

**N/REF: 0051/2021**

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, solicitado de esta Agencia Española de Protección de Datos (AEPD) de conformidad con lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en relación con el artículo 57.1, letra c), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 389/2021, de 1 de junio, cumples 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**

El texto remitido tiene por finalidad la transposición de la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo.

La citada Directiva, partiendo de que la lucha contra las formas graves de delincuencia, en particular contra el fraude financiero y el blanqueo de capitales, sigue siendo una prioridad para la Unión (Considerando 5) y que facilitar el uso de la información financiera es necesario para prevenir, detectar, investigar o enjuiciar delitos graves (Considerando 1), tiene por objetivo mejorar el acceso a la información por parte de las Unidades de Información Financiera (UIF) y las autoridades públicas responsables de la prevención, detección, investigación o enjuiciamiento de delitos graves, potenciar su capacidad para llevar a cabo investigaciones financieras y mejorar la cooperación entre ellas (Considerandos 2 y 31).

De este modo, la Directiva establece medidas destinadas a facilitar el acceso a la información financiera y a la información sobre cuentas bancarias, así como su uso por las autoridades competentes, para la prevención, detección, investigación o enjuiciamiento de infracciones penales graves (Capítulo II). Asimismo, establece medidas destinadas a facilitar el intercambio de información entre las autoridades competentes y las UIF y entre las UIF (Capítulo III) y el intercambio de información con Europol (Capítulo IV).

Durante la tramitación de la citada Directiva, distintos órganos informaron sobre la necesidad de conciliar los objetivos perseguidos por la misma con el necesario respeto del derecho fundamental a la protección de datos personales. En este sentido, el Comité de Control Reglamentario destacó, especialmente, que el alcance de esta iniciativa no estaba bien definido, especialmente en lo que respecta a la ampliación cooperación transfronteriza y la justificación para operar sin una autorización judicial y que los impactos sobre los derechos fundamentales no eran exhaustivamente examinados, en particular dada la extensión de su ámbito a los delitos graves. Asimismo, el Supervisor Europeo de Protección de Datos, en su dictamen de 10 de septiembre de 2018, destacó la importancia de resaltar la plena aplicación de la normativa europea sobre protección de datos personales, haciendo especial referencia a los principios de limitación de la finalidad, necesidad y proporcionalidad y valorando positivamente algunas de las garantías que se establecían, como los registros de accesos o de solicitudes de información.

La Directiva aprobada ha recogido parcialmente dichas observaciones, siendo numerosas las referencias que contiene a la necesidad de respetar el derecho a la protección de datos personales (Considerandos 23, 24, 25, 26 ,27 y 28) y estableciendo algunas garantías específicas, entre las que se incluyen, además de las continuas referencias a la necesidad y la proporcionalidad, las condiciones que debe reunir el personal que puede acceder a los registros centralizados de cuentas bancarias o la necesidad de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos (artículo 5), o el establecimiento por las autoridades que gestionan los registros centralizados de cuentas bancarias de un registro de cada vez que las autoridades competentes designadas acceden y consultan la información sobre las cuentas bancarias, que se examinarán regularmente por los delegados de protección de datos y estarán a disposición de la autoridad de control competente (artículo 6). Asimismo, incluye un capítulo específico relativo a las disposiciones suplementarias relativas al tratamiento de los datos personales (Capítulo V), aplicable los supuestos de intercambios de información regulados en los Capítulos III y IV que se refiere al tratamiento de datos personales sensibles (artículo 16), el registro de las solicitudes de información (artículo 17) y las restricciones de los derechos de los interesados (artículo 18).

## II

El Anteproyecto objeto de informe procede a la transposición de la Directiva (UE) 2019/1153 incluyendo la mayoría de las garantías relativas a la protección de datos personales a las que anteriormente se ha hecho referencia.

No obstante, dentro del margen de apreciación que deja la Directiva y al objeto de su adecuada incorporación a nuestro ordenamiento jurídico, debe tenerse en cuenta, en determinados supuestos a los que posteriormente se hará referencia, la doctrina del Tribunal de Justicia de la Unión Europea y de nuestro Tribunal Constitucional referente a las medidas limitativas del derecho fundamental a la protección de datos personales.

Por ello, antes de proceder al análisis concreto del texto remitido, se considera conveniente recordar dicha doctrina, así como los criterios mantenidos por esta Agencia en cuestiones directamente relacionadas con el contenido de la norma, como lo relativo a los tratamientos de datos personales por la Policía Judicial o la exigencia de autorización judicial para el acceso al Fichero de Titularidades Financieras.

A este respecto, y partiendo de los fines perseguidos por la Directiva, debe recordarse que en la **Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, en el asunto *Digital Rights Ireland* (asuntos acumulados C-293/12 y C-594/12)** reconocía que la lucha contra el terrorismo internacional y los delitos graves constituye un objetivo de interés general, si bien cuando las herramientas legales promulgadas para perseguir ese objetivo interfieren con los derechos fundamentales a la privacidad y protección de datos, es necesario analizar la proporcionalidad de tales medidas (apartados 41 a 48).

Por otro lado, el Tribunal Constitucional ha tenido ocasión de examinar los requisitos para que las leyes que establecen tratamientos de datos personales, en cuanto que restricciones al derecho fundamental a la protección de datos personales del interesado, puedan considerarse conformes a la Constitución.

En este sentido, la **STC 292/2000, de 30 de noviembre**, después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en su lo siguiente:

Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [ RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido ( SSTC 57/1994, de 28 de febrero [ RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [ RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. **Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen.** Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que

la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional [...]”. (Fundamento Jurídico 11)

“De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales ( SSTC 104/2000, de 13 de abril [ RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley ( STC 178/1985 [ RTC 1985, 178] ), **éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación.** Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como **certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho** (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [ RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [ RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar

opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica [...]”. (FJ 15).

“Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que **la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora**. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [ RTC 1989, 37], y 49/1999, de 5 de abril [ RTC 1999, 49] ).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concorra algún derecho o bien constitucionalmente protegido. **Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias**. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. [...] (FJ 16)”.

Más recientemente, analizando igualmente los límites al derecho fundamental a la protección de datos personales, la **sentencia núm. 76/2019 de 22 mayo** después de recordar que “A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental. En este fundamento jurídico precisaremos la



naturaleza y el alcance de este específico requisito constitucional”, analiza cuál es la norma que debe contener las citadas garantías:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. **Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado.** Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa **regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales.** Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares” (FJ 8).

Por otro lado, y en lo que se refiere al principio de proporcionalidad la **Sentencia del Tribunal Constitucional 14/2003, de 28 de enero**, recuerda lo siguiente:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario

constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [ RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [ RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [ RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [ RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [ RTC 2000, 186] , F. 6).”

De acuerdo con la citada doctrina constitucional, los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.

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

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



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

Asimismo, debe citarse la doctrina del Tribunal Constitucional contraria a los tratamientos masivos de datos personales, recogida, entre otras, en la **sentencia 17/2013, de 31 de enero de 2013**, en la que determinó la constitucionalidad del artículo 16.3 de la Ley de Bases de Régimen Local referente a la comunicación de los datos del Padrón municipal a otras Administraciones Públicas.

Tal y como ha sido interpretado por el TC en dicha sentencia (FJ 8), este precepto se refiere a la cesión no consentida de los datos relativos a la residencia o el domicilio a otras Administraciones públicas que así lo soliciten solamente en aquellos casos en los que, para el ejercicio de sus competencias, sean aquellos datos relevantes. En suma, esta petición, que no se refiere específicamente a la cesión de datos del padrón en lo concerniente a los datos de los extranjeros, tiene por finalidad poder disponer de los datos relativos a la residencia o el domicilio que constan en el padrón municipal, (...). De esta forma, de acuerdo con la Ley Orgánica de protección de datos, la finalidad inicial que justificó la recogida de los datos por parte de una Administración pública no impide el destino posterior de los datos para su uso en finalidades diferentes de aquellas que motivaron su recogida respetando, en todo caso, el principio de reserva de ley para establecer dicho cambio, (...) la Ley de bases de régimen local en su condición, además, de norma reguladora de un fichero como el padrón municipal puede prever cesiones de datos entre Administraciones públicas.

(...) los datos cedidos han de ser los estrictamente necesarios para el cumplimiento de las funciones asignadas a los órganos administrativos de forma que deberá motivarse la petición de aquellos datos que resulten relevantes, pues es necesario distinguir entre el análisis y seguimiento de una situación individualizada relativa a un caso concreto y el suministro generalizado e indiscriminado de toda la información contenida en un registro personal. El precepto ha contemplado ambos extremos de manera que cualquier cesión de los datos del padrón debe fundamentarse en la necesidad por parte de la Administración cesionaria actuando en el ejercicio de sus competencias, de conocer, en cada caso concreto, el dato relativo al domicilio de la persona afectada, extremos que han de ser adecuadamente valorados por la cedente a fin de apreciar si los datos que se solicita son realmente necesarios, pertinentes y proporcionados, atendiendo a la competencia que pretende ejercer la Administración cesionaria (art. 4 in fine de la Ley 30/1992). Se trata así de una regla de por sí restringida a los datos relativos a la residencia y al domicilio en cada caso concreto, y a la que le resultarán de aplicación, de más está decirlo, el resto de principios y previsiones que conforman el contenido del derecho reconocidos en la legislación sobre protección de datos.

De lo anteriormente transcrito, y del resto de la fundamentación jurídica contenida en dicha sentencia resulta que el TC ha determinado que (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley (art. 16.3 LBRL).

Por otro lado, la citada sentencia del Tribunal Constitucional 17/2013 analizaba, en su Fundamento Jurídico Noveno, un supuesto específico de acceso a los datos del padrón, por vía telemática, por la Dirección General de la Policía, para la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley Orgánica de Derechos y Libertades de los Extranjeros en España y su Integración Social, sobre control y permanencia de extranjeros en España, y que se recoge en la disposición adicional séptima de la LBRL, introducida por el art. 3.5 de la Ley Orgánica 14/2003, de 20 de noviembre, en la que se señala lo siguiente:

“Ahora bien, dicha previsión legal ha de ser entendida de forma acorde con las exigencias de proporcionalidad que nuestra doctrina exige en la

limitación de un derecho fundamental como es el aquí concernido, relativo la protección de datos de carácter personal. Eso significa que la cesión de datos que el acceso regulado por el precepto supone ha de venir rodeado de una serie de garantías específicas, garantías que, cumplimentadas por el órgano administrativo al que el precepto hace referencia, son, evidentemente, susceptibles de control. Entre ellas se encuentra la necesidad de motivar y justificar expresamente tanto la concreta atribución de la condición de usuario para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos accesos de que se trate, evitando –en cuanto que la exigible motivación de tales decisiones facilita su correspondiente control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional Contencioso-Administrativo– que se produzca tanto un uso torticero de dicha facultad como accesos indiscriminados o masivos. Límites al contenido del acceso que también resultan de determinadas previsiones de la legalidad ordinaria, las cuales han de ser aplicadas teniendo presente, en todo caso, la necesaria unidad del ordenamiento jurídico, tales como el art. 16.3 LBRL, que ya hemos examinado o, incluso, otras regulaciones específicas de la Ley Orgánica de protección de datos, en especial su art. 22.2. Resulta de ello que el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte pertinente y necesario en relación con la finalidad que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la Ley pues, en caso contrario, no resultará posible su uso. Con tales garantías el acceso regulado en la disposición cuestionada resulta ser proporcionado en relación con la finalidad perseguida, ya que, en tanto que el dato resultante solo puede ser utilizado para la finalidad establecida en el precepto, ha de realizarse de forma puntual por quien se encuentre expresamente habilitado para ello y en relación a datos concretos cuya necesidad ha de ser también justificada de forma expresa y, por tanto, sometida a control, en los términos que acabamos de exponer.”

Dicha interpretación restrictiva de los límites al derecho fundamental a la protección de datos, así como la necesidad de que el legislador establezca garantías adecuadas para legitimar dicha injerencia, incluido, en su caso, el control judicial previo, resulta, igualmente, conforme a la jurisprudencia que va emanando del Tribunal de Justicia de la Unión Europea.

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

Pues bien, la **STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros**, en su apartado 175, recuerda que:

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

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

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

En definitiva, el apartado 175 de la **STJUE de 16 de julio de 2020, C-311/2020, Schrems 2**, dice:

Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

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

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

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

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

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

Precisamente, la falta de garantía de un control judicial previo fue la que determinó que el TJUE (**sentencia de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y otros**, anteriormente citada) anulara la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, al concluir que, aunque los fines que persigue son de interés general, no contempla medidas ni garantías suficientes para evitar que se excedan los límites del principio de proporcionalidad ni que se produzca un abuso en el acceso y uso de los datos por parte de las autoridades nacionales al investigar los delitos graves que justifiquen la intrusión, destacando que “En particular, la Directiva 2006/24 no establece ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el

objetivo perseguido. **En especial, el acceso a los datos conservados por las autoridades nacionales competentes no se supedita a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido y se produzca a raíz de una solicitud motivada de dichas autoridades presentada en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos.** Tampoco se ha establecido una obligación concreta de los Estados miembros de que se fijen tales limitaciones”.

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

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

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



efectos de dicha lucha (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 51)".

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

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

Será a juicio del Tribunal "el Derecho nacional en que debe determinar los requisitos conforme a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder dicho acceso. **No obstante, la normativa nacional de que se trata no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, ni siquiera el de la lucha contra la**

**delincuencia grave. En efecto, tal normativa nacional debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 61)” (apartado 118).**

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

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

Precisamente, el establecimiento de garantías específicas y adicionales a las previstas en la Directiva 2006/24 por la legislación nacional de transposición de la misma es la que permite mantener su plena vigencia no obstante la anulación de la Directiva por el TJUE, tal y como expresamente razona el **Tribunal Supremo** en Sentencia **núm. 727/2020 de 23 de marzo**:

A este fin debemos hacer una primera observación. El hecho de que se haya declarado la invalidez de la Directiva 2006/24/CE no significa que las leyes nacionales de trasposición que la desarrollaron en cada país sigan la misma suerte.

Una Directiva es un instrumento de armonización de las legislaciones nacionales pero que admite márgenes de discrecionalidad. Tan es así que en relación con la conservación de datos las legislaciones de cada Estado miembro evidencian notorias diferencias. De ahí, que una vez

vigente la norma nacional, si es respetuosa con el derecho de la Unión, tiene autonomía respecto de la Directiva que justifica su nacimiento y sólo puede ser derogada por una norma posterior. Ciertamente las sentencias del Tribunal de Justicia de la Unión son vinculantes, pero en lo que atañe a este caso, las sentencias que se acaban de citar no conllevan de forma ineludible la nulidad de la Ley 25/2007, sino que obligan a analizar si el régimen de conservación de datos en España, cuya regulación no se limita a la ley citada, es conforme con el derecho de la Unión.

Resulta obligada una segunda observación. En este momento la Unión Europea, una vez anulada la Directiva 2006/24/CE, carece de un instrumento de armonización de las legislaciones nacionales. La ausencia de una norma comunitaria obliga a centrar la atención en la doctrina del TJUE y no podemos dejar de destacar que cada nueva sentencia del alto tribunal, tal y como hemos tratado de resumir anteriormente, añade matices, establece excepciones, diseña nuevos requisitos y modulaciones, estableciendo doctrinas que adicionan y acumulan conceptos normativos que acrecientan su complejidad jurídica. Y tan es así que el propio TJUE en buena medida ha desplazado el problema de la licitud de la norma a la validez probatoria de la información obtenida a partir de los datos conservados por exigencias de las normativas nacionales, lo que, a nuestro juicio, evidencia que el alto tribunal es consciente de la complejidad de la situación creada como consecuencia de su propia doctrina y, sobre todo, de la ausencia de un marco normativo que dote de la necesaria seguridad jurídica a esta compleja materia.

Según venimos comentando, en España esta materia se regula por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuyo objeto declarado en la Exposición de Motivos, se promulgó con la finalidad de trasponer al derecho interno la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo.

Esta Ley ha sido confirmada en su vigencia por dos leyes posteriores: La Ley 9/2014, de 9 de mayo, General de las Telecomunicaciones, y la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que en sus respectivos artículos 42 y 52 remiten a la Ley 25/2007 en todo lo concerniente a la conservación y de cesión de datos con fines de detección, investigación y enjuiciamiento de delitos graves. Por lo tanto, el Legislador no sólo no ha dudado de la

legalidad de la ley de referencia sino que la ha confirmado expresamente en las dos leyes posteriores, precisamente las leyes que han establecido la regulación básica en este ámbito normativo.

La anulación de la Directiva 2006/24/CE nos podría llevar a considerar nula la ley española de desarrollo pero semejante automatismo no es admisible. La Directiva en cuestión no fue anulada por un único motivo. El TJUE realizó un profundo análisis de conjunto y detectó deficiencias diversas o ausencia de controles también diversos que conferirían a la norma comunitaria una laxitud que daba como resultado la ausencia de protección suficiente de los derechos fundamentales afectados. La interacción de esas deficiencias es lo que motivó la declaración de nulidad.

Así, se analizaron factores como los siguientes: a) Afección generalizada a todas las personas sin vinculación directa o indirecta a acciones penales; b) Ausencia de límites temporales o geográficos que vinculen la conservación con hechos delictivos concretos o que permitan contribuir a la prevención, detección o enjuiciamiento de delitos graves; c) Falta de precisión respecto de las personas que puedan tener acceso y posterior uso de los datos; d) Ausencia de criterios objetivos respecto al uso posterior de los datos a lo estrictamente necesario, sin supeditarlos a un previo control judicial o de un organismo autónomo independiente; e) Ausencia de criterios objetivos para que la cesión se limite estrictamente a fines de prevención y detección de delitos graves; f) Establecimiento de un plazo de conservación único sin distinción entre la categoría de datos; g) Falta de un alto nivel de protección y seguridad de los datos conservados, a través de medidas técnicas y organizativas, frente a abusos y accesos ilícitos y que garanticen la integridad y confidencialidad de los datos.

Si hacemos ese análisis en la normativa española se puede comprobar que gran parte de las deficiencias advertidas en la Directiva anulada no se producen en nuestro ordenamiento jurídico. Destacamos, a este respecto, las siguientes notas:

- (i) La ley española obliga a la conservación de datos de tráfico y localización durante un año y permite su cesión a las autoridades judiciales, si bien esa cesión está sujeta a estrictas garantías.
- (ii) Los prestadores de servicios obligados por ley a la conservación de datos no pueden realizar operación alguna de

tratamiento, a salvo de la cesión singularizada que pueda recabar la autoridad judicial.

Esto es importante, porque la doctrina del TJUE ha tenido como finalidad esencial la protección de los derechos a la vida privada, a la protección de datos y a la libertad de expresión, hasta el punto de en sus sentencias se ha insistido en que los datos conservados "considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan" ( STJUE de la Gran Sala de 8 de abril de 2014 (TJCE 2014, 104) - Caso Digital Rights- 27).

La Ley española no genera ese riesgo. Los datos conservados permanecen custodiados y no pueden tener más uso que su cesión a la autoridad judicial cuando ésta, lo ordene bajo un riguroso sistema de garantías. Ciertamente la conservación de datos y la obligación de cesión es en sí "tratamiento de datos" y así lo ha reiterado el TJUE en varias de sus sentencias para afirmar la competencia del derecho comunitario sobre esta cuestión, pero no puede desconocerse que los obligados por la Ley 25/2007 sólo deben y pueden almacenar los datos, pero no están habilitados para realizar ninguna de las operaciones de tratamiento que podrían ser especialmente lesivas para los derechos que se pretenden salvaguardar. Los prestadores no pueden, por tanto, estructurar, seleccionar, divulgar, transmitir, combinar o utilizar para fines de investigación criminal esos datos.

(iii) Sólo cabe ceder los datos conservados para la detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en leyes especiales (artículo 1.1), precepto que antes debía ser integrado acudiendo a los artículos 13.1 y 33.1 CP y actualmente acudiendo al artículo 579.1 de la LECrim que sólo autoriza este tipo de injerencias en delitos castigados con al menos pena de prisión de 3 años, en delitos de terrorismo y en el delitos cometidos por grupos u organizaciones criminales.

(iv) Los datos que deben conservarse son los necesarios para rastrear e identificar el origen y destino de una comunicación, el tipo de comunicación y el equipo de comunicación de los usuarios (artículo 3.1) pero en ningún caso se pueden conservar datos que revelen el contenido de la comunicación (artículo 3.2)

(v) Los datos sólo pueden ser cedidos previa autorización judicial (artículo 6.1) y la resolución judicial que autorice la cesión deberá ser motivada y ajustarse a los principios de necesidad y proporcionalidad, especificando los datos que han de ser cedidos (artículo 7.2). Esta garantía es esencial y muchas de las legislaciones de los Estados de la Unión autorizaban la cesión a autoridades no judiciales.

(vi) La cesión se limita a su utilización en investigaciones penales por delitos graves (artículo 7) y no cabe la conservación o cesión para finalidades distintas de la investigación penal, como ha ocurrido en otras legislaciones, ni para la investigación de delitos de escasa entidad

(vii) Los datos sólo pueden ser cedidos a agentes especialmente facultados, señalando como tales a los miembros de los Cuerpos Fuerzas de Seguridad del Estado, Agentes de Vigilancia Aduanera y agentes del CNI) y deberán limitarse a la información imprescindible (artículo 6.2);

(viii) La ley impone a los sujetos obligados todo un conjunto de obligaciones para garantizar la integridad, seguridad, calidad y confidencialidad de los datos en el artículo 8 y establece un régimen de sanciones para caso de incumplimiento (artículo 11). Además, hay todo un desarrollo reglamentario que detalla las especificaciones técnicas en la forma de cesión de las operadoras a los agentes ( Orden PRE/199/2013, de 29 de enero, que en todo caso ha de limitarse a lo estrictamente necesario. Y la ley española prevé un nivel de seguridad medio para este tipo de ficheros lo que garantiza la confidencialidad de los datos almacenados (artículo 81.4 del Real Decreto 1720/2007, de 21 de diciembre sobre Reglamento de Protección de Datos).

(ix) La Ley de Enjuiciamiento Criminal ha realizado una completa regulación de las intervenciones telefónicas y telemáticas, incluyendo en ellas el uso de los datos conservados por obligación legal (artículo 588 ter j), sujetando todas ellas a un estricto control judicial en su adopción y en su ejecución, con aplicación de los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad.



Conviene destacar que el uso de los datos almacenados está sujeto a estrictas limitaciones que se contienen en los artículos 588 bis a) y siguientes de la LECrim, entre las que destacamos:

- (i) La utilización de datos está sujeta al principio de especialidad, de forma que sólo podrá autorizarse cuando la injerencia esté relacionada con un delito concreto.
- (ii) No pueden autorizarse injerencias prospectivas, es decir, que tengan por objeto prevenir o descubrir delitos de forma indiscriminada o sin base objetiva.
- (iii) La injerencia debe definir su ámbito objetivo y subjetivo conforme al principio de idoneidad.
- (iv) La injerencia está también sujeta a los principios de excepcionalidad y necesidad sólo puede acordarse si no existen otras medidas menos gravosas y sólo cuando sea imprescindible

Por tanto, es cierto que muchos de los déficits de normatividad de la Directiva anulada por el TJUE no se dan en nuestra ordenación nacional al establecer garantías suficientes para que los datos personales conservados por obligación legal están suficientemente protegidos frente al riesgo de abuso ilegal tanto en relación con el acceso a esos datos como en el uso de los mismos. Y esa es la razón por la que esta Sala en anteriores sentencias ha considerado que nuestro ordenamiento en materia de conservación y cesión de datos es conforme con el derecho de la Unión.(...)

### III

Dicha interpretación restrictiva es igualmente conforme con el criterio que viene manteniendo la Agencia Española de Protección de Datos en relación con la actuación de la Policía Judicial, al amparo de los preceptos de la LOPD de 1999, y que se han reiterado en informas más recientes, como el Informe 13/2020, relativo al acceso de la policía judicial a los datos del censo electoral o el Informe 29/2020 referente al Anteproyecto de Ley Orgánica de Protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública.

Como es sabido, esta Agencia ha mantenido desde antiguo un criterio amplio en relación con las comunicaciones de datos a las Fuerzas y Cuerpos

de Seguridad en los supuestos en que desarrollen sus actuaciones como policía judicial, entendiendo que tanto la Ley Orgánica del Poder Judicial como el artículo 22.2 de la Ley Orgánica 15/1999 habilitaban esa comunicación.

No obstante, en aras a garantizar el adecuado cumplimiento de los principios de protección de datos en todos los dictámenes favorables a la comunicación de información se ha puesto de manifiesto la necesidad de que la misma reuniese una serie de requisitos que garantizaban ese cumplimiento.

Así se recogió en el Informe 297/2005, reiterado en muchos posteriores:

## I

“La consulta plantea si resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, la comunicación a los miembros de la Policía judicial por parte de las empresas de telecomunicaciones de los datos contractuales de sus abonados, a fin de que por los mismos pueda procederse a la realización de las investigaciones que sean necesarias para el esclarecimiento de hechos presuntamente delictivos.

Es preciso señalar que el contenido del presente informe se referirá a la adecuación de dicha comunicación a lo dispuesto en la citada Ley Orgánica 15/1999, sin entrar a analizar otras cuestiones relacionadas con derechos cuya garantía no corresponde a esta Agencia, tales como el derecho al secreto de las comunicaciones.

## II

Dicho lo anterior, con carácter previo al análisis del supuesto concreto sujeto a la presente consulta deben analizarse las normas reguladoras de las funciones atribuidas a los miembros de la Policía Judicial, a efectos de determinar el alcance de sus actividades.

En este sentido, conforme dispone el artículo 549.1 de la Ley Orgánica del Poder Judicial, tras la reforma operada por la Ley Orgánica 19/2003, de 23 de diciembre, “corresponden específicamente a las unidades de Policía Judicial las siguientes funciones:

a) La averiguación acerca de los responsables y circunstancias de los hechos delictivos y la detención de los primeros, dando cuenta seguidamente a la autoridad judicial y fiscal, conforme a lo dispuesto en las leyes.

b) El auxilio a la autoridad judicial y fiscal en cuantas actuaciones deba realizar fuera de su sede y requieran la presencia policial.

c) La realización material de las actuaciones que exijan el ejercicio de la coerción y ordenare la autoridad judicial o fiscal.

d) La garantía del cumplimiento de las órdenes y resoluciones de la autoridad judicial o fiscal.

e) Cualesquiera otras de la misma naturaleza en que sea necesaria su cooperación o auxilio y lo ordenare la autoridad judicial o fiscal”.

Del transcrito precepto, que reproduce el texto del antiguo artículo 445.1 de la Ley Orgánica, se desprende que, junto con las funciones encomendadas a la Policía judicial para el cumplimiento de las actuaciones ordenadas por la Autoridad Judicial o el Ministerio Fiscal, existen otras, directamente dirigidas a la averiguación de las actuaciones delictivas y detención de los presuntos responsables, que se llevarán a cabo con carácter previo a la iniciación del correspondiente proceso penal, siendo la finalidad de éstas últimas, precisamente, la determinación de los elementos de convicción precisos para que pueda proceder esa iniciación. En este caso, será obligación de la Policía Judicial poner los hechos en inmediato conocimiento de la Autoridad Judicial o del Ministerio Fiscal.

En lógica correlación con ello, el artículo 2 del Real Decreto 769/1987, de 19 de junio, regulador de la Policía Judicial, establece que “los miembros de las Fuerzas y Cuerpos de Seguridad, en sus funciones de Policía Judicial, desarrollarán los cometidos expresados en el artículo 1, a requerimiento de la Autoridad Judicial, del Ministerio Fiscal o de sus superiores policiales o por propia iniciativa a través de estos últimos, en los términos previstos en los artículos siguientes”. En este mismo sentido, añade el artículo 4 del citado Real Decreto que “todos los componentes de las Fuerzas y Cuerpos de Seguridad, cualquiera que sea su naturaleza y dependencia, practicarán por su propia iniciativa y según sus respectivas atribuciones, las primeras diligencias de prevención y aseguramiento así que tengan noticia de la perpetración del hecho presuntamente delictivo, y la ocupación y custodia de los objetos que provinieren del delito o estuvieren relacionados con su ejecución, dando cuenta de todo ello en los términos legales a la Autoridad Judicial o Fiscal, directamente o a través de las Unidades Orgánicas de Policía Judicial”.

### III

Sentado este marco normativo, la presente consulta tiene por objeto delimitar el alcance de la posible cesión de datos de carácter personal a los efectivos de la Policía Judicial que la solicitan en ejercicio de sus actividades.

Para resolver esta cuestión no será posible estar a la Resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de 28 de septiembre de 2004, aportada junto con la consulta, dado que la habilitación otorgada en dicha Resolución a la Dirección General de la Policía y a la Dirección General de la Guardia Civil lo es al amparo de lo dispuesto en el artículo 38.5 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y en la Orden CTE/711/2002, de 26 de marzo.

De este modo, la citada Resolución autoriza la comunicación de datos de abonados a los citados Órganos en tanto prestan servicios de atención de llamadas de urgencia a través de los números 091 y 062 y no atiende a las funciones atribuidas a los integrantes de los mismos por el artículo 549.1 de la Ley Orgánica del Poder Judicial.

Precisamente por este motivo, el apartado segundo de la resolución dispone que “los datos obtenidos serán utilizados exclusivamente como soporte para una efectiva prestación de los servicios de atención de llamadas de urgencia”, aclarando el apartado tercero que las entidades estarán sometidas a lo dispuesto en la Ley Orgánica 15/1999, cuyo artículo 4.2 dispone que “Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”, habiendo considerado la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que el término “incompatibles”, incluido en el precepto deberá ser objeto de una interpretación restrictiva, de modo que los datos no podrán ser objeto de tratamiento para otros fines distintos de los que motivaron su recogida.

#### IV

No obstante, será posible analizar la cuestión planteada directamente a la luz de lo dispuesto en la Ley Orgánica 15/1999, sin tener en consideración la autorización otorgada por el Acuerdo al que acaba de hacerse referencia.

Para ello deberán distinguirse aquellas actuaciones de la Policía Judicial que son llevadas a cabo en cumplimiento de un mandato judicial o de un requerimiento efectuado por el Ministerio Fiscal de aquéllas

otras que se llevan a cabo por propia iniciativa o a instancia de su superior jerárquico.

Respecto de las primeras resulta aplicable el artículo 11.2 d) de la Ley Orgánica 15/1999, no requiriéndose el consentimiento del interesado a la cesión, por cuanto los efectivos de la Policía Judicial solicitantes de los datos no son sino meros transmisores de la solicitud efectuada por el Ministerio Fiscal o el Órgano Jurisdiccional, actuando éste en el cumplimiento de las funciones que le han sido legalmente atribuidas y siendo el propio Juzgado o Tribunal o el Ministerio Fiscal el destinatario de los datos cedidos, como exige el artículo referido.

El problema se plantea, sin embargo, en relación con aquellos supuestos en los que la Policía Judicial requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del responsable, al no existir en ese caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión.

En este caso nos encontramos, a nuestro juicio, ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Resultará, en consecuencia, aplicable a este segundo supuesto lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999, según el cual “La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad”

El citado artículo habilita, a nuestro juicio, a los miembros de la Policía Judicial para la obtención y tratamiento de los datos requeridos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando, como se indica en el informe de la Comisaría General de la Policía Judicial adjunto a la consulta y esta Agencia Española de Protección de Datos ha venido indicando reiteradamente, se cumplan las siguientes condiciones:

a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y

que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.

b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.

c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.

d) Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados “cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento”.

Con referencia a la última de las conclusiones señaladas, debe indicarse que, tratándose de actuaciones llevadas a cabo en el ámbito de las competencias consagradas en el apartado a) del artículo 445.1 de la Ley Orgánica del Poder Judicial, encontrándose por ello la Policía Judicial obligada a dar cuenta de los hechos a la Autoridad Judicial y Fiscal de forma inmediata, deberá procederse a la destrucción del registro de los datos obtenidos, una vez producida esa comunicación.

A mayor abundamiento, debe recordarse que, conforme dispone el artículo 11.2 d) de la Ley Orgánica 15/1999, procederá la cesión si ésta tiene por destinatario al Ministerio Fiscal o los Jueces o Tribunales, lo que, conforme se ha señalado, ocurre en el presente supuesto, dada la obligación de los miembros de la Policía Judicial de poner los datos que hayan sido obtenidos en conocimiento de la Autoridad Judicial o Fiscal. Por ello, la cesión solicitada tendrá amparo no sólo en el artículo 22.2 de la Ley Orgánica 15/1999, sino también en el propio artículo 11.2 d) de la misma.

## V

En virtud de todo lo cual, cabe concluir que procede la cesión de los datos que solicite la Policía Judicial, bien por aplicación del artículo 11.2 d), bien del artículo 22 de la Ley Orgánica 15/1999, si bien, en este último supuesto, la solicitud deberá cumplir las condiciones manifestadas en el apartado IV del presente informe.”

Dicho criterio amplio solo cedía en los supuestos en que una norma especial exige la intervención judicial. En este sentido, se pronuncia el informe 330/2013 en relación con un requerimiento de información de la policía judicial a la Tesorería General de la Seguridad Social, en el que después de transcribir el Informe 297/2005, se añadía:



“El presente supuesto, sin embargo, presenta una importante peculiaridad frente a los referidos, con carácter general, en el citado informe y en otros muchos formulados por esta Agencia, dado que las normas reguladoras de los tratamientos y ficheros de los que procederían los datos, que deben ser consideradas *lex specialis* frente a la ley general, que en este caso sería la Ley Orgánica 15/1999, establecen normas específicas relacionadas con los supuestos en que será posible la comunicación de los datos.

Así, el artículo 66 del Texto Refundido de la Ley General de la Seguridad Social, aprobada por Real Decreto Legislativo 1/1994, de 22 de junio, especifica taxativamente los supuestos en los que procederá la comunicación de los datos, informes o antecedentes obtenidos por la Administración de la Seguridad Social en el ejercicio de sus funciones, toda vez que indica la Ley que los mismos “tienen carácter reservado y sólo podrán utilizarse para los fines encomendados a las distintas entidades gestoras y servicios comunes de la Seguridad Social, sin que puedan ser cedidos o comunicados a terceros”. Entre estos supuestos, a los efectos que interesan al presente caso se encontraría (letra a), la cesión que tuviera por objeto “la investigación o persecución de delitos públicos por los órganos jurisdiccionales, el Ministerio Público o la Administración de la Seguridad Social”.

De este modo, el legislador ha querido limitar, por una parte, los supuestos de cesión de los datos a los que estamos haciendo referencia y, por otra, que cuando se trate de la investigación criminal la cesión no se produzca a las Fuerzas y Cuerpos de Seguridad, sino directamente al órgano jurisdiccional o al Ministerio Fiscal.

Por este motivo, y sin perjuicio del criterio general manifestado por esta Agencia en anteriores informes, en el supuesto concreto al que se refiere el presente caso será preciso que el acceso se produzca o bien por el órgano jurisdiccional o por la consultante, contando no obstante para ello con el correspondiente mandamiento judicial al afectado”.

En idéntico sentido se pronunció poco después esta Agencia en relación con la información tributaria, atendiendo a lo dispuesto en el artículo 95 de la LGT, en el Informe 423/2013:

“El presente supuesto, sin embargo, presenta una importante peculiaridad frente a los referidos, con carácter general, en el citado informe y en otros muchos formulados por esta Agencia, dado que las normas reguladoras de los tratamientos y ficheros de los que procederían los datos, que deben ser consideradas *lex specialis* frente a la ley general, que en este caso sería la Ley Orgánica 15/1999,

establecen normas específicas relacionadas con los supuestos en que será posible la comunicación de los datos.

Así, el artículo 95 de la Ley 58/2003, de 17 de diciembre, General tributaria, especifica taxativamente los supuestos en los que procederá la comunicación de los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones, toda vez que indica la Ley que los mismos “tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros”. Entre estos supuestos, a los efectos que interesan al presente caso se encontraría (letra a), la cesión que tuviera por objeto “la colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada”.

Este régimen resulta igualmente aplicable a las entidades locales cuando se trata de datos de naturaleza tributaria, dado que el artículo 2 de la Ley reguladora de las Haciendas Locales dispone que “para la cobranza de los tributos y de las cantidades que como ingresos de Derecho público debe percibir la Hacienda de las Entidades locales, de conformidad con lo previsto en el apartado anterior, dicha Hacienda ostentará las prerrogativas establecidas legalmente para la Hacienda del Estado, y actuará, en su caso, conforme a los procedimientos administrativos correspondientes”.

De este modo, el legislador ha querido limitar, por una parte, los supuestos de cesión de los datos tratados en el ejercicio de la potestad tributaria y, por otra, que cuando se trate de la investigación criminal la cesión no se produzca a las Fuerzas y Cuerpos de Seguridad, sino directamente al órgano jurisdiccional o al Ministerio Fiscal.

Por este motivo, y sin perjuicio del criterio general manifestado por esta Agencia en anteriores informes, en el supuesto concreto al que se refiere el presente caso será preciso que el acceso se produzca o bien por el órgano jurisdiccional o por la consultante, contando no obstante para ello con el correspondiente mandamiento judicial al afectado”.

Igualmente, en relación con los datos de la historia clínica, y atendiendo a lo dispuesto en el artículo 16.3 de Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en el Informe 60/2017 se razonaba lo siguiente:

“El art. 16.3 de dicha norma, en lo que concierne al caso establece:

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

De la misma manera que ya hemos mencionado que establece el art. 11.2 c) LOPD, esta ley requiere que el acceso a los datos clínicos quede restringido a lo que dispongan los jueces y tribunales en el proceso correspondiente, y en todo caso limitado estrictamente a los fines específicos de cada caso. Si la autoridad judicial requiriese una determinada información de dichos datos clínicos, le corresponde a dicha autoridad judicial el análisis de su pertinencia al caso concreto.

## V

Todo lo anteriormente citado está en consonancia con el principio de proporcionalidad que se contiene en el artículo 4.1 LOPD, que dice: 1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

En definitiva, y sin perjuicio de que pueda existir un mandamiento judicial o solicitud del ministerio fiscal en el ejercicio de sus funciones que las fuerzas y cuerpos de seguridad estén ejecutando en su función de policía judicial, no se considera de conformidad con la legislación de protección de datos una solicitud por parte de dichas fuerzas de seguridad relativa a la información médica de la posible víctima que vaya más allá de lo estrictamente necesario y pertinente para determinar la situación del lesionado en relación con el delito público que la ley de

enjuiciamiento criminal obliga a denunciar al profesional médico cuando una persona hubiere sido víctima de lesiones, y que se contiene en el Parte Judicial de Lesiones. En estos casos, y salvo que hubiera mandamiento judicial o solicitud del ministerio fiscal, se considera necesario el consentimiento del afectado para la entrega de la información médica a que hace referencia la consulta”.

Por consiguiente, en los supuestos en que existe una norma especial que regula el acceso a determinados datos personales, debe estarse a lo dispuesto en dicha norma. Como puede observarse, en las normas citadas en los anteriores informes se equipara, en determinados supuestos, el régimen de acceso a los datos personales por los órganos jurisdiccionales y el Ministerio Fiscal para la investigación y persecución de los delitos públicos, e incluso existen otras normas en las que se incluye específicamente a la policía judicial, como la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, cuyo artículo 7 señala que “1. Los datos contenidos en la base de datos objeto de esta Ley sólo podrán utilizarse por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas de la Policía y de la Guardia Civil en el ejercicio de las funciones previstas en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, así como por las Autoridades Judiciales y Fiscales, en la investigación de los delitos enumerados en la letra a) del apartado primero del artículo 3 de esta Ley”.

Partiendo del criterio sostenido por esta Agencia y que, como se ha indicado, se recogió en el Informe 29/2020 relativo al Anteproyecto de Ley por el que se transponía la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales regula en su artículo 7 la colaboración con las autoridades competentes, y, en particular, los requisitos para la colaboración con la Policía Judicial, señalando lo siguiente:

#### Artículo 7. Deber de colaboración.

1. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. **La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el**

**artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.**

**La comunicación de datos, informes, antecedentes y justificantes por la Administración Tributaria, la Administración de la Seguridad Social y la Inspección de Trabajo y Seguridad Social, se efectuará de acuerdo con su legislación respectiva.**

2. En los restantes casos, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

**3. No será de aplicación lo dispuesto en los apartados anteriores cuando legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.**

[...]

#### IV

Por último, ante de proceder al análisis concreto del texto remitido, debe recordarse la postura que ha venido manteniendo esta Agencia respecto del acceso a los datos del Fichero de Titularidades Financieras.

En este sentido, ya en el **Informe 590/2009, referente al artículo 41 del Anteproyecto de Ley de Prevención del blanqueo de capitales y de la financiación del terrorismo** y que venía a regular, por vez primera, el denominado “Fichero de titularidades financieras”, se manifestaba lo siguiente:

#### IV

En cuanto a las cesiones de datos a las que se refiere el precepto sometido a informe, es preciso tener en consideración lo ya apuntado con anterioridad en relación con el necesario cumplimiento de los principios contenidos en la Ley Orgánica 15/1999 y, en particular, el de proporcionalidad.

Tomando en cuenta lo anterior, cabe considerar que la comunicación de los datos a los órganos jurisdiccionales y al Ministerio Fiscal, así como a las Fuerzas y Cuerpos de Seguridad cuando exista previa autorización judicial, con la finalidad de la investigación de los delitos relacionados con la prevención de capitales y la financiación del terrorismo ya se encontraría planamente amparada por el artículo 11.2 d) de la Ley Orgánica 15/1999 que legitima la cesión de datos sin consentimiento del interesado a los órganos judiciales y al Ministerio Fiscal, habiendo señalado esta Agencia que en caso de existir autorización judicial debe entenderse incluida en este supuesto la cesión de datos a la policía judicial.

En cuanto al acceso a los datos por el Servicio Ejecutivo, y sin perjuicio de lo ya indicado en cuanto a la posible atribución a éste de la condición de responsable del fichero, debe señalarse que dicho acceso también se encontraría amparado por las funciones atribuidas al aquél por el Anteproyecto en que se incluye el precepto ahora sometido a informe. En particular, debe recordarse que corresponde al Servicio Ejecutivo prestar el necesario auxilio a los órganos judiciales, al Ministerio Fiscal, a la Policía Judicial y a los órganos administrativos competentes. Por tanto, la cesión se encontraría amparada por el artículo 11.2 a) de la Ley Orgánica 15/1999, siendo congruente y proporcional a las funciones que el ordenamiento atribuye al Servicio Ejecutivo.

Por último, el precepto prevé que los datos serán comunicados a la Agencia Estatal de la Administración Tributaria, que tendrá acceso a los mismos en los términos previstos en la Ley General Tributaria.

El artículo 93.1 de la citada Ley dispone que “Las personas físicas o jurídicas, públicas o privadas, así como las entidades mencionadas en el apartado 4 del artículo 35 de esta ley, estarán obligadas a proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes con trascendencia tributaria relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas”.

Asimismo, conforme al artículo 94.1 “Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas,



estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones”.

Del tenor de ambos preceptos parece desprenderse la existencia de una habilitación legal para la comunicación de los datos a la Administración Tributaria. Ahora bien, debe plantearse si dicha cesión resultaría congruente con la propia estructura y finalidad del fichero, teniendo en cuenta el hecho de que la obligación impuesta a las entidades de crédito por el artículo sometido a informe ya se deriva, en cuanto a las comunicaciones de datos destinadas a la Administración Tributaria de lo dispuesto en la citada Ley General Tributaria.

De este modo, nos encontraríamos ante dos cauces de comunicación de la citada información a un mismo destinatario: una directa y derivada directamente de la Ley general tributaria y otra indirecta, a través del fichero de titularidades financieras creado por el precepto sometido a informe, cuya finalidad no guarda relación con las competencias propias de la Administración Tributaria sino con las relacionadas con la prevención del blanqueo de capitales y la financiación del terrorismo.

Teniendo en cuenta lo anterior, sería preciso plantearse si es realmente necesaria la adopción de una medida como la prevista en el precepto ahora informado, que implica la utilización del fichero para fines distintos de los que justifican su existencia, dado que los mismos datos habrán de ser comunicados directamente a la Administración Tributaria por las entidades financieras. De este modo, únicamente si cabe apreciar el carácter complementario de las dos cesiones podría mantenerse la que se incluye en el apartado 3 del precepto.

Posteriormente, en **el informe 41/2018, referente al Anteproyecto de Ley por la que se modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo**, y ante las modificaciones que se introducían en la regulación del Fichero, singularmente, la supresión de la autorización judicial, esta Agencia se opuso manifestando lo siguiente:

## VIII

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

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

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

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

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

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

– respecto del cliente-titular de la cuenta y de cualquier persona que pretenda actuar en nombre del cliente: el nombre y los apellidos, complementados con los demás datos de identificación requeridos por las disposiciones nacionales que incorporen el artículo 13, apartado 1, letra a), o con un número de identificación único;

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

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

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

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

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

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

con independencia de las que corresponden a esta Agencia, se prevén en el apartado 4 del artículo 43.

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

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

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

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

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

vulnera dichos preceptos, por lo que la declara inválida (sentencia de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y otros).

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

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

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

Se concluye así que “una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva

2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta (apartado 107), siendo sin embargo conforme al Derecho de la Unión “una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido” (apartado 108), para lo que la norma nacional “debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso. Debe indicar, en particular, en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, garantizando que tal medida se limite a lo estrictamente necesario (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 54 y jurisprudencia citada)” (apartado 109). El apartado 11 señala que la delimitación del colectivo afectado “puede garantizarse mediante un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos, que existe un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas”.

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

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



conservados (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 61)” (apartado 118).

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

## IX

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

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

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

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

Así, en primer lugar, se prevé una ampliación de la finalidad del fichero a la persecución de los delitos precedentes al blanqueo o la financiación

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

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

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

X

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

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

La Oficina de Recuperación y Gestión de Activos se encuentra regulada por la Disposición adicional sexta de la Ley de Enjuiciamiento Criminal, introducida por el apartado dieciocho del artículo único de la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales. El apartado 1 de la citada disposición señala en su primer párrafo que “la Oficina de Recuperación y Gestión de Activos es el órgano administrativo al que corresponden las funciones de localización, recuperación, conservación, administración y realización de efectos procedentes de actividades delictivas en los términos previstos en la legislación penal y procesal”. El párrafo segundo de dicho apartado 1 añade que “cuando sea necesario para el desempeño de sus funciones y realización de sus fines, la Oficina de Recuperación y Gestión de Activos podrá recabar la colaboración de cualesquiera entidades públicas y privadas, que estarán obligadas a prestarla de conformidad con su normativa específica”.

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

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

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

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

- b) Recibir de las Administraciones Públicas y personas obligadas la información relacionada con el bloqueo de la financiación de actividades del terrorismo a que se refiere el artículo 4 de la Ley 12/2003, de 21 de mayo.
- c) Recibir y tramitar, conforme a las normas de este Reglamento, las solicitudes de autorización de liberación o puesta a disposición de fondos o recursos económicos bloqueados en ejecución de un acuerdo de la Comisión.
- d) Recibir y tramitar las peticiones de supresión de personas y entidades de las listas de terroristas elaboradas por la Unión Europea y Naciones Unidas.
- e) Elaborar informes que permitan a la Comisión decidir sobre las solicitudes de verificación de identidad a que se refiere el artículo 12.
- f) Cualesquiera otras tareas que le encomiende la Comisión.”

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

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

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

ese supuesto sería posible considerar amparado en los principios de minimización y proporcionalidad el mencionado acceso.

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

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

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

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

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

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

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

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

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

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

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

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

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

Más recientemente, en **el Informe 83/2020 referente al Anteproyecto de Ley por la que se modifica la ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo**, cuyo objetivo básico era la transposición de la 5ª Directiva en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, esta Agencia reiteró su criterio contrario a la supresión de la autorización judicial para el acceso a los datos del Fichero de Titularidades Financieras. En este sentido, después de señalar que la modificación del art. 43 LPBC, relativo al Fichero de Titularidades Financieras, respondía a la introducción en la Directiva 2015/849 del art. 32 bis por la Directiva 2018/843, relativo a la necesidad por los Estados miembros de mecanismos centralizados automatizados, como registros o sistemas centrales electrónicos de consulta de datos, que permitan la identificación, en tiempo oportuno, de cualquier persona física o jurídica que posea o controle cuentas de pago y cuentas bancarias y cajas de seguridad en una entidad de crédito, si bien se introducían otras modificaciones no derivadas de la Directiva 2018/843, destacaba lo siguiente:



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

[...]

Asimismo, el **Consejo General del Poder Judicial** se opuso a la supresión de dicho requisito en su **Informe de 17 de diciembre de 2020**, señalando lo siguiente:

119.- Especial significación tiene la nueva redacción dada al apartado 3 del artículo 43 LPBCFT que regula el acceso al FTF. Un primer aspecto relevante es que se elimina la previsión vigente que condiciona el acceso de las Fuerzas y Cuerpos de Seguridad a los datos obrantes en el FTF a la obtención de «previa autorización judicial o del Ministerio Fiscal». La V Directiva, que prevé en su artículo 32 bis la obligación de los Estados miembros de crear un instrumento del tipo FTF, nada dice respecto del condicionamiento a autorización judicial previa, y tan sólo se ordena que la información «sea directamente accesible» por las Unidades de Inteligencia Financiera y las autoridades competentes.

120.- En el estado actual de la normativa europea es claro que el prelegislador no puede invocar la existencia de una norma del Derecho de la Unión Europea que impida condicionar el acceso al FTF por parte de las Fuerzas y Cuerpos de Seguridad a la previa obtención de autorización judicial. En este punto la previsión del Anteproyecto debe evaluarse a partir de su compatibilidad con las garantías constitucionales de los derechos fundamentales que pueden resultar afectados por este tipo de acceso a datos personales.

121.- La valoración sostenida en el informe de 25 de abril de 2018 respecto de una previsión sustancialmente idéntica a la contenida en el Anteproyecto debe ser corregida en un sentido más garantista. En esta materia que afecta al ámbito de reserva sobre informaciones relativas al desarrollo de la vida privada de las personas en el contexto de la transposición de una Directiva, la doble filiación de los derechos al respeto de la esfera personal consagrados en el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea y en el artículo 18.1 de nuestra Constitución determina una concurrencia de estándares de protección. En esta tesitura, y sin perjuicio de la conocida doctrina Melloni (sentencia del Tribunal de Justicia de 26 de febrero de 2013, C-399/11), a la vista de la reciente STC 26/2020, de 24 de febrero (FJ 6), resulta más prudente sostener la preferencia de aquel estándar que

resulte más protector del derecho concernido. Por ello, desde esta perspectiva iusfundamental, la supresión proyectada de la garantía consistente en la autorización judicial previa al acceso al FTF por parte de los Cuerpos y Fuerzas de Seguridad debe ser valorada desfavorablemente.

122.- En relación con la denominada intimidad económica, la doctrina del Tribunal Constitucional ha sostenido que no sólo los movimientos de una cuenta bancaria se encuentran en el ámbito de protección del derecho a la intimidad del artículo 18.1 de la C.E., sino todos aquellos referentes a su situación económica: «No hay duda –afirma el Alto Tribunal- de que los datos relativos a la situación económica de una persona entran dentro del ámbito de la intimidad constitucionalmente protegido, menos aún puede haberla de que la información concerniente al gasto en que incurre un obligado tributario, no sólo forma parte de dicho ámbito, sino que a través de su investigación o indagación puede penetrarse en la zona más estricta de la vida privada o, lo que es lo mismo, en «los aspectos más básicos de la autodeterminación personal» del individuo» (STC 233/2005, de 26 de septiembre, FJ 4, con cita de otras muchas).

123.- Con base en este criterio jurisprudencial de delimitación del ámbito protegido por el derecho fundamental a la intimidad, no parece difícil argumentar que los datos contenidos en el FTF son exhaustivamente definitorios de la situación económica de una persona y de sus relaciones negociales con otras muchas (apoderados, gestores, administradores, familiares, etc.), y más aún si se considera que los datos identificativos pueden ser ampliados por vía reglamentaria.

124.- El acceso por parte del poder público a información que se integra en el ámbito protegido por el derecho a la intimidad requiere, como regla general, autorización judicial. Como ha puesto de manifiesto el Tribunal Constitucional, «entre los requisitos para determinar la legitimidad de la injerencia en el derecho a la intimidad reconocido en el art. 18.1 CE hemos reclamado en varias ocasiones la existencia de resolución judicial previa; pero no es menos cierto que sólo hemos exigido dicha decisión «como regla general» [STC 71/2002, de 3 de abril, FJ 10 a)]. En efecto, hemos señalado que, «a diferencia de lo que ocurre con otras medidas restrictivas de derechos fundamentales que pueden ser adoptadas en el curso del proceso penal (como la entrada y registro en domicilio del art. 18.2 CE o la intervención de comunicaciones del art. 18.3 CE), respecto de las restricciones del derecho a la intimidad (art. 18.1 CE) no existe en la Constitución reserva absoluta de previa resolución judicial» [SSTC 234/1997, de 18 de diciembre, FJ 9, in fine; 70/2002, de 3 de abril, FJ 10.b.3; en el mismo sentido, STC 207/1996, de 16 de diciembre, FJ 4 c)]. De manera que, en la medida en que no se establece en el art. 18.1 CE reserva alguna de resolución judicial, como hemos señalado en otras ocasiones, «no es constitucionalmente exigible que sea el Juez quien tenga que autorizar esta medida limitativa, pudiéndola adoptar, siempre que una ley

expresamente la habilite, la autoridad que, por razón de la materia de que se trate, sea la competente» (STC 234/1997, de 18 de diciembre, FJ 9, in fine)» (STC 233/2005, FJ 7).

125.- Pues bien, el proyectado artículo 43.3 se refiere a la limitación del derecho a la intimidad «con ocasión de la investigación de los delitos relacionados con el blanqueo de capitales o la financiación del terrorismo», es decir, en el curso de una instrucción penal cuya única autoridad competente es el Juez de Instrucción de acuerdo con la Ley de Enjuiciamiento Criminal, siendo a este órgano jurisdiccional al que debe corresponder valorar los principios de necesidad, motivación, excepcionalidad, idoneidad, especialidad y proporcionalidad concurrentes en la adopción de una medida restrictiva de un derecho fundamental como el de la intimidad personal. Por ello, la previsión contemplada en el Anteproyecto no merece un juicio favorable al tener como resultado que la genuina función judicial de ponderar derechos e intereses en juego sea sustituida en el seno de la investigación del delito por la Policía.

## V

Procediendo ya al análisis de las principales cuestiones que, desde la perspectiva de la protección de datos plantea la transposición de la Directiva 2019/1153 (UE) mediante el Anteproyecto de Ley Orgánica, debe partirse, necesariamente, de la existencia de un régimen jurídico consolidado respecto de los tratamientos de datos personales que se contienen en el Fichero de Titularidades Financieras, incluidas las garantías específicas para el acceso a los datos que figuran en el mismo por las autoridades competentes.

La creación del Fichero de Titularidades Financieras fue prevista, en primer término, por el artículo 43 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Informe AEPD 590/2009), desarrollándose su régimen jurídico por la Sección Tercera del Capítulo V del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Informe AEPD 27/2014), y cuya disposición transitoria primera preveía que su entrada en funcionamiento se produjera en la fecha que se determinara por Orden del Ministro de Economía y Competitividad, que fue fijada el 6 de mayo de 2016 por la Orden ECC/2314/2015, de 20 de octubre, por la que se determina la fecha de entrada en funcionamiento del Fichero de Titularidades Financieras.

Asimismo, se han aprobado la Orden ECC/2503/2014, de 29 de diciembre, por la que se crea el fichero de datos de carácter personal denominado “Fichero de Titularidades Financieras” (Informe AEPD 498/2014), la Instrucción de 19 de diciembre de 2014, de la Secretaría de Estado de

Economía y Apoyo a la Empresa, por la que se establecen los datos de identificación adicionales que deben ser declarados por las entidades de crédito al Fichero de Titularidades Financieras, a fin de la adecuada identificación de intervinientes, cuentas y depósitos (Informe AEPD 499/2014), y la Instrucción de 2 de julio de 2015, de la Secretaría de Estado de Economía y Apoyo a la Empresa, por la que se establecen los requisitos mínimos que deben cumplir las solicitudes de datos del Fichero de Titularidades Financieras, efectuadas a través de los puntos únicos de acceso (Informe AEPD 238/2015).

Asimismo, las sucesivas modificaciones de la Ley 10/2010 han sido igualmente informadas por esta Agencia, tal y como se ha señalado anteriormente, informándose con carácter desfavorable, tanto en el Informe 41/2018 como en el 83/2020 la supresión de la preceptiva autorización judicial para el acceso a los datos del Fichero.

Por consiguiente, España cuenta ya, incluso con anterioridad a que se previera con carácter general en la Quinta Directiva, con un registro centralizado de cuentas bancarias, el Fichero de Titularidades Financieras, plenamente operativo desde el 6 de mayo de 2016 con un régimen jurídico que incluye garantías específicas, que han sido oportunamente informadas, entre otros órganos consultivos, por esta Agencia, y en el que, según informa en su página web el SEPBLAC se encuentran actualmente las titularidades de más de 130 millones de cuentas y de depósitos.

**Por todo ello, la primera observación que se formula es la necesidad de incluir en el texto remitido las garantías actualmente existentes en la normativa española para el acceso por las autoridades competentes a la información obrante en el Fichero de Titularidades Financieras, que no son incompatibles con la finalidad pretendida por la Directiva (UE) 2019/1153, objeto de transposición, singularmente, la relativa a la necesaria autorización judicial.**

A este respecto, no puede admitirse, tal y como se plantea en la MAIN, que la supresión de dicha autorización judicial cumpla “con el espíritu de la Directiva (UE) 2019/1153, cuando exige que el acceso a la información financiera resulte directo e inmediato”. Al contrario, esta Agencia entiende que la misma es una garantía indispensable en nuestro ordenamiento jurídico para la protección del derecho fundamental a la protección de datos personales, así como del derecho fundamental a la intimidad, sin que sea incompatible con el establecimiento de un régimen de acceso directo e inmediato.

A este respecto, la propia Directiva objeto de transposición prevé en su artículo 4.1 que “El acceso y las consultas también se considerarán inmediatos y directos, entre otros casos, cuando las autoridades nacionales que gestionan los registros centralizados de cuentas bancarias transmitan rápidamente la información sobre las cuentas bancarias a las autoridades competentes

mediante mecanismos automatizados, siempre que ninguna entidad intermediaria pueda interferir en los datos solicitados o en la información que se haya de proporcionar”.

Por consiguiente, el acceso directo e inmediato queda garantizado con la transmisión de la información mediante mecanismos automatizados en los que ninguna entidad intermediaria interfiera, lo que no es incompatible con la previa obtención de la correspondiente autorización judicial.

A estos efectos, basta con recordar que la Directiva 2018/843, cuando introdujo en la Directiva 2015/849 el art. 32 bis relativo a la necesidad por los Estados miembros de mecanismos centralizados automatizados, como registros o sistemas centrales electrónicos de consulta de datos, que permitan la identificación, en tiempo oportuno, de cualquier persona física o jurídica que posea o controle cuentas de pago y cuentas bancarias y cajas de seguridad en una entidad de crédito, ya preveía en su párrafo 2 ese acceso directo e inmediato, al señalar que

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

Y no obstante dicha previsión, tanto esta Agencia como el CGPJ informaron negativamente la supresión del requisito de la previa autorización judicial, que se ha mantenido en el artículo 43 tras la reforma operada por el Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores y por el que se ha procedido a la transposición de la Quinta Directiva.

## **VI**

En segundo lugar, procede analizar la identificación de las autoridades competentes a los efectos de la misma que se contiene en el artículo 3.



A este respecto, la Directiva deja un importante margen de apreciación a los Estados miembros, atendiendo a las competencias atribuidas por su normativa nacional, señalando en su Considerando 9 *in fine* que “[...] Al aplicar la presente Directiva, los Estados miembros deben tener en cuenta la naturaleza, el estatuto organizativo, las funciones y las prerrogativas de dichas autoridades y organismos de acuerdo con lo establecido en su Derecho nacional, incluidos los mecanismos existentes para la protección de los sistemas financieros contra el blanqueo de capitales y la financiación del terrorismo.”

Asimismo, dichas autoridades competentes no han de coincidir, necesariamente, con las autoridades competentes a efectos de la prevención, detección, investigación o enjuiciamiento de infracciones penales, designadas de conformidad con la Directiva 2016/680 y que se recogen en el artículo 4 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ya que como señala el artículo 3 de la Directiva 2019/1153 “Cada Estado miembro designará, **de entre** sus autoridades competentes a efectos de la prevención, detección, investigación o enjuiciamiento de infracciones penales, a las autoridades competentes facultadas para acceder a su registro nacional centralizado de cuentas bancarias, y consultarlo”.

Por otro lado, en dicha designación debe tenerse especialmente en cuenta el principio de proporcionalidad, al que se refiere específicamente el Considerando 9: “Dado que en cada Estado miembro existen numerosas autoridades u organismos competentes para la prevención, detección, investigación o enjuiciamiento de infracciones penales, y **para garantizar un acceso proporcionado** a la información financiera y de otro tipo en el marco de la presente Directiva, se debe requerir a los Estados miembros para que designen a las autoridades u organismos que están facultados para acceder a los registros centralizados de cuentas bancarias y pueden recabar información de las UIF a los efectos de la presente Directiva.”

A juicio de esta Agencia, para aplicar dicha proporcionalidad debe tenerse muy en cuenta la importancia de la información que se contiene en el Fichero, conteniendo numerosos datos relativos a las personas físicas y que afectan singularmente a su privacidad, al permitir inferir información relativa a su intimidad, así como el hecho de que se ha ampliado el ámbito del acceso, que ya no se limita a los delitos de prevención del blanqueo de capitales o financiación del terrorismo, extendiéndose a los delitos graves.

**Por todo ello, deberá limitarse el acceso a las autoridades estrictamente indispensables, lo que se debería justificar adecuadamente en la memoria. Asimismo, en cuanto al acceso por parte de las Fuerzas y Cuerpos de Seguridad del Estado, Policías Autonómicas y Vigilancia**



**Aduanera, debería limitarse a su actuación como Policía Judicial. Y, en todo caso, supeditarla a la previa obtención de la correspondiente autorización judicial, conforme a lo indicado en el apartado anterior.**

## VI

El artículo 12 del anteproyecto lleva por rúbrica “Protección de datos de carácter personal”, y comienza haciendo referencia a la normativa aplicable, señalando lo siguiente:

- c. El tratamiento de datos de carácter personal, en aplicación de esta ley  
orgánica, estará a lo dispuesto en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Por su parte, la Directiva objeto de transposición recuerda en su Considerando 25 que “Es fundamental garantizar que el tratamiento de los datos personales en virtud de la presente Directiva respete plenamente el derecho a la protección de los datos personales. Dicho tratamiento está sujeto a lo dispuesto en el Reglamento (UE) 2016/679 y en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, en sus respectivos ámbitos de aplicación. En lo que respecta al acceso de los organismos de recuperación de activos a los registros centralizados de cuentas bancarias y a los sistemas de recuperación de datos, será de aplicación la Directiva (UE) 2016/680, mientras que el artículo 5, apartado 2, de la Decisión 2007/845/JAI del Consejo no debe aplicarse [...]”

Asimismo, la Exposición de motivos del anteproyecto se refiere a la normativa aplicable en materia de protección de datos personales, señalando lo siguiente:

Dado el carácter sensible de los datos financieros, debe establecerse, de manera específica, el tipo y alcance de la información susceptible de intercambio para lograr un equilibrio entre la eficiencia y la protección de los datos personales. Para ello, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención,

detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales; y en la Ley 10/2010, de 28 de abril.

[...]

El capítulo IV establece una serie de disposiciones suplementarias relativas al tratamiento de los datos personales derivadas de la aplicación de la Ley Orgánica 7/2021, de 26 de mayo, así como del Reglamento General de Protección de Datos y de la Ley Orgánica 3/2018, de 5 de diciembre, que adapta el Reglamento en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

A este respecto, procede traer a colación lo manifestado por esta Agencia en el Informe 29/2020 referente al Anteproyecto de Ley Orgánica de Protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública, en el que se señalaba cómo la Directiva 2016/680 del Parlamento Europeo y del Consejo, cuya transposición se lleva a cabo por el presente Anteproyecto de Ley, “viene a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el Reglamento general de protección de datos. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento”.

Asimismo, en dicho informe se destacaba la necesidad de deslindar entre la normativa aplicable a los sujetos a los que el ordenamiento jurídico imponga un específico deber de colaboración con las autoridades competentes, quedando sometidos los tratamientos de datos personales al RGPD y a la LOPDGGDD, de los tratamientos que puedan realizar las autoridades competentes una vez que se les han comunicado los datos, que quedarían sujetos a la normativa de transposición de la Directiva (UE) 2016/680, recordando lo que ya se había dicho en el Informe 122/2018, relativo a una versión anterior del Anteproyecto:

En relación con esta previsión, debe indicarse que el tratamiento de datos llevado a cabo por las entidades sometidas al Reglamento general de protección de datos se regirá por éste, junto con la normativa que adapte el derecho interno a sus previsiones. Ciertamente el artículo 6.1 c) del reglamento habilita el tratamiento de los datos de carácter personal cuando se encuentre previsto en una disposición con rango legal, pero ello no supone que dicha disposición desplace las previsiones

del Reglamento en lo que atañe al tratamiento llevado a cabo por ese responsable.

De este modo, no es dable al legislador nacional establecer restricciones en lo que afecta a la atención de los derechos en relación con el tratamiento que lleve a cabo el responsable, sin perjuicio de las que pudieran proceder una vez comunicados los datos a las autoridades competentes cuando el derecho se ejercite ante las mismas. Del mismo modo, las entidades sometidas al ámbito de aplicación del Reglamento lo son también al régimen de reclamaciones, responsabilidad y sanciones impuesto por el mismo, sin que sea posible considerar que respecto del tratamiento primigeniamente llevado a cabo por el responsable no serán de aplicación las normas del Reglamento.

En este sentido, el considerando 11 de la Directiva señala que “Conviene por lo tanto que esos ámbitos estén regulados por una directiva que establezca las normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Entre dichas autoridades competentes no solo se deben incluir autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, sino también cualquier otro organismo o entidad en que el Derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva. Cuando dicho organismo o entidad trate datos personales con fines distintos de los previstos en la presente Directiva, se aplica el Reglamento (UE) 2016/679. Así pues, el Reglamento (UE) 2016/679 se aplica en los casos en los que un organismo o entidad recopile datos personales con otros fines y proceda a su tratamiento para el cumplimiento de una obligación jurídica a la que esté sujeto. Por ejemplo, con fines de investigación, detección o enjuiciamiento de infracciones penales, las instituciones financieras conservan determinados datos personales que ellas mismas tratan y únicamente facilitan dichos datos personales a las autoridades nacionales competentes en casos concretos y de conformidad con el Derecho del Estado miembro. Todo organismo o entidad que trate datos personales en nombre de las citadas autoridades dentro del ámbito de aplicación de la presente Directiva debe quedar obligado por un contrato u otro acto jurídico y por las disposiciones aplicables a los encargados del tratamiento con arreglo a la presente Directiva, mientras que la aplicación del Reglamento (UE) 2016/679 permanece inalterada para el tratamiento de datos personales por encargados del tratamiento fuera del ámbito de aplicación de la presente Directiva”.

En este mismo sentido, el considerando 34 de la Directiva añade “El tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a amenazas para la seguridad pública, debe abarcar toda operación o conjunto de operaciones con datos personales o conjuntos de datos personales que se lleve a cabo con tales fines, ya sea de modo automatizado o no, y entre las que se incluye la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, utilización, cotejo o combinación, limitación del tratamiento, supresión o destrucción de datos. En particular, las normas de la presente Directiva deben aplicarse a la transmisión de datos personales a los efectos de la presente Directiva a un destinatario que no esté sometido a la misma. Por «destinatario» debe entenderse toda persona física o jurídica, autoridad pública, servicio u otro organismo al que la autoridad competente comunique los datos personales de forma lícita. Si los datos personales fueron recopilados inicialmente por una autoridad competente para alguno de los fines previstos en la presente Directiva, el tratamiento de dichos datos para fines distintos de los previstos en la presente Directiva se regirá por lo dispuesto en el Reglamento (UE) 2016/679, siempre que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. En particular, las normas del Reglamento (UE) 2016/679 deben aplicarse a la transmisión de datos personales con fines no previstos en el ámbito de aplicación de la presente Directiva. Para el tratamiento de datos personales por parte de un destinatario que no sea una autoridad competente o que esté actuando como tal en el sentido de la presente Directiva y a quien una autoridad competente haya comunicado datos personales lícitamente, se estará a lo dispuesto en el Reglamento (UE) 2016/679. Al aplicar la presente Directiva, los Estados miembros deben poder precisar también la aplicación de las normas del Reglamento (UE) 2016/679, con sujeción a las condiciones establecidas en el mismo”.

El ejemplo mencionado en el considerando 11 es expresivo al indicar claramente que el tratamiento llevado a cabo por el sujeto obligado a comunicar los datos a una autoridad competente está sometido a las disposiciones del Reglamento general de protección de datos y no a las de la Directiva, sin perjuicio de que una vez comunicados los datos a la autoridad competente sí será aplicable a ese tratamiento lo establecido en la Directiva, pero sin que esa aplicación implique que el sujeto obligado se encuentra sujeto a las previsiones de ésta última, toda vez que la comunicación se habrá llevado a cabo al amparo del artículo 6.1 c) del reglamento.

En el presente caso, hay que tener en cuenta que los datos no se comunican directamente a las autoridades competentes por las entidades obligadas, sino que se comunican al responsable del Fichero de Titularidades Financieras, que carece de dicha condición. En este sentido, el Fichero de Titularidades Financieras se constituye como consecuencia de la obligación que el artículo 43 de la LPBFC impone a las entidades declarantes, con la finalidad de prevenir e impedir el blanqueo de capitales y la financiación del terrorismo, de declarar al Servicio Ejecutivo de la Comisión la información que determina, actuando dicho Servicio Ejecutivo como mero encargado del tratamiento, ya que el responsable es la Secretaría de Estado de Economía y Apoyo a la Empresa. De ahí que el artículo 43.2 de la LPBCFT prevea que “El tratamiento de los datos personales contenidos en el Fichero de Titularidades Financieras por el Servicio Ejecutivo de la Comisión se regirá por lo establecido en el artículo 28.3 del Reglamento (UE) 2016/679, de 27 de abril de 2016”, sin perjuicio de que “El Servicio Ejecutivo de la Comisión podrá utilizar la información obrante en el mismo para el ejercicio de sus competencias”.

Por consiguiente, es preciso diferenciar, por un lado, en cuanto a la normativa de protección de datos personales aplicable, los tratamientos de datos derivados de la gestión del Fichero de Titularidades Financieras, y que incluyen tanto la comunicación de los datos por las entidades obligadas como la comunicación de los mismos a las autoridades competentes, que quedan sometidos al RGPD y a la LOPDGDD, sin perjuicio de las limitaciones de los derechos de los afectados que se recogen en la propia LPBCFT, admisibles al amparo del artículo 23 del RGPD. Y por otro, los tratamientos de datos personales que puedan realizar las autoridades competentes una vez que se les han comunicado los datos personales, que quedan sometidos a la Ley Orgánica 7/2021.

**Por consiguiente, teniendo en cuenta que el Anteproyecto no solo regula los tratamientos de datos personales, incluidas las comunicaciones de los mismos, entre autoridades competentes, sino que también regula las condiciones en que se puede producir el acceso por partes de las autoridades competentes al Fichero de Titularidades Financieras, debería modificarse el artículo 12 para incluir esta distinción, incluyendo entre la normativa de protección de datos personales aplicable, en su respectivo ámbito, el RGPD y la LOPDGDD, tal y como, expresamente, se prevé en la Exposición de motivos de la norma informada.**

## **VII**

Los apartados 2 y 3 del artículo 12 regulan los tratamientos de categorías especiales de datos, señalando lo siguiente:

2. En el ámbito de aplicación de esta ley orgánica se podrán tratar categorías especiales de datos personales cuando sea necesario para

cumplir con los fines del artículo 1. En las solicitudes de información se motivará esta necesidad y sólo se accederá a la misma en los supuestos en los que tal circunstancia pueda acreditarse.

3. Estos datos sólo podrán ser tratados por las personas que hayan recibido una formación específica y sean individualmente autorizadas para ello, de conformidad con las normas aplicables en materia de protección de datos y de acuerdo con las orientaciones del delegado de protección de datos designado por la autoridad competente.

Dichos preceptos son transposición del artículo 16 de la Directiva (UE) 2019/1153:

#### Tratamiento de datos personales sensibles

1. El tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas de una persona, o la pertenencia a un sindicato, o datos relativos a la salud de una persona física, o a la vida sexual u orientación sexual de una persona únicamente se autorizarán a reserva de las garantías pertinentes en relación con los derechos y libertades del interesado, de conformidad con las normas aplicables en materia de protección de datos.

2. Únicamente las personas que hayan recibido una formación específica y que hayan sido específicamente autorizadas por el responsable del tratamiento podrán acceder a los datos a que se refiere el apartado 1 y tratarlos, conforme a las orientaciones del delegado de protección de datos.

Como puede observarse, el apartado 1 supedita la autorización del tratamiento de dichos datos “a reserva de las garantías pertinentes en relación con los derechos y libertades del interesado, de conformidad con las normas aplicables en materia de protección de datos”.

A este respecto, procede traer de nuevo a colación la doctrina constitucional respecto de los requisitos para el tratamiento de las categorías especiales de datos personales, que se resume en la sentencia del Tribunal Constitucional (STC) 76/2019, de 22 de mayo. Esta sentencia contiene la doctrina relevante de este sobre el derecho fundamental a la protección de datos personales, y aborda tanto las características como el contenido que ha de tener la normativa que pretenda establecer una injerencia en ese derecho fundamental.



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

En consecuencia, y tal y como exige el Tribunal Constitucional, la ley que establezca unas determinadas injerencias en el derecho fundamental a la protección de datos personales de los interesados, como es, en el caso presente, la posibilidad de tratar datos personales de los interesados de categorías especiales, como son datos relativos a su salud, requiere que esta en primer lugar, y para cada tratamiento de datos personales de categorías especiales que contemple:

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

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

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

procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”.

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

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo, F. 5; 55/1996, de 28 de marzo, FF. 7, 8 y 9; 270/1996, de 16 de diciembre, F.4.e; 37/1998, de 17 de, F. 8; 186/2000, de 10 de julio, F. 6).”

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

A este respecto, el texto del Anteproyecto, además de las garantías recogidas en la Directiva y que se transponen en el apartado 3 del artículo 12, relativas a los requisitos de las personas que pueden acceder a los datos, añade en su apartado 2, como garantías específicas, que “En las solicitudes de información se motivará esta necesidad y sólo se accederá a la misma en los supuestos en los que tal circunstancia pueda acreditarse”. Aunque el principio de necesidad, derivado del principio de proporcionalidad, y la necesidad de motivación, es un requisito general aplicable a todos los tratamientos de datos personales regulados por el anteproyecto, esta Agencia valora positivamente que se recalque la necesidad de cumplir con el mismo en relación con los

tratamientos de categorías especiales de datos, exigiendo la oportuna acreditación.

No obstante, y al igual que se señaló en nuestro Informe 29/2020, deberían incorporarse todas las garantías que se estimen adecuadas para salvaguardar el derecho a la protección de datos personales de los afectados, atendiendo al tipo de datos que se tratan y a la finalidad del tratamiento, como pueden ser las de limitar el acceso a los datos que sean estrictamente necesarios (principio de minimización), prohibiendo o limitando su utilización para fines distintos de los originales (principio de limitación de la finalidad), ordenando su supresión cuando dejen de ser necesarios en relación con la finalidad perseguida (principio de limitación del plazo de conservación) o la necesidad de adoptar medidas de seguridad adecuadas al nivel de riesgo derivado del tipo de datos que se tratan. Asimismo, en el apartado 3 podría incluirse el sometimiento del personal que trate dichos datos a un deber específico de secreto.

Al objeto de valorar las garantías específicas que puedan resultar adecuadas al nivel del riesgo del tratamiento de los datos personales para los derechos y libertades de los afectados, esta Agencia viene destacando en sus informes sobre disposiciones normativas la conveniencia de que se realice un análisis de riesgos e, incluso, una Evaluación de impacto en la protección de datos, y que los mismos se incorporen a la MAIN.

Por otro lado, hay que tener en cuenta que la Directiva prevé únicamente el tratamiento de categorías especiales de datos en relación con los supuestos de intercambio de información entre las autoridades competentes y las UIF, y entre UIF, lo que debería precisarse igualmente en el artículo 12.2 del anteproyecto.

## VIII

En cuanto a la disposición final primera del anteproyecto, que modifica el artículo 43 de la LPBCFT, suprimiendo la necesidad de autorización judicial, se **informa negativamente** por esta Agencia, por las razones que se han expuesto con anterioridad.

## IX

Por último, procede hacer una serie de observaciones específicas al articulado del anteproyecto, al no haberse recogido adecuadamente las

garantías que, en relación con la protección de datos de carácter personal, han sido expresamente previstas en la Directiva.

En primer lugar, en el artículo 6, relativo al “Seguimiento del acceso y la consulta”, no se ha recogido la finalidad del registro tal y como se identifica en el artículo 6.3. de la Directiva: “Los registros únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación de la admisibilidad de una solicitud y de la legalidad del tratamiento de los datos, así como para garantizar la seguridad de los datos”. Tampoco se ha recogido la obligación de que los registros “estarán protegidos por medidas adecuadas contra el acceso no autorizado”. Asimismo, no se recoge la obligación del personal del Servicio Ejecutivo de la Comisión de conocer “el Derecho de la Unión y nacional aplicable, incluidos los requisitos aplicables en materia de protección de datos. Tales medidas incluirán programas de formación especializados”.

En relación con las solicitudes de información dirigidas al Servicio Ejecutivo de la Comisión por parte de las autoridades competentes reguladas en el artículo 7, así como en el intercambio de información financiera y análisis financieros con autoridades competentes de Estados miembros de la Unión Europea, no se ha recogido el principio de necesidad que se prevé tanto en el artículo 7.1. como 10.1 al referirse a la circunstancia de “dicha información financiera o dicho análisis financiero sean necesarios”.

El artículo 13, relativo al Registro de solicitudes de información que deben llevar tanto las autoridades competentes como el Servicio Ejecutivo de la Comisión ha reducido el plazo de conservación a un año, cuando el artículo 17 de la Directiva prevé expresamente que dicho plazo ha de ser de 5 años.

**En consecuencia, procede modificar todos los artículos señalados para adecuarlos a las garantías previstas en la Directiva.**