de abril de 2009. Ese informe fue emitido en fecha 16 de noviembre de 2009, incluyendo una serie de observaciones que en su mayor parte no fueron tenidas en cuenta en el texto finalmente aprobado. No obstante, sin perjuicio de que la plasmación legal del fichero en la Ley 10/2010 puede implicar que algunas de esas observaciones no hayan de ser ahora reproducidas, existen otras que deben nuevamente tenerse en consideración, en cuanto el texto sometido a informe pueda exceder del contenido del artículo 43 o de la interpretación que deba darse a dicho precepto a la luz de los principios contenidos en la Ley Orgánica 15/1999.



Entrando ya en los preceptos que han de ser objeto de estudio, y siguiendo el orden establecido en la Sección 3ª, el artículo 49 especifica la finalidad del fichero, que será exclusivamente la de prevenir e impedir el blanqueo de capitales y la financiación del terrorismo, tal y como se desprende del artículo 43.1 de la Ley 10/2010, así como la condición de encargado del tratamiento del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, siendo responsable la Secretaría de Estado de Economía y Apoyo a la Empresa.

La primera de las cuestiones mencionadas ha de ser lógicamente informada de forma favorable por esta Agencia, no considerando redundante, sino clarificador, la inclusión del adjetivo “exclusiva”, al hacer referencia a la finalidad del fichero.

En cuanto a la condición de encargado del tratamiento del Servicio Ejecutivo, la misma se deriva directamente de lo establecido en el párrafo segundo del artículo 43.2 de la Ley 10/2010, por lo que, sin perjuicio de los comentarios que deban hacerse posteriormente acerca del alcance de su función, nada cabe objetar a esta circunstancia.

Respecto a la determinación del responsable del fichero, en el informe de 16 de noviembre de 2009 esta Agencia ya ponía de manifiesto que la Secretaría de Estado podía ostentar esta condición, pero únicamente como consecuencia del hecho de que ostenta la presidencia de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y de que la Secretaría de la citada Comisión se encuentra integrada en la misma. Así, el informe señalaba:

“Teniendo en cuenta este marco competencial, parece lógico entender que, en caso de procederse a su creación, el fichero se encuentre bajo la responsabilidad de los órganos competentes en materia de prevención del blanqueo de capitales y la financiación del terrorismo. De este modo, debería existir una relación entre la Comisión, a la que la Ley otorga la competencia en lo referente al impulso y coordinación de la ejecución de la normativa en esta materia, directamente o a través de los órganos que la integran y el fichero de titularidades financieras, dada la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo perseguida por el fichero.

Por ello, parece lógico concluir que el responsable del fichero habría de ser la propia Comisión o el Servicio Ejecutivo, dada su función de colaboración en la persecución del blanqueo de capitales y de la financiación del terrorismo.

En caso de persistir la atribución contenida en el Anteproyecto de la responsabilidad del fichero a la Secretaría de Estado de Economía, dicha atribución debería justificarse en la presidencia que la Ley atribuye



al Secretario de Estado o en el hecho de que una unidad de la Secretaría de Estado ostenta a su vez la secretaría de la Comisión.

Por este motivo, debería clarificarse la atribución de la condición de responsable del fichero, especificándose que la misma corresponderá a la Secretaría de Estado, “al ostentar la presidencia de la Comisión” o directamente a “la Unidad que ostente, conforme a lo previsto en esta Ley, la Secretaría de la Comisión”.

A la vista de todo ello, sería preciso que se justifique en el Anteproyecto sometido a informe la proporcionalidad de la creación del fichero citado, en los términos que se han expuesto, que se determine la finalidad del fichero y que, por último, se identifique al responsable, también en los términos que se han expuesto.”

A juicio de esta Agencia, el Proyecto debería tener en cuenta las conclusiones que acaban de reproducirse, de forma que se completase lo dispuesto en el apartado 2 del artículo 49, indicando lo siguiente:

“El Servicio Ejecutivo de la Comisión actuará como encargado del tratamiento por cuenta de la Secretaría de Estado de Economía y Apoyo a la Empresa, que será responsable del fichero de titularidades financieras al ostentar la Presidencia de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.”

VII

El artículo 50.1 del Proyecto regula la información que habrá de facilitarse al Servicio Ejecutivo, de conformidad con lo establecido en el artículo 43.1 de la Ley 10/2010. En este punto, el precepto viene a reproducir prácticamente lo establecido en el citado artículo de la Ley, aclarando que la referencia a titular habrá de entenderse también extensiva al titular real, lo que resulta acorde con la normativa de protección de datos, habida cuenta de que la finalidad del fichero es exclusivamente la de prevención del blanqueo de capitales y financiación del terrorismo, en que el concepto de titular real adquiere relevancia jurídica. Del mismo modo, la delimitación de lo que habrá de entenderse como datos identificativos resulta ajustada a la cobertura legal dada por la Ley 10/2010.

El párrafo segundo del artículo 50.1, no obstante, concluye diciendo que “mediante instrucción del Servicio Ejecutivo de la Comisión se podrán determinar otros datos de identificación que deban ser asimismo declarados a fin de la adecuada identificación de intervinientes, cuentas y depósitos”.

El informe de 16 de noviembre ya vino a clarificar cuál podría ser el alcance de las actuaciones del Servicio Ejecutivo en caso de ostentar la



condición de encargado del tratamiento, señalando que el mismo “dentro de los límites a los que se ha venido haciendo referencia, podrá adoptar las medidas que sean necesarias, siempre con respeto a lo dispuesto en la Ley Orgánica 15/1999 y sin que ello pueda afectar a su condición de mero prestador de servicios al responsable del fichero, a fin de garantizar las adecuadas garantías en el tratamiento de los datos. Sin embargo, dichas instrucciones deberán tener un carácter técnico y organizativo, no pudiendo el encargado, en nombre propio, adoptar por sí solo medidas tales como las relativas al modo en que deberían ser comunicados los datos al fichero, dado que las mismas deberán ser adoptadas por el responsable (bien directamente o a través del mencionado encargado, pero actuando éste último única y exclusivamente en nombre del responsable)”.

Quiere ello decir que la determinación de nuevos datos identificativos exigiría una decisión del órgano responsable del fichero y no de su encargado del tratamiento. En este sentido, las instrucciones a las que se refiere el artículo 50.2 deberían dictarse por la Secretaría de Estado o por la Comisión. Además, sería preciso que la adopción de tal decisión se llevase a cabo previo informe de esta Agencia.

Por tanto, será necesario modificar el párrafo segundo del artículo 50.1, en el sentido de **especificar que la instrucción a la que el mismo se refiere será adoptada por el responsable del fichero o por la Comisión, previo informe de esta Agencia y no por el Servicio Ejecutivo**, al ostentar éste la condición de encargado del tratamiento y no ser la delimitación de los datos contenidos en el fichero una “característica técnica” del mismo, en el sentido establecido en el artículo 43.2, párrafo segundo, de la Ley 10/2010.

Los apartados 2 y 3 del artículo 50 se refieren a la periodicidad de las comunicaciones al Servicio Ejecutivo y el deber de exactitud de las mismas, estableciéndose una comunicación mensual de datos, sin perjuicio de la obligación de corrección inmediata de los datos cuya inexactitud se aprecie por el Servicio ejecutivo o de aquellos respecto de los que las propias entidades detecten la existencia de irregularidades.

El párrafo primero del artículo 50.3 establece que “Las entidades de crédito declarantes serán responsables de la calidad, integridad y veracidad de los datos declarados, aplicando en origen los procedimientos de validación necesarios”.

Quiere ello decir que el sistema queda sometido a la diferenciación, ya consagrada por el tribunal Supremo, entre los responsables del tratamiento, las entidades informantes, y el responsable del fichero, la Secretaría de Estado, respondiendo las primeras de las posibles vulneraciones de la legislación de protección de datos que se deriven de la información facilitada y la segunda de las irregularidades que pudieran producirse en el propio funcionamiento del fichero.



Por otra parte, el último párrafo del artículo 50.2, a diferencia del párrafo segundo, se limita a señalar que las correcciones que deban efectuarse por haberse detectado una inexactitud por los sujetos obligados deberán llevarse a cabo, sin indicar que dicho deber de corrección habrá de ser inmediato.

Debe a tal efecto recordarse que el artículo 8.5 del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone en su párrafo segundo que “si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello”.

De este modo, **sería necesario que se especificase en el párrafo tercero del artículo 50.3 que la corrección a la que el precepto se refiere deberá llevarse a cabo “de inmediato” o “en el plazo máximo de diez días”.**

VIII

El artículo 51 del Proyecto de Reglamento regula los supuestos de acceso al fichero de titularidades financieras, limitadas en cuanto a los sujetos, por el artículo 43.3, párrafo primero, de la Ley 10/2010. El artículo 51.1 establece en su párrafo primero que los accesos serán “de carácter telemático”, encomendándose al Servicio Ejecutivo de la Comisión el establecimiento de los “procedimientos técnicos de consulta del fichero”, lo que a diferencia de lo previsto en el artículo 50, sí encaja en las facultades del Servicio Ejecutivo como encargado del tratamiento a la vista del artículo 43.3 de la Ley 10/2010.

Por otra parte, el precepto establece que el acceso se llevará a cabo “necesariamente a través de los puntos únicos de acceso designados a tal efecto en el Consejo General del Poder Judicial, en el Ministerio Fiscal, en las Fuerzas y Cuerpos de Seguridad del Estado y en la Agencia Española de Administración Tributaria”, añadiendo que “Cada organismo, a través de su punto único de acceso, comprobará la identidad de la autoridad o funcionario solicitante, verificará su habilitación legal para realizar la petición de acceso y velará por la pertinencia de las solicitudes, que deberán estar adecuadamente motivadas y quedarán bajo la responsabilidad de la autoridad o funcionario solicitante”.

Además, se prevé que “En cada punto único de acceso se mantendrá un registro pormenorizado de las peticiones realizadas, en el que figurará en todo caso la autoridad o funcionario solicitante y la justificación de la petición”. Finalmente, el artículo 51.3 dispone que “El Servicio Ejecutivo de la Comisión

llevará un registro de las consultas y accesos realizados en el ejercicio de sus funciones y por los puntos únicos de acceso”.

Debe en este punto tenerse en cuenta que el fichero de titularidades financieras, habida cuenta de su vinculación exclusiva a la prevención del blanqueo de capitales y el hecho de que su gestión será llevada a cabo por el Servicio Ejecutivo deberían implantarse, conforme a lo dispuesto en el artículo 32 de la Ley 10/2010, las medidas de seguridad de nivel alto establecidas en la normativa de protección de datos de carácter personal.

Dentro de estas medidas, el artículo 103.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone que “De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado”. Se establece así la medida del registro de accesos, a fin de verificar que la información contenida en los ficheros ha sido efectivamente conocida únicamente por los usuarios autorizados para ello, así como quién ha realizado cada acceso concreto, a fin de poder efectuar una trazabilidad de la información en caso de que se produzca un uso inadecuado de la información.

En el fichero de titularidades financieras la gestión del registro de accesos se llevará a cabo a través de dos capas sucesivas: en primer lugar, cada punto único de acceso evaluará y conservará información de los accesos que se soliciten del fichero por parte de los órganos integrantes del mismo; en segundo términos, el Servicio ejecutivo llevará a cabo un registro de sus accesos y de los efectuados desde cada uno de los puntos únicos de acceso.

Esta circunstancia podría, como se analizará con posterioridad, plantear algunos problemas, habida cuenta de la concurrencia junto con las competencias de esta Agencia de la competencia del Ministerio fiscal a la que se refiere el artículo 43.4 de la Ley 10/2010 y que se estudiará, en cuanto a su desarrollo reglamentario, en un lugar posterior de este informe.

Por otra parte, el último párrafo del artículo 51.1 dispone que “Las solicitudes de datos del Fichero de Titularidades Financieras deberán identificar a la persona o personas respecto de las que requiere información, no resultando admisibles búsquedas abiertas, genéricas o por aproximación. Mediante instrucción del Servicio Ejecutivo de la Comisión, se determinarán los requisitos mínimos de información que deberán cumplir las solicitudes”.

En cuanto al primer inciso, resulta plenamente congruente con lo establecido en el artículo 4.1 de la Ley Orgánica 15/1999, dado que el principio de proporcionalidad exigirá que los accesos al ficheros sean adecuados a la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo y a las competencias propias de quienes se encuentran legitimados para acceder a él. De este modo, no será conforme a la Ley Orgánica un acceso genérico a la información.

Por lo que respecta a la segunda de las previsiones contenidas en este párrafo, debe nuevamente tenerse en cuenta lo indicado con respecto a las competencias del Servicio Ejecutivo. De este modo, si bien podría adoptar como medida de índole técnica, un formulario de acceso a la información, cabe considerar que la determinación de los requisitos mínimos para el acceso debería corresponder al responsable del fichero y no al Servicio Ejecutivo.

Por ello, **sería necesario tener en cuenta en el segundo inciso del último párrafo del artículo 51.1 del Proyecto de Reglamento lo que ya se indicó en relación con el párrafo segundo del artículo 50.1, atribuyendo la competencia para fijar los requisitos mínimos necesarios para el acceso a la Secretaría de Estado o a la Comisión.**

IX

El artículo 52 establece las normas esenciales de protección de datos del fichero, estableciéndose como principio en el artículo 52.1 que “El Fichero de Titularidades Financieras quedará sometido a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su normativa de desarrollo” y en el artículo 52.3 que “La Agencia Española de Protección de Datos ejercerá respecto del Fichero de Titularidades Financieras todas las competencias que le atribuye la normativa en materia de protección de datos de carácter personal y, en particular, la potestad de inspección prevista en el artículo 40 de la Ley Orgánica 15/1999”.

Efectivamente, como se ha venido indicando, el fichero de titularidades financieras se encuentra plenamente sometido a la Ley Orgánica 15/1999 y sus normas de desarrollo, siendo la Agencia Española de Protección de Datos la competente para velar por el cumplimiento por el fichero de las normas contenidas en dicha Ley, de modo que dicha Agencia desplegará respecto del fichero la totalidad de las competencias establecidas en el artículo 37 de la Ley Orgánica.

De este modo, debe considerarse que la referencia a la potestad de inspección únicamente ha de ser entendida como aclaración de que la misma es una de dichas competencias que es particularmente considerada por el artículo 32.3, siendo a tal efecto relevante la cita del artículo 40 de la Ley Orgánica, que establece las especiales potestades de inspección de esta Agencia.

Las menciones que acaban de reproducirse resultan particularmente relevantes si se tiene en cuenta el especial régimen del fichero y las competencias atribuidas por el artículo 43.4 al ministerio Fiscal, que deberán ser en todo caso ejercidas sin que se produzca ningún menoscabo de las competencias propias de esta Agencia, tal y como se desprende del artículo



43.4, cuyo primer inciso señala terminantemente que la actuación del Ministerio Fiscal se llevará a cabo “sin perjuicio de las competencias que corresponden a la Agencia Española de Protección de Datos”, que en ningún caso podrán verse afectadas por lo dispuesto en ese precepto.

Por otra parte, el párrafo segundo del artículo 52.1 dispone que “Serán aplicables al Fichero de Titularidades Financieras las disposiciones contenidas en los apartados 2 y 3 del artículo 32 de la Ley 10/2010, de 28 de abril”.

Los citados preceptos exceptúan el cumplimiento de las obligaciones legales de información al interesado, consentimiento del mismo y atención al ejercicio por aquél de los derechos de acceso, rectificación, cancelación y oposición, disponiendo el artículo 32.3 de la Ley 10/2010 que estas excepciones legales se aplican a los ficheros “creados y gestionados por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta Ley”. No obstante, esta referencia exige dos clarificaciones:

En primer lugar, como se ha indicado en el apartado IV de este informe, las excepciones contenidas en los apartados 2 y 3 del artículo 32 van necesariamente unidas a la exigencia de medidas de seguridad de nivel alto impuesta por el artículo 32.5 de la Ley 10/2010, a la que sin embargo el artículo 52.1 del Proyecto no hace referencia, siendo así que será necesario que se indique expresamente que serán de aplicación al fichero tales medidas.

En segundo lugar, las exenciones de los apartados 2 y 3 del artículo 32 serán de aplicación a la Secretaría de Estado como responsable del fichero y al Servicio Ejecutivo en su condición de encargado del tratamiento, pero en ningún caso deberían considerarse predicables de las entidades obligadas a facilitar la información al fichero, que únicamente quedarían exoneradas de recabar el consentimiento del interesado al existir una legitimación legal para la cesión de los datos al Servicio Ejecutivo al amparo del artículo 11.2 a) de la Ley Orgánica 15/1999, en conexión con el artículo 43.1 de la Ley 10/2010.

Es decir; dado que la existencia del fichero de titularidades financieras deriva directamente de su creación a través de la Ley 10/2010 y, en consecuencia, no se trata de un fichero respecto de cuya existencia sea aplicable la prohibición de revelación establecida en el artículo 24 el citado texto legal, las entidades financieras debería informar a los clientes que la información referida a los titulares, autorizados y representantes así como la identificación de los productos financieros que se incluyen en el fichero van a ser objeto de transmisión al citado fichero, debiendo además atender a las solicitudes de ejercicio de derechos que les planteen los interesados, lo que por otra parte contribuirá a garantizar la exactitud de la información incluida en el fichero.

Estos deberes no son, sin embargo aplicables al Servicio Ejecutivo, dada su función de inteligencia financiera, lo que justifica que la exclusión efectuada



por el artículo 32.3 se aplique a la totalidad de los ficheros creados o gestionados por el mismo sin establecerse ningún tipo de vinculación con la obligación de prohibición de revelación establecida en la Ley.

Estas dos matizaciones exigirían que el artículo 52.1 se complete, estableciendo así lo siguiente:

“1. El Fichero de Titularidades Financieras quedará sometido a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su normativa de desarrollo.

Serán de aplicación al Fichero de Titularidades Financieras las medidas de seguridad de nivel alto establecidas en la normativa de protección de datos de carácter personal.

Serán aplicables al Fichero de Titularidades Financieras las disposiciones contenidas en los apartados 2 y 3 del artículo 32 de la Ley 10/2010, de 28 de abril. **No obstante, las entidades de crédito deberán informar a los titulares, representantes y autorizados de la cesión de los datos al Fichero.”**

X

Resta por último hacer referencia a lo dispuesto en los artículos 53 a 56 del Proyecto de Reglamento, relacionados con las funciones atribuidas al Ministerio Fiscal por el artículo 43.4 de la Ley 10/2010, reproducido en un lugar anterior de este informe.

Del tenor de este precepto, y al margen de las indicaciones relacionadas con la identidad y requisitos de la persona que habrá en la práctica de ostentar las funciones establecidas en el precepto dentro de la estructura organizativa del Ministerio Fiscal, es preciso extraer dos conclusiones que habrán de ser tenidas necesariamente en cuenta en el análisis de los preceptos a los que ahora se está haciendo referencia:

- En primer lugar, la actuación del Ministerio Fiscal se llevará a cabo “sin perjuicio de las competencias que correspondan a la Agencia Española de Protección de Datos”, lo que significa que, encontrándose el fichero sometido plenamente a la Ley Orgánica 15/1999 esta Agencia ostentará respecto del mismo, como se ha indicado en un lugar anterior, la totalidad de las competencias establecidas en la normativa de protección de datos de carácter personal. Esta afirmación, en todo caso, se contiene expresamente en el artículo 52.3 del Proyecto sometido a informe.



- En segundo lugar, la función del Fiscal designado consistirá en velar “por el uso adecuado del fichero, a cuyos efectos podrá requerir justificación completa de los motivos de cualquier acceso”.

Ambas conclusiones deben interpretarse de forma armonizada, lo que conduce a que sea especialmente relevante indicar desde este lugar que la función del Ministerio Fiscal no se referirá al cumplimiento de la legislación de protección de datos, materia ésta reservada a la competencia de esta Agencia, sino únicamente controlar a quienes resultan competentes para acceder al fichero y a los solos efectos de verificar que los accesos se han producido con cumplimiento de los requisitos legales. De este modo, si en el ejercicio de sus potestades de verificación el Fiscal que resultase designado en aplicación del artículo 43.4 de la ley 10/2010 comprobase que existen indicios de vulneración de la Ley Orgánica 15/1999 deberá poner estos hechos en conocimiento de la Agencia Española de Protección de Datos, por cuanto no ostentará ninguna de las competencias atribuidas por la Ley Orgánica 15/1999 a esta Agencia.

Como única peculiaridad, debe señalarse que este deber de comunicación a la Agencia únicamente quedará exceptuado en caso de que se aprecie que ha existido una vulneración de las normas de protección de datos por parte de los órganos judiciales, dado que ese punto deberá tenerse en consideración la doctrina derivada de la Sentencia del Tribunal Supremo de 5 de diciembre de 2011, en cuyo fundamento de derecho tercero se señala lo siguiente, en relación con los ficheros de los órganos jurisdiccionales:

“El propio Consejo General del Poder Judicial, con posterioridad a la LOPD, ha ratificado su competencia en esta materia en virtud del apoderamiento del art. 230 LOPJ al aprobar el Reglamento 1/2005, de 15 de septiembre, de los Aspectos Accesorios de las Actuaciones Judiciales. Este Reglamento dedica su Título V, en desarrollo del art. 230 de la LOPJ, a regular el establecimiento y gestión de los ficheros automatizados bajo responsabilidad de los órganos judiciales, comprendiendo tanto los ficheros de datos automatizados de carácter personal dependientes de los Juzgados y Tribunales como los del Consejo General del Poder Judicial, e incluyendo también en su ámbito tanto los ficheros jurisdiccionales (aquellos que incorporan datos de carácter personal que deriven de actuaciones jurisdiccionales), como los ficheros no jurisdiccionales o gubernativos (aquellos que incorporan datos de carácter personal que deriven de los procedimientos gubernativos así como los que, con arreglo a las normas administrativas aplicables, sean definitorios de la relación funcional o laboral de las personas destinadas en tales órganos y de las situaciones e incidencias que en ella acontezcan) y a todos ellos sitúa bajo el control del Consejo General del Poder Judicial con sujeción a un régimen específico de tutela ante los órganos de gobierno interno, mediante la articulación del correspondiente sistema de reclamaciones y recursos, en cuanto al ejercicio de los derechos de acceso, rectificación y cancelación.



Régimen de protección del que es ajeno la Agencia Española de Protección de Datos, a la que no se reconoce facultades de intervención, correspondiendo éstas a los órganos de gobierno judicial.”

En consecuencia, la competencia del miembro del Ministerio Fiscal nunca será la de velar por el cumplimiento de la Ley Orgánica, sino exclusivamente la de verificar que las solicitudes de acceso al fichero reúnen los requisitos exigidos por la legislación de prevención del blanqueo de capitales y la financiación del terrorismo.

De este modo, **en caso de que el representante del Ministerio Fiscal aprecie la existencia de una vulneración de lo dispuesto en la Ley Orgánica 15/1999 por el Servicio Ejecutivo o por quienes ostentan derecho a acceder a la información contenida en el Fichero de Titularidades Financieras deberá ponerlo en conocimiento de esta Agencia, salvo que la irregularidad se aprecie de los órganos jurisdiccionales, en cuyo caso habrá de poner los hechos en conocimiento del Consejo General del Poder Judicial**, siguiendo la doctrina sustentada por el Tribunal Supremo en la sentencia que acaba de citarse, lo que deberá hacerse constar en el Proyecto sometido a informe.

El artículo 53.2 del Proyecto dispone que “Las funciones del Ministerio Fiscal consistirán en autorizar la relación de puntos únicos de acceso a quienes el Servicio Ejecutivo de la Comisión habilitará su conexión al sistema y verificar que las consultas o accesos al Fichero de Titularidades Financieras han sido realizados por las autoridades o funcionarios autorizados y para los fines establecidos en la ley. Esta verificación se realizará en la forma prevista en los artículos siguientes”.

La determinación de quién ha de resultar competente para designar los puntos únicos de acceso al fichero, habilitando su conexión al mismo no corresponde estrictamente a esta Agencia. No obstante, **cabe considerar que dicha competencia debería recaer en el responsable del fichero; es decir, en la Secretaría de Estado de Economía y Apoyo a la Empresa o, por cuenta de ésta, al propio Servicio Ejecutivo, en su condición de encargado del tratamiento**, dado que según el concepto establecido en el artículo 3 d) de la Ley Orgánica 15/1999 es al responsable del fichero al que corresponde el poder de decisión sobre el uso del mismo, no pareciendo que dentro de las competencias establecidas en el artículo 43.4 de la Ley 10/2010 tenga encaje la designación de usuarios del fichero a la que se refiere este artículo ni menos aún la habilitación de la conexión al mismo que, como cuestión técnica parecería corresponder al Servicio Ejecutivo.

La cuestión donde sí resulta más relevante el análisis a llevar a cabo en el presente informe, habida cuenta de la posible concurrencia de la actuación del Fiscal designado con la que pudiera llevar a cabo esta Agencia en el ejercicio de sus competencias, es la relacionada con la verificación de la

regularidad de los accesos al Fichero, a la que se refieren los artículos 54 a 56 del Proyecto sometido a informe.

En este punto, señala el primer inciso del artículo 54.1 que “el Servicio Ejecutivo de la Comisión mantendrá permanentemente a disposición del Fiscal designado el registro de consultas y accesos previsto en el apartado 3 del artículo 51. Además, conforme al artículo 54.2 “el Fiscal podrá realizar la auditoría de accesos al Fichero de Titularidades Financieras cuando lo considere necesario para el control del adecuado uso del mismo, a cuyos efectos tendrá acceso inmediato al registro pormenorizado de accesos que debe mantenerse en cada punto de acceso según se establece en el apartado 1 del artículo 51. Asimismo, los puntos de acceso deberán facilitar al Fiscal cuanta información y documentación les solicite, por sí o a través del Servicio Ejecutivo de la Comisión, para llevar a cabo la auditoría de accesos”.

El segundo inciso del artículo 54.1 añade que “sin perjuicio de ello, cuando por cualquier motivo el Servicio Ejecutivo de la Comisión tuviera conocimiento de que se ha producido una consulta o acceso irregular al Fichero de Titularidades Financieras o se solicite un acceso fuera del cauce previsto en los apartados anteriores, dará traslado al Fiscal o, en su caso, al punto único correspondiente”.

El acceso a la información contenida en estos preceptos resulta congruente con la función atribuida al Fiscal por el artículo 43.4 de la Ley 10/2010, dado que este precepto le legitima para velar por el adecuado uso del precepto y acceder a la información necesaria para ello. Ahora bien esa competencia no puede en ningún caso menoscabar la propia de esta Agencia Española de Protección de Datos, que ha de poder igualmente acceder a la información referida a los accesos producidos en el Fichero, así como a la información que se conservase en los puntos de acceso al mismo.

Lo antedicho puede predicarse igualmente del acceso por parte del Consejo General del Poder Judicial a la información que pudiera obrar en el punto único de acceso que se estableciese para los órganos jurisdiccionales o para las autoridades autonómicas de protección de datos en relación con los puntos únicos de acceso por parte de las Fuerzas y Cuerpos de Seguridad de las correspondientes Comunidades Autónomas (actualmente la Autoridad Catalana de Protección de Datos en relación con los Mossos d'Escuadra y la Agencia Vasca de Protección de Datos en lo que afecta a la Ertzaintza).

Por ello, para que el artículo 54 resultase plenamente congruente con el ordenamiento jurídico en su totalidad, y no solamente con el último inciso del artículo 43.4 de la Ley 10/2010, sería necesario que se explicitase en el texto sometido a informe que los accesos a los que se refiere el precepto se entenderán en todo caso sin menoscabo alguno de que la información se encuentre igualmente a disposición de la Autoridad competente en materia de protección de datos para el ejercicio por la



misma de las competencias que le atribuye la Ley Orgánica 15/1999 o su normativa específica de aplicación en materia de protección de datos.

En relación al procedimiento de verificación, el artículo 55 del Proyecto prevé en su apartado 1 que en caso de apreciarse indicios de irregularidad en la consulta se procederá a la iniciación de actuaciones previas “que se registrarán, en cuanto no se opongan a lo dispuesto en este Reglamento, por lo establecido en los artículos 122 a 126, ambos inclusive, del Reglamento de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre”, pudiéndose tramitar igualmente las actuaciones en caso de que el Fiscal tenga conocimiento de la existencia de una consulta irregular, conforme al artículo 55.2.

Señala el artículo 55.3 que “las actuaciones previas tendrán por objeto determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación de un procedimiento sancionador por consulta o acceso irregular, así como identificar la persona que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso”, de forma que conforme indica el artículo 56.1 “si de las actuaciones previas resultara que la consulta o acceso investigado ha sido irregular, el Fiscal remitirá copia de lo actuado al órgano al que corresponda el inicio del correspondiente procedimiento disciplinario, salvo que los hechos sean constitutivos de delito, en cuyo caso remitirá lo actuado al órgano competente del Ministerio Fiscal”, debiendo el destinatario “incoar el procedimiento disciplinario correspondiente, notificando la resolución que ponga fin al procedimiento al Fiscal, que podrá interponer contra la misma recurso contencioso”.

A nuestro juicio, el régimen contenido en las normas que acaban de reproducirse puede introducir una grave confusión, al no deducirse claramente del mismo la diferencia que debe existir necesariamente entre las competencias del Fiscal designado al efecto y las autoridades competentes en materia de protección de datos y, particularmente, esta Agencia.

Así, en primer lugar, la apertura por el Fiscal de actuaciones previas al amparo de lo dispuesto en los artículos 122 y siguientes del Reglamento de desarrollo de la Ley Orgánica 15/1999 parece atribuir al mismo competencias en relación con la aplicación de las normas de protección de datos, siendo así que tal competencia se encuentra vedada expresamente por el artículo 43.4 de la Ley 10/2010, amén de por la propia Ley Orgánica 15/1999.

Debe a tal efecto tenerse en cuenta que las normas a la que el Proyecto establece una remisión no podrían ser aplicables a las actuaciones previas a las que se refiere el texto ahora informado. Así, ni las actuaciones pueden traer causa de la existencia de indicios de una presunta infracción de la Ley Orgánica 15/1999, ni podrán dirigirse a la determinación de su existencia y su presunto autor, ni se desarrollarían por el personal al que se refiere el artículo 123 del Reglamento, ni sería preciso atender a las previsiones de los artículos



124 y 125 en cuanto a la obtención de información y actuaciones presenciales, dado que el propio Proyecto establece especificaciones al efecto, ni sería aplicable el artículo 126, dado que el artículo 56 del Proyecto establece cuál puede ser el resultado de las actuaciones.

Por su parte, de lo dispuesto en los artículos 55 y 56 se desprende una aparente contradicción, dado que mientras el primero de ellos se refiere a la procedencia de la incoación de un procedimiento sancionador por consulta o acceso irregular, el segundo hace referencia al procedimiento disciplinario que habrá de seguirse por el órgano competente contra quien efectivamente hubiera realizado un acceso irregular al fichero.

En este punto, la diferencia entre la actuación del Fiscal designado y la competencia de esta Agencia resulta sustancial, toda vez que las actuaciones del Fiscal deberán dirigirse no contra un responsable del fichero o encargado del tratamiento, sino contra quien efectivamente hubiese realizado un acceso indebido al fichero; es decir, el objeto del procedimiento sería la adopción por el órgano competente de las medidas disciplinarias que pudieran corresponder contra esa persona concreta e individualizada, contra la que deberá dirigirse la actuación del Ministerio Fiscal.

Siendo esto así, la consecuencia que cabe extraer es que la contradicción que podría producirse entre las normas citadas debería ser superada especificando que el procedimiento que habrá de seguirse será el disciplinario y no el sancionado, lo que podría generar una distorsión con la aplicación de las normas de protección de datos.

Además, si como consecuencia de las actividades llevadas a cabo por el Fiscal designado se apreciase la existencia de una vulneración de la normativa de protección de datos, los hechos deberán ser puestos en conocimiento de la autoridad competente en materia de protección de datos y, particularmente, de esta Agencia.

A la vista de todo ello, **sería necesaria la adopción de tres modificaciones en las previsiones de los artículos 55 y 56 del Proyecto:**

- Suprimir la remisión efectuada a los artículos 122 y siguientes del Reglamento de desarrollo de la Ley Orgánica 15/1999, estableciendo si se estima pertinente, en el propio texto, las especialidades que pudieran corresponder, como por ejemplo el establecimiento de un período máximo de un año para la realización de las actuaciones previas.

- Clarificar en el artículo 55.3 que las actuaciones tendrán por objeto determinar la procedencia de la incoación de un procedimiento disciplinario por consulta o acceso irregular al fichero.



- Añadir en el artículo 56.1 que en caso de que se apreciase la existencia de una vulneración de la Ley Orgánica 15/1999 los hechos serán puestos inmediatamente en conocimiento de esta Agencia o de la autoridad de protección de datos que, en su caso, resulte competente.

XI

En relación con el tratamiento de datos de personas con responsabilidad pública, el artículo 13 del Proyecto de Reglamento se refiere a la posible cesión de los ficheros que contengan los datos identificativos de las mismas entre sujetos obligados, disponiendo que “para la determinación de la condición de persona con responsabilidad pública, los sujetos obligados podrán acordar la cesión de ficheros creados al amparo de lo establecido en el artículo 15.1 de la Ley 10 /2010, de 28 de abril. En estos supuestos, los acuerdos de formalización incluirán las respectivas obligaciones de las partes a fin de cumplir con las limitaciones y requisitos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal”.

Es preciso tener en consideración que dicho precepto se refiere únicamente a los ficheros creados por los sujetos obligados al amparo del artículo 15.1 de la Ley 10/2010, a cuyo tenor “los sujetos obligados podrán proceder a la creación de ficheros donde se contengan los datos identificativos de las personas con responsabilidad pública, aun cuando no mantuvieran con las mismas una relación de negocios”, pudiendo a tal efecto los sujetos obligados “recabar la información disponible acerca de las personas con responsabilidad pública sin contar con el consentimiento del interesado, aun cuando dicha información no se encuentre disponible en fuentes accesibles al público”. Dichos ficheros quedan limitados exclusivamente en cuanto a su finalidad al cumplimiento de los deberes de diligencia debida, tal y como establece el último párrafo del precepto.

En consecuencia, el Proyecto no establece ninguna previsión en relación con el acceso a los ficheros que fueran creados por sujetos distintos de los sujetos obligados para facilitar el cumplimiento del deber de identificación de las personas con responsabilidad pública, lo que se ve reforzado por el hecho de que el artículo 13 del Proyecto sea inmediatamente posterior al artículo 12, que desarrolla a su vez el artículo 8 de la Ley 10/2010, referente a la aplicación por terceros sujetos obligados de las medidas de diligencia debida. Es decir, nos encontramos ante una norma que se refiere a la colaboración entre sujetos obligados y no a la colaboración de terceros, respecto de la que el Proyecto parece considerar suficiente el marco normativo establecido por la Ley.

Hecha esta precisión, debe entenderse que la cesión entre sujetos obligados de los datos meramente identificativos de las personas con responsabilidad pública se encuentra legitimada por la posibilidad contemplada por el párrafo segundo del artículo 15.1 de recabar información sobre los



misimos de cualesquiera fuentes, sean o no de acceso público. Por tanto la cesión se ampararía en el artículo 11.2 a) de la Ley Orgánica 15/1999, en conexión con el citado párrafo segundo del artículo 15.1 de la Ley 10/2010.

Implicando la conclusión anterior la licitud de lo previsto en el artículo 13 del Proyecto, cabría no obstante introducir en aquél determinadas aclaraciones, tendentes a precisar su alcance.

Así en primer lugar, cabría plantearse la elección por el Proyecto del término cesión, que podría ser interpretado en un sentido restrictivo de desplazamiento material o transmisión de los datos entre sujetos obligados. En este sentido, podría ser recomendable reemplazar este término por la habilitación de los sujetos obligados para acceder a los ficheros de otros sujetos obligados que fueran creados al amparo de lo dispuesto en el artículo 15.1, dado que ese acceso podría implicar tanto la transmisión de los datos como su posible consulta individualizada on-line, fuera dicha consulta o no precedida de una solicitud específica. De este modo, la utilización del término “acceso” permitiría ampliar la libertad para que los sujetos obligados pudieran establecer libremente los términos y alcance del intercambio de información derivada del artículo 13 del Proyecto.

En segundo lugar, cabría plantearse si la referencia a los sujetos obligados podría también extenderse a los órganos centralizados de prevención a los que se refieren los artículos 42 y 43 del Proyecto, en desarrollo del artículo 27 de la Ley 10/2010.

Ciertamente, los órganos centralizados de prevención no tienen en sí mismos la condición de sujetos obligados en materia de prevención del blanqueo de capitales y la financiación del terrorismo. No obstante, como se ha analizado en un lugar anterior de este informe, el papel que a los mismos otorga la Ley 10/2010 y detalla el Proyecto sometido a informe, especialmente en cuanto a los órganos de integración obligatoria de notarios y registradores, regulados por el artículo 42 viene a imponer a aquéllos una serie de obligaciones que, como se señaló también en un lugar anterior, les acercan a la condición de sujetos obligados.

En este punto, la referencia a los órganos centralizados de prevención podría resultar relevante, por cuanto su inclusión en la norma otorgaría una cobertura específica a las cesiones de los ficheros que pudieran ser creados para el cumplimiento de los deberes vinculados a la identificación de las personas con responsabilidad pública, que diferiría de la legitimación genérica establecida por el artículo 15.2 de la Ley 10/2010, siempre y cuando dichos órganos dieran estricto cumplimiento a las disposiciones de la Ley Orgánica 15/1999. En este punto la cobertura del artículo 8 de la Ley 10/2010 resultaría más compleja, dado que los citados órganos centralizados no son estrictamente, como se ha dicho, sujetos obligados.



La cobertura podría referirse exclusivamente a los órganos centralizados de prevención mencionados en el artículo 42, dada la obligación de integración en los mismos, sin perjuicio de que pudiera analizarse su aplicabilidad a los órganos previstos en el artículo 43. Su referencia expresa en el precepto evitaría el que hubiera de plantearse si dichos órganos tienen la condición de sujeto obligado, por cuanto se incluyen de forma específica junto con aquéllos.

Por último, el precepto prevé que en los acuerdos de acceso o cesión que se suscriban se incluirán las respectivas obligaciones a cumplir en relación con la Ley Orgánica.

Debe en este punto señalarse que dicho cumplimiento habrá de ser íntegro por ambos sujetos obligados, si bien el establecimiento de las obligaciones de las partes que coadyuven al cumplimiento puede considerarse adecuado. No obstante, sería relevante que se estableciesen específicamente en el precepto los deberes a cumplir en relación con dos deberes específicamente establecidos en la Ley 10/2010: el de seguridad y el de garantía de exactitud de los datos.

En cuanto al primero, es preciso recordar que los ficheros de las personas con responsabilidad pública quedan sometidos a las medidas de seguridad de nivel alto, ello implica, en particular, que sea necesario el establecimiento de ciertas medidas específicas.

En primer lugar, en caso de que se procediera a la transmisión física de los datos, el artículo 101.2 del reglamento de desarrollo de la Ley Orgánica 15/1999 establece que “la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte”.

En caso de comunicación telemática, el artículo 104 del mismo Reglamento dispone que “cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros”.

Además, en caso de acceso electrónico a los datos, será necesario que el responsable del fichero de personas con responsabilidad pública respecto del que se produzcan los accesos establezca el sistema de registro de los mismos al que se refiere el artículo 103 del Reglamento, analizado en un lugar anterior de este informe.

En cuanto al deber de actualización, el artículo 15.4 de la Ley 10/2010 establece que “los sujetos obligados y los terceros a que se refiere el apartado



2 deberán establecer procedimientos que permitan la actualización continua de los datos contenidos en los ficheros relativos a las personas con responsabilidad pública”.

Por todo ello, se propone la siguiente redacción para el artículo 13 del Proyecto de Reglamento sometido a informe:

“Para la determinación de la condición de persona con responsabilidad pública, los sujetos obligados podrán **acceder a los ficheros** creados al amparo de lo establecido en el artículo 15.1 de la Ley 10 /2010, de 28 de abril **por otros sujetos obligados o los órganos centralizados de prevención a los que se refieren el artículo 42 de este Reglamento.** En estos supuestos, los acuerdos de formalización incluirán las respectivas obligaciones de las partes a fin de cumplir con las limitaciones y requisitos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, **en particular en los referido a la seguridad en la transmisión de los datos y a los procedimientos a adoptar para garantizar la actualización continua de los datos contenidos en los ficheros.**”

XII

Resta, por último, hacer referencia a determinadas previsiones del Proyecto de Reglamento que pudieran incidir en la aplicación de la normativa de protección de datos o en la actuación de esta Agencia:

La primera de ellas se deriva de lo dispuesto en el artículo 22, relativo al examen especial y, particularmente, a los supuestos en que dicho examen proceda de la información facilitada por directivos, empleados y agentes, a los que se refiere el artículo 22.2, dado que el último párrafo del artículo 22.5 dispone que “en aquellos supuestos en que la detección de la operación derive de la comunicación interna de un empleado, agente o directivo de la entidad, la decisión final adoptada sobre si procede o no la comunicación por indicio de la operación, será puesta en conocimiento del comunicante”.

En este punto debería plantearse si no podría perjudicar el deber de prohibición de revelación establecido en el artículo 24 de la Ley 10/2010 el hecho de que quienes pusiesen los hechos en conocimiento de los órganos de prevención tuvieran conocimiento de su la operación ha sido finalmente comunicada al Servicio Ejecutivo.

Ciertamente sería posible entender que dado que el artículo 24.1 hace referencia a los directivos y empleados del sujeto obligado la comunicación a los mismos de la información estaría excluida de esta prohibición.

No obstante, cabría diferenciar los supuestos en los que la comunicación pudiera ser necesaria, por cuanto fuera el empleado o agente quien tuviera relación directa con el sujeto al que se refiriera el examen especial o el directivo hubiera de participar en la toma de decisiones en materia de comunicación, de aquéllos en los que no concurre esta circunstancia y la revelación pudiera implicar una brecha en la citada prohibición de revelación.

No debe olvidarse que la aplicación de este precepto desencadena una serie de consecuencias relevantes en materia de protección de datos, que implican serias restricciones a los derechos de los interesados y la exigencia de garantías especiales de seguridad, como se analizó en lugares anteriores.

Por este motivo, **debería plantearse si la previsión del artículo 22.5, párrafo último, del Proyecto no debería ser matizada o suprimida en atención a lo que se acaba de indicar.**

En segundo lugar, debe hacerse referencia al artículo 34.1, cuyo párrafo segundo *in fine* dispone que “cuando el intercambio de información se haga con países no considerados como equivalentes en materia de protección de datos, dicho intercambio de información se realizará conforme a normas aprobadas por la Agencia Española de Protección de Datos”.

Las observaciones a este inciso son de carácter meramente técnico y se refieren a la aplicación establecida en la normativa de protección de datos de carácter personal del régimen de las transferencias internacionales de datos, definidas por el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999 como “Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español”.

El artículo 33.1 de la Ley Orgánica 15/1999 dispone que “No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas”. En su desarrollo, el artículo 66 del Reglamento dispone lo siguiente:

“1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se



otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente Reglamento.

La autorización se otorgará conforme al procedimiento establecido en la Sección Primera del Capítulo V del Título IX de este Reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el Capítulo II de este Título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la Sección Primera del Capítulo IV del Título IX del presente Reglamento.”

De este modo, serían necesarias dos correcciones terminológicas en el precepto informado:

- En primer lugar, debería reemplazarse la referencia a “países no considerados equivalentes” por “países que no ofrezcan un nivel adecuado de protección” de conformidad con la normativa de protección de datos.
- En segundo lugar, debería indicarse que el intercambio de la información exigirá la autorización del Director de la Agencia Española de Protección de Datos en lugar de someter el mismo a las “normas” adoptadas por esta Agencia, sin perjuicio de su posible adopción al amparo del artículo 37.1 c) de la Ley Orgánica 15/1999.

Por tanto, se propone la siguiente redacción para el párrafo segundo del artículo 34.1:

“En estas políticas se incluirán los procedimientos para el intercambio de información entre los miembros del grupo, estableciendo las cautelas adecuadas en relación con el uso de la información intercambiada. Cuando el intercambio de información se haga con países que **no ofrezcan un nivel de protección adecuado de conformidad con lo dispuesto en la normativa de protección de datos, **será precisa la autorización de la transferencia internacional de datos por parte de la Agencia Española de Protección de Datos, en los términos****



establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y sus disposiciones de desarrollo.”

Una tercera cuestión aparece igualmente vinculada con el artículo 34 del Proyecto, que en su apartado 4 dispone que “a efectos del presente Reglamento, resulta de aplicación la definición de grupo recogida en el artículo 42 del Código de Comercio”.

Ciertamente, esta previsión tiene en cuenta la excepción establecida en el artículo 24.2 a) de la Ley 10/2010, que se refiere igualmente al artículo 42 del Código de Comercio. No obstante, debe recordarse que la interpretación estricta de esta norma propició la emisión por esta Agencia del informe de 21 de diciembre de 2010, emitido a instancia de la entonces Dirección General del Tesoro y Política Financiera, en que se planteaba “cuál es el régimen jurídico aplicable a las cesiones de datos en el seno de los Sistemas Institucionales de Protección, previstos en el artículo 8.3.d) de la Ley 13/1985, de 25 de mayo, para el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo establecidas en la Ley 10/2010, de 28 de abril, a la luz de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre”.

Tras analizar en el citado informe la existencia o no de una posible cobertura legal a la cesión de datos ente entidades integrantes de Grupos que no se correspondieran íntegramente con lo establecido en el artículo 42 del Código de Comercio y, particularmente, lo establecido en la Directiva 2005/60/CE, el informe concluía que “aun cuando el citado artículo 24.2 a) está, para la definición de grupo, a lo dispuesto en el artículo 42 del Código de Comercio, dicho precepto debe ser interpretado a la luz de la norma que el mismo transpone al derecho español; es decir, del artículo 28.3 de la Directiva, que establece un concepto de Grupo más amplio que el establecido por el legislador español, debiendo tenerse en cuenta que de la redacción del precepto que acaba de citarse no se desprende el mero establecimiento de una opción que puede adoptarse o no por el legislador nacional, sino de una excepción clara precisa e incondicional a la prohibición general de revelación que tiene, precisamente, por objeto, el establecimiento de un mecanismo que garantice y refuerce la efectividad de las medidas de prevención del blanqueo de capitales y la financiación del terrorismo perseguidas por esa norma comunitaria”.

Por tanto, se concluía entonces que “de este modo, y teniendo en cuenta todo lo que ha venido indicándose y en particular la necesidad de interpretar lo dispuesto en el artículo 24.2 a) de la Ley 10/2010 a la luz de la norma que es objeto de transposición a través de dicho precepto, cabe considerar que la cesión de datos entre las entidades que conforman un sistema institucional de protección con la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo se encuentra amparada por el artículo 11.2 a) de la



Ley Orgánica 15/1999, en conexión con el artículo 24.2 a) de la Ley 10/2010 y, particularmente, del artículo 28.3 de la Directiva 2005/60/CE

En consecuencia, **cabría valorar si cabe efectuar una delimitación de Grupo que exceda de la prevista estrictamente en el artículo 34.4, siempre dentro de los límites establecidos en la normativa de la Unión Europea.**

Es cuanto tiene el honor de informar,

Madrid, 18 de febrero de 2014.

EL ABOGADO DEL ESTADO
JEFE DEL GABINETE JURIDICO

Fdo.- Agustín Puente Escobar.

SR. DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS