N/REF: 0029/2020

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.

Asimismo, hay que destacar que una versión anterior del presente Anteproyecto fue objeto de estudio por esta Agencia en su informe 122/2018, en el que ya se indicaba cómo, dada su naturaleza, "la práctica totalidad de las disposiciones del mismo se refieren a materias respecto de las que es competente esta Agencia Española de Protección de Datos", razón por la cual se formularon numerosas observaciones, muchas de las cuales se han tenido en consideración en el nuevo texto remitido.

Por lo tanto, el presente informe se centrará, fundamentalmente, en el análisis de las novedades introducidas en el nuevo texto así como, en su caso, a incidir en aquellas observaciones que no se han recogido en el mismo.

I

En el Informe 122/2008, esta Agencia ya destacaba 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, se destacaba que el carácter de norma especial era igualmente predicable respecto de la norma que adapte el derecho español al Reglamento General de Protección de Datos (RGPD), constituida en el presente momento por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), cuyas disposiciones deberían

ser tenidas en cuenta al constituir “la lex generalis aplicable para garantizar el derecho fundamental a la protección de datos de carácter personal”.

Partiendo de las anteriores observaciones, el nuevo texto remitido, ha recogido en su artículo 1.1 relativo al objeto de la Ley el texto que, partiendo del inicialmente recogido en el Anteproyecto, había sido propuesto por esta Agencia, con el objeto de incluir la referencia al derecho fundamental del artículo 18.4 de la Constitución.

No obstante, y ante algunas imprecisiones observadas en el nuevo texto remitido, como ocurre en el artículo 7.2 relativo a las categorías de interesados al que posteriormente se hará referencia, el artículo 1 del Anteproyecto tan sólo puede interpretarse en relación con las infracciones y sanciones penales, de manera que dado que el objeto de la Directiva es regular las normas relativas a la protección de las personas físicas respecto de los tratamientos de sus datos personales por parte de las autoridades competentes con fines de prevención, investigación detección o enjuiciamiento infracciones penales o de ejecución de infracciones penales, “incluidas” la protección y la prevención frente a las amenazas contra seguridad pública, dicha referencia a la prevención frente a las amenazas contra la seguridad pública sólo puede referirse a aquellas amenazas que constituyan delito.

Cualquier tratamiento en relación con la prevención de amenazas a la seguridad pública que puedan constituir infracciones administrativas se regulará conforme al RGPD, que establece mayores derechos para los interesados.

Por ello, se estima necesario que se sustituya en el apartado 1 del artículo 1 la expresión “así como” por “incluidas”, que es la prevista en la Directiva, quedando redactado de la siguiente manera:

> “Esta ley orgánica tiene por objeto regular el derecho fundamental, reconocido por el artículo 18.4 de la Constitución, a la protección de datos personales en relación a los tratamientos de datos llevados a cabo por las autoridades competentes con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, **incluidas la protección y la prevención** frente a las amenazas contra la seguridad pública”.

Por otro lado, en el nuevo texto del Anteproyecto se ha incluido un apartado 2 con la siguiente redacción:

> “2. El derecho fundamental que ostentan las personas físicas a la protección de datos personales se ejercerá, en aquellas cuestiones que le sean de aplicación, con arreglo a lo establecido en la Ley Orgánica

3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, siempre que el resultado de dicha aplicación no sea contrario a los fines del tratamiento a los que se refiere el apartado anterior".

No obstante, esta Agencia considera que el régimen general, contenido en el RGPD y en la LOPDGDD resultará de aplicación no sólo en aquello que no sea contrario a los fines del tratamiento del artículo 1.1., sino en todo lo que no esté específicamente regulado en al Anteproyecto – y por supuesto, siempre que el Anteproyecto, y posteriormente el texto de la ley cuando se apruebe, no sobrepase el ámbito de la Directiva (UE) 2016/680 que viene a trasponer- al objeto de garantizar dichos fines, teniendo en cuenta que, como también señalábamos en nuestro Informe 122/2018, el régimen de la Directiva representa el mínimo exigible de garantía del derecho fundamental a la protección de datos en relación con los tratamientos sometidos a su ámbito de aplicación y que las normas de derecho interno pueden recoger garantías adicionales del derecho, tal y como expresamente prevé el artículo 1.3 de la Directiva, pero en ningún caso establecer un régimen más restrictivo del derecho fundamental que el recogido en la norma de derecho de la Unión.

Por consiguiente, teniendo en cuenta que la normativa general de protección de datos de carácter personal resultará de aplicación en lo que no esté específicamente regulado en el texto sometido a informe, se propone la siguiente redacción del artículo 1.2:

"2. El derecho fundamental que ostentan las personas físicas a la protección de datos personales se ejercerá, en aquellas cuestiones que le sean de aplicación, con arreglo a lo establecido 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 por el que se deroga la Directiva 95/46/CE y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, **en todo lo que no esté específicamente regulado en la presente Ley Orgánica para garantizar** los fines del tratamiento a los que se refiere el apartado anterior".

II

En el artículo 2 del Anteproyecto se han introducido importantes modificaciones respecto al texto inicialmente informado. En este sentido, se ha modificado el apartado 1 para clarificar que los tratamientos a los que se refiere son los mencionados en el artículo 1, tal y como se había planteado por esta Agencia, si bien la nueva redacción, que se aparta de la recogida en el texto

inicial y que se correspondía con la de la Directiva, resulta confusa ya que la coma detrás del “no automatizados” podría interpretarse en el sentido de que el modificativo “contenidos o destinados a ser incluidos en un fichero” se aplica tanto a los tratamientos automatizados como no automatizados, cuando en realidad sólo aplica a estos últimos.

Por ello, se propone la siguiente redacción del artículo 2.1:

> **“1. Esta ley orgánica se aplicará a los tratamientos de datos personales referidos en el art. 1, ya se trate de un tratamiento total o parcialmente automatizado, ya de un tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.”**

Por otro lado, se ha introducido un nuevo apartado 2 relativo a la videovigilancia, con el siguiente contenido:

> “2. Se aplicará también al tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios, así como para el control, regulación, vigilancia y disciplina del tráfico con los fines del artículo 1. Fuera de estos supuestos, dichos tratamientos se regirán por su legislación específica y, supletoriamente, por 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”.

La introducción de dicho apartado se corresponde con lo previsto en la LOPDGDD, cuyo artículo 22, dedicado a los “Tratamientos con fines de videovigilancia” señala en su apartado 6 lo siguiente:

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga 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 contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

No obstante, debe modificarse la redacción del artículo 2.2. para establecer igualmente la aplicación supletoria de la LOPDGDD.

III

El apartado 3 del artículo 2 se refiere a las autoridades competentes y en el mismo se han introducido importantes modificaciones en relación con la redacción inicialmente informada. Así, después de mantener en su apartado 1, con carácter general, la consideración de autoridades competentes, a efectos de esta ley orgánica, de "toda autoridad pública que tenga competencias encomendadas legalmente, para la consecución de los fines del artículo 1", identifica a continuación algunas de ellas en particular:

> "En particular tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:
>
> a) Las Fuerzas y Cuerpos de Seguridad.
> b) Las Administraciones Penitenciarias.
> c) La Agencia Estatal de Administración Tributaria.
> d) La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.
> e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo".

Dicha redacción difiere de la recogida en el texto inicial, que enumeraba como autoridades competentes a las Fuerzas y Cuerpos de Seguridad, los Jueces y Tribunales, el Ministerio Fiscal, las Administraciones Penitenciarias y la Dirección Adjunta de Vigilancia Aduanera del Departamento de Aduanas e Impuestos Especiales de la Agencia Estatal de Administración Tributaria.

A este respecto, se debe partir de lo señalado en el artículo 3.7 de la Directiva que define como tales "toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública", o "cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública".

Por consiguiente, la inclusión de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, atendiendo a las

competencias que le atribuye el artículo 44 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo regulada en el artículo 9 de Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo y en el 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, y la referencia genérica a la Agencia Estatal de Administración Tributaria y no solo a su Departamento de Aduanas e Impuestos Especiales, atendiendo a las competencias que a la misma le atribuyen el artículo 103 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991 y la normativa tributaria y aduanera, y a la distribución de competencias entre Departamentos que se realiza en la Orden PCI/327/2019, de 20 de marzo, por la que se modifica la Orden PRE/3581/2007, de 10 de diciembre, por la que se establecen los departamentos de la Agencia Estatal de Administración Tributaria y se les atribuyen funciones y competencias, encajaría, en principio, en la definición de autoridades competentes contenida en el artículo 3.7 de la Directiva, siempre que actúen para la consecución de los fines del artículo 1 del Anteproyecto.

Sin embargo, llama la atención la supresión de la mención que en dicho precepto se realizaba a los Jueces y Tribunales y al Ministerio Fiscal, al que el nuevo texto dedica los apartados 5 y 6 del mismo artículo 2 para referirse a la normativa aplicable a los tratamientos realizados por los mismos y a los que posteriormente nos referiremos.

En este punto, y como ya se ha mencionado, hay que tener en cuenta que la Directiva define como autoridad competente a “toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública”, no existiendo la menor duda que, atendiendo a las competencias constitucional y legalmente atribuidas, dicha conceptualización la ostentan los Jueces y Tribunales del orden jurisdiccional penal, y el Ministerio Fiscal cuando actúa en dicho orden penal. Asimismo, ostentarán dicha condición los Jueces Togados y los Tribunales Militares de la Jurisdicción militar, si bien solo en los casos en que actúen en materia penal, de acuerdo con el Capítulo I del Título I de la Ley Orgánica 4/1987, de 15 de julio, de la Competencia y Organización de la Jurisdicción Militar, así como la Fiscalía Jurídico Militar, integrada en el Ministerio Fiscal, igualmente cuando actúe en el ámbito penal.

Así se recoge expresamente en la Directiva, cuyo Considerando 80 señala que “Aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales y otras autoridades judiciales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los órganos jurisdiccionales actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en

el desempeño de sus funciones. Esta excepción debe limitarse a actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho del Estado miembro. Los Estados miembros pueden disponer también que la competencia de la autoridad de control no abarque el tratamiento de datos personales realizado por otras autoridades judiciales independientes en el ejercicio de su función jurisdiccional, por ejemplo la fiscalía. En todo caso, el cumplimiento de las normas de la presente Directiva por los órganos jurisdiccionales y otras autoridades judiciales independientes debe estar sujeto siempre a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta". Y, consecuentemente, el artículo 45.2 de la Directiva señala que 2. Los Estados miembros dispondrán que cada autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función judicial. Los Estados miembros podrán disponer que su autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por otras autoridades judiciales independientes en el ejercicio de su función judicial".

Igualmente, se recogen referencias expresas a los órganos jurisdiccionales en el Considerando 63, en el que se indica que "El responsable del tratamiento designará a una persona para que le asista en la supervisión del cumplimiento interno de las disposiciones adoptadas en virtud de la presente Directiva, salvo en los casos en los que un Estado miembro decida eximir a los órganos jurisdiccionales y demás autoridades judiciales independientes cuando actúen en el ejercicio de su función jurisdiccional", y en el Considerando 20, relativo a la normativa aplicable en los procesos penales, al que posteriormente se hará referencia.

Por consiguiente, siendo claramente los Jueces y Tribunales del orden jurisdiccional penal y de la Jurisdicción Militar en el ámbito penal y el Ministerio Fiscal autoridades competentes a los efectos de la Directiva y del Anteproyecto de Ley, sería conveniente recogerlos en la enumeración que, de las autoridades competentes en particular, se contiene en el artículo 2.3 del Anteproyecto.

Por otro lado, en cuanto a la normativa aplicable a los tratamientos realizados por los órganos jurisdiccionales y por el Ministerio Fiscal, se han introducido los apartados 5 y 6 del artículo 2, en los que se recoge lo siguiente:

5. Los tratamientos realizados por los órganos jurisdiccionales en el ámbito del artículo 1 se regirán por lo dispuesto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, por las leyes procesales penales y, subsidiariamente, por lo dispuesto en el capítulo III de esta ley orgánica.

6. Los tratamientos que se lleven a cabo por el Ministerio Fiscal en el ámbito del artículo 1 se regirán por lo dispuesto en el apartado anterior y por la

Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

Por otro lado, como ya señaló en el informe 122/2018, atendiendo a lo dispuesto en el artículo 236 ter.1 de la Ley Orgánica del Poder Judicial, según el cual "Los Tribunales podrán tratar datos de carácter personal con fines jurisdiccionales o no jurisdiccionales. En el primer caso, el tratamiento se limitará a los datos en tanto se encuentren incorporados a los procesos de que conozcan y su finalidad se relacione directamente con el ejercicio de la potestad jurisdiccional", **sólo el tratamiento de datos con fines jurisdiccionales en el orden penal , podría encajar dentro del propio de las autoridades competentes a las que se refiere el artículo 3.7 de la Directiva, por lo que debería modificarse el apartado 5 para hacer referencia a "los tratamientos realizados con fines jurisdiccionales por los órganos jurisdiccionales del Orden Penal o de la Jurisdicción Militar en materia penal".**

Por otro lado, en cuanto a la normativa aplicable a dichos tratamientos, ya hemos visto anteriormente que los mismos quedan incluidos en el ámbito de aplicación de la Directiva, uno de cuyos objetivos principales es asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros, tal y como señala el Considerando 7:

Para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, es esencial asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros. A tal efecto, el nivel de protección de los derechos y libertades 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, debe ser equivalente en todos los Estados miembros. La protección eficaz de los datos personales en toda la Unión requiere tanto el fortalecimiento de los derechos de los interesados y de las obligaciones de quienes tratan dichos datos personales, como el fortalecimiento de los poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos personales en los Estados miembros.

Sin perjuicio de lo anterior y, como señala su Considerando 20, "La presente Directiva no impide que, en las normas nacionales relativas a los

procesos penales, los Estados miembros especifiquen operaciones y procedimientos de tratamiento relativos al tratamiento de datos personales por parte de tribunales y otras autoridades judiciales, en particular en lo que respecta a los datos personales contenidos en resoluciones judiciales o en registros relacionados con procesos penales".

Por consiguiente, los tratamientos de datos personales realizados por los órganos jurisdiccionales y por el Ministerio Fiscal quedan sometidos a la Directiva y, por ende, a su norma de transposición, sin perjuicio de las especialidades establecidas por la normativa nacional relativa a los procesos penales. Por tanto, a juicio de esta Agencia, dichos tratamientos, en lo que no esté específicamente previsto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en las leyes procesales penales y en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal deben quedar sujetos a la normativa contenida en el Anteproyecto, y no solo a lo previsto en su Capítulo III.

Asimismo, y conforme a lo ya señalado respecto de la Jurisdicción Militar, debe incluirse entre la normativa específica la Ley Orgánica 2/1989, de 13 de abril, Procesal Militar.

IV

El apartado 4 del artículo 2 mantiene la referencia que se contenía en el texto inicial respecto a los tratamientos para la protección y prevención frente a las amenazas contra las infraestructuras críticas, especificando en la nueva redacción que se refiere a tratamientos llevados a cabo por sujetos distintos de las autoridades competentes:

4. A los tratamientos que se lleven a cabo por sujetos distintos de las autoridades competentes y cuyo fin sea la protección y prevención frente a las amenazas contra las infraestructuras críticas les será de aplicación los capítulos III, VII y VIII.

En relación con esta cuestión esta Agencia se pronunció en su Informe 122/2018:

> Por otra parte, el artículo 2.3 del Anteproyecto prevé que "A los tratamientos cuyo fin sea la protección y prevención frente a las amenazas contra la seguridad de las infraestructuras críticas, les será de aplicación los capítulos III, VII y VIII de esta ley orgánica", es decir, los referidos a los derechos de los afectados, el procedimiento de reclamación y el régimen sancionador.

En relación con este precepto no se alcanza a comprender su sentido, toda vez que el caso de referirse a tratamientos que tengan por objeto la prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública sería plenamente de aplicación lo establecido en el Anteproyecto y no únicamente los Capítulos que se señalan en el artículo 2.3.

Del mismo modo, si la finalidad de dichos tratamientos no fuese la que acaba de mencionarse y recoge el artículo 1 del Anteproyecto sería plenamente aplicable a dichos tratamientos lo establecido en el Reglamento general de protección de datos, sin que el legislador nacional pueda restringir, a través de la norma de trasposición de la Directiva 2016/680 el ámbito de aplicación de una norma de derecho de la Unión plenamente y directamente aplicable dada su naturaleza. No obstante, no es posible determinar si se produce esta circunstancia, dado que el Proyecto ni siquiera parece referirse al hecho de que el tratamiento de datos se lleve a cabo por las autoridades competentes, siendo así que sólo en ese caso, por definición y conforme a lo dispuesto en el artículo 1.1 de la citada norma de la Unión serían de aplicación sus disposiciones.

En este sentido, debe recordarse que el Reglamento, como ya se ha dicho, establece un régimen específico tanto en lo referente a los derechos de los afectados como a los procedimientos en caso de reclamación, la posibilidad de solicitar el resarcimiento de los perjuicios derivados del tratamiento y el régimen sancionador, siendo el previsto en la Directiva más restrictivo del derecho fundamental que el contenido en el reglamento. Por ello, no sería dable al legislador nacional determinar la aplicación a estos tratamientos, si no encajan en el ámbito de aplicación de la Directiva, normas que trasponen esa disposición al derecho interno.

Por ello, procedería la supresión del artículo 2.3 del Proyecto, toda vez que en caso de que se refiriera a tratamientos que encajan dentro del ámbito de aplicación de la Directiva deberían someterse en su integridad al Anteproyecto, mientras que si se tratase de supuestos regulados, con carácter general, por el Reglamento general de Protección de datos no es posible restringir la aplicación de dicha norma de la Unión a través de una disposición de derecho interno.

Por consiguiente, especificándose en la nueva redacción que la misma se refiere a tratamientos realizados por sujetos distintos de las autoridades competentes no se trataría de una norma de transposición de la Directiva y

estaría extendiendo a supuestos no contemplados en la misma una regulación más restrictiva del derecho fundamental a la protección de datos personales que la establecida en el RGPD, que sería la norma general aplicable a los mismos.

Todo ello sin perjuicio de que, al amparo del artículo 23 del RGPD y siempre que se justifique la concurrencia de alguno de los supuestos previstos en el mismo, puedan establecerse limitaciones a los derechos de los afectados, que deberán responder al principio de proporcionalidad, pero sin que sea extensible, sin más, una regulación más restrictiva prevista para un supuesto diferente, como es la contenida en la Directiva.

Por ello, esta Agencia insiste en la necesidad de suprimir el apartado 4 del artículo 2 del Anteproyecto.

V

Procede a continuación hacer referencia a los supuestos de exclusión del ámbito de aplicación de la Ley Orgánica contenidos en el apartado 7 del artículo 2.

El apartado a) recogiendo la observación realizada por esta Agencia, ha establecido la sujeción de los tratamientos realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos, a lo dispuesto en el RGPD. No obstante, dichos tratamiento quedan, asimismo, sujetos a lo establecido en la normativa nacional que adapta al mismo el derecho español, por lo que debería añadirse **“y en la Ley Orgánica 3/2018, de 5 de diciembre”.**

Por otro lado, el artículo 2.3.a) de la Directiva establece que la misma no se aplica al tratamiento de datos personales en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, especificando el Considerando 14 que “Puesto que la presente Directiva no debe aplicarse al tratamiento de datos personales en el marco de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, no deben considerarse comprendidas en el ámbito de aplicación de la presente Directiva las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional y las actividades de tratamiento de datos personales que lleven a cabo los Estados miembros en el ejercicio de las actividades incluidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (TUE)”.

Partiendo de lo anterior, el Anteproyecto excluye de su aplicación en el artículo 2.7 los siguientes tratamientos:

b) Los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del capítulo II del título V del Tratado de la Unión Europea.

c) Los derivados de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión Europea.

d) Los sometidos a la normativa sobre materias clasificadas, Defensa o Seguridad Nacional.

En relación con dichos tratamientos, la no aplicación de la normativa contenida en el Anteproyecto no implica que haya de quedar desprotegido el derecho a la protección de datos personales, reconocido en el ordenamiento interno como un derecho fundamental en el artículo 18.4 de la Constitución. En este sentido, en el Informe 122/2018 se señalaba lo siguiente:

> "Tampoco resulta problemática la exclusión que el artículo 2.4 b) del Anteproyecto realiza de los tratamientos vinculados con la política exterior y de seguridad común, regulada por el Capítulo II del Título V del Tratado de Funcionamiento de la Unión. En efecto, el Reglamento general de protección de datos diferencia claramente en su artículo 2.2 estos tratamientos de los sometidos a la propia Directiva, por lo que no estarían sometidos a su ámbito de aplicación tampoco lo estarían al de la norma que la traspone al derecho interno, pudiendo considerarse que esta previsión resulta clarificadora, dada la naturaleza de las actividades relacionadas con estos tratamientos.
>
> El apartado c) se refiere a los tratamientos "derivados de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión Europea".
>
> En relación con este supuesto, debe tenerse en cuenta que el artículo 2.2 a) de la Directiva se refiere al mismo, lo que justificaría su exclusión. Ahora bien, la previsión del Anteproyecto debería cohonestarse con el resto de las disposiciones del derecho español que regulan el derecho fundamental a la protección de datos de carácter personal, toda vez que, lógicamente, este derecho no sólo debe resultar garantizado en los supuestos expresamente sometidos al derecho de la Unión, sino que aparece reconocido como derecho fundamental en el artículo 18.4 de la Constitución, tal y como ha puesto de manifiesto reiterada doctrina del Tribunal Constitucional.

Quiere ello decir que aun siendo obvio que las disposiciones de la Ley de trasposición de la Directiva 2016/680 al derecho interno no son de aplicación a estos tratamientos ello no supone que el derecho fundamental a la protección de datos de carácter personal pueda quedar desprotegido en estos casos.

Por este motivo, el Proyecto de Ley orgánica de Protección de datos de carácter personal establece en su artículo 2.3 que "Los tratamientos a los que no sea directamente aplicable el Reglamento UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica".

Pues bien, a fin de garantizar una interpretación armonizada de la totalidad de las normas reguladoras del derecho fundamental a la protección de datos de carácter personal, sería conveniente modificar la letra c) del artículo 2.4 del Anteproyecto, añadiendo a lo ahora establecido "a los que se aplicarán las disposiciones que establece el artículo 2.3 de la Ley Orgánica XXX de protección de datos de carácter personal".

Esta misma consideración debería tenerse en cuenta en lo que afecta a la remisión efectuada por el artículo 2.4 e) del Anteproyecto a la Defensa nacional".

El precepto se refiere, dentro de los supuestos excluidos al que acaba de mencionarse junto con los tratamientos sometidos a materias clasificadas.

Debe en este punto traerse a colación lo señalado por el considerando 14 de la Directiva, en el sentido de considerar que la regulación de las materias clasificadas puede considerarse, lógicamente, incluida dentro del concepto de seguridad nacional mencionado en dicho considerando.

Sin embargo, no cabe extraer la misma conclusión en relación con todos los tratamientos vinculados a la defensa nacional que, no encajando lógicamente en el ámbito de aplicación del Anteproyecto, conforme a su artículo 1, sí se someterán al régimen general de protección de datos, no quedando excluidos de la aplicación de la Ley Orgánica general, al encontrarse dentro de los regulados por el artículo 2.3 al que se ha hecho referencia con anterioridad.

Por este motivo, sería procedente separar las dos materias mencionadas por el artículo 2.4 e) del Anteproyecto, aplicando a los tratamientos "sobre defensa nacional" la misma regla que se ha señalado

anteriormente en relación con los tratamientos referidos a materias no comprendidas en el derecho de la Unión".

Partiendo de lo informado anteriormente, debe hacerse una especial referencia a la exclusión de las materias relacionadas con la Seguridad Nacional, a las que se refiere la Directiva e igualmente el artículo 2.2 del RGPD, que señala que "El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión" y el Considerando 16 "El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión".

El concepto de seguridad nacional es de cuño reciente, empezándose a utilizar doctrinalmente en la década de los 80 del siglo pasado, derivado de la aparición de amenazas híbridas que impiden mantener la tradicional diferenciación entre defensa (para hacer frente a la amenazas procedentes del exterior y a las amenazas interiores más graves para la supervivencia del propio Estado, tal como se refleja en el artículo 8 de la Constitución que atribuye a las Fuerzas Armadas la misión de garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional) y seguridad pública (para hacer frente a la amenazas de orden público interiores, de acuerdo con el artículo 104 del texto constitucional, que atribuye a las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, la misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana). La aparición de dichas amenazas obligan a una concepción integral de la Seguridad que garantice la acción coordinada de los distintos actores, y si bien era una idea que subyacía en la definición de defensa nacional que contenía el artículo 2 de la Ley Orgánica 6/1980, de 1 de julio, por la que se regulan los criterios básicos de la defensa nacional y la organización militar ("La defensa nacional es la disposición, integración y acción coordinada de todas las energías y fuerzas morales y materiales de la Nación, ante cualquier forma de agresión, debiendo todos los españoles participar en el logro de tal fin") en España no se recoge normativamente hasta la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

En el ámbito europeo se ha ido produciendo la misma adaptación, no recogiéndose el concepto de Seguridad Nacional hasta el Tratado de Lisboa (en vigor desde el 1 de diciembre de 2009). Así, actualmente el término solo se recoge en el artículo 4 de la versión consolidada del Tratado de la Unión Europea que señala que la seguridad nacional seguirá siendo responsabilidad

exclusiva de cada Estado miembro y en el artículo 73 de la versión consolidada del Tratado de Funcionamiento de la Unión Europea relativo a la cooperación y coordinación en materia de seguridad nacional.

Por el contrario, son muchos los preceptos del tratado que mantienen la tradicional diferenciación entre seguridad pública (artículos 36, 45, 52, 66), o seguridad interior (artículo 72) y defensa (artículos 2, 222 y 333), sin perjuicio de las disposiciones correspondientes a la política común de seguridad y defensa.

Este concepto también ha sido igualmente utilizado por las normas europeas coetáneas y posteriores al Tratado de Lisboa, como la Directiva 2009/81/CE del Parlamento Europeo y del Consejo de 13 de julio de 2009 sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE que comienza señalando que “La seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, tanto en el ámbito de la defensa como de la seguridad”.

En todo caso, tratándose la seguridad nacional de una excepción a la aplicación de los Tratados, y según reiterada jurisprudencia del Tribunal de Justicia, ha de ser objeto de interpretación restrictiva. A estos efectos, puede citarse la extensa doctrina jurisprudencial existente en relación al concepto de “intereses esenciales de la seguridad” que contiene el vigente artículo 346 del TFUE (Sentencia TJUE de 4 de octubre de 1991, Asunto C-367/89, Caso Rickardt y Les Accesories Scientifiques, Sentencia TJUE de 3 de mayo de 1994, Asunto C-328/92 Caso Comisión contra España, Sentencias TJUE 11 de enero de 2000, Asunto C-285/98, Caso Tanja Kreril contra Bundesrepublik, Sentencia de 28 de marzo de 1995 Asunto C-234/93, Caso Evans Medical, Sentencia 11 de septiembre de 2008, Asunto C-141/07 Caso Comisión contra Alemania, Sentencia de 2 de octubre de 2008, Asunto C-157/06, Caso comisión contra Italia, Sentencia de 16 de septiembre de 1999, Asunto C-414/97, Caso Comisión contra España, Sentencia de 15 de diciembre de 2009, Asunto C-372/05, Caso Comisión contra Alemania, Sentencia de 4 de septiembre de 2014, Caso Schiebel, Sentencia 15 de mayo de 1986, Asunto 222/84, Johnston, entre otras muchas) y que puede sintetizarse en los siguientes criterios:

1) Las excepciones que se establecen en dicho artículo, al igual que todos aquellos artículos que permiten no aplicar los principios y normas del tratado, han de ser objeto de interpretación estricta.

2) La carga de la prueba de que existen realmente las circunstancias excepcionales que justifican la excepción incumbe a quien pretenda beneficiarse de ellas.

3) Las autoridades nacionales disponen de cierto margen de apreciación al adoptar las medidas que consideran necesarias para garantizar la seguridad pública de un Estado miembro.

4) El concepto de seguridad pública se refiere tanto a la seguridad interior de un Estado miembro como a su seguridad exterior.
5) No se puede deducir la existencia de una reserva general, inherente al Tratado, que excluya del ámbito de aplicación del Derecho comunitario cualquier medida adoptada por motivos de seguridad pública.
6) Corresponde a las autoridades nacionales demostrar que esas disposiciones son necesarias para alcanzar el objetivo invocado, y que éste no puede alcanzarse mediante prohibiciones o limitaciones de menor amplitud o que afecten en menor medida al comercio intracomunitario (principio de proporcionalidad).

En el ámbito de la protección de datos, avala igualmente el criterio restrictivo el propio RGPD, que después de excluir su aplicación en los supuestos de seguridad nacional, según lo visto, establece la sujeción al mismo si bien pueden establecerse limitaciones en los supuestos de seguridad del Estado, defensa y seguridad pública (artículo 23).

Sin embargo, atendiendo a la evolución doctrinal anteriormente señalada, y con una finalidad clara de mejorar la coordinación de las diferentes Administraciones Pública, después de señalar en su Exposición de Motivos que "la Seguridad Nacional debe ser considerada un objetivo compartido por las diferentes Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte", la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional la define en su artículo 3 señalando que "A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos". Y en su artículo 9 establece como componentes fundamentales de la Seguridad Nacional a los efectos de esa ley la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica.

Por consiguiente, en la única definición normativa de la Seguridad Nacional se establece un concepto amplio para garantizar una respuesta integral y coordinada a los diferentes riesgos y amenazas, criterio amplio que reconoce la Estrategia de Seguridad Nacional de 2017 al definir la política de Seguridad Nacional como "una política de Estado que parte de una concepción amplia de la seguridad". Sin embargo, en lo que se refiere a la protección del derecho fundamental a la protección de datos personales, el concepto de Seguridad Nacional ha de ser objeto de interpretación restrictiva conforme a la jurisprudencia anteriormente citada, siendo el TJUE el que deberá ir perfilando el mismo a los efectos del RGPD y de la Directiva, para garantizar el carácter

homogeneizador que en materia de protección del derecho fundamental a la protección de datos quieren establecer dichas normas.

Por ello, no pudiendo excluirse el derecho fundamental a la protección de datos personales en los supuestos de Seguridad Nacional, sin perjuicio de las limitaciones que puedan establecerse en su normativa específica, y al fin de establecer una regulación coherente de dicho derecho, **se insiste en la necesidad, ya recogida en nuestro anterior informe, de incluir las referencias a la defensa nacional y a la seguridad nacional en el apartado b) referido a las materias no comprendidas en el derecho de la Unión, e incluir un apartado en el que se recoja que "Los tratamientos que afecten a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018".**

Asimismo, atendiendo a lo anteriormente señalado**, esta Agencia considera necesario suprimir la exclusión específica de los tratamientos relativos a la lucha contra el terrorismo a los que se refiere la letra e) del artículo 2.7**

> e) Los relativos a la lucha contra el terrorismo que afecten a la Seguridad Nacional, y los relativos a las formas graves de delincuencia organizada dirigida a desestabilizar gravemente el normal funcionamiento del Estado y de las Instituciones. A las actividades de tratamiento recogidas en este apartado no les será de aplicación ni el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ni la Ley Orgánica 3/2018, de 5 de diciembre, sino que estarán sujetos a lo dispuesto en la normativa sobre materias clasificadas y seguridad de la información. No obstante, en estos supuestos el responsable del fichero comunicará previamente su existencia y su finalidad a la Autoridad de control.

En relación con dichos tratamientos, el Informe 122/2018 señalaba lo siguiente:

> Finalmente debe hacerse referencia a la exclusión efectuada en el artículo 2.4 d) del Anteproyecto, según el cual, no será de aplicación a los tratamientos "relativos a la lucha contra el terrorismo y a las formas graves de delincuencia organizada dirigida a desestabilizar gravemente el normal funcionamiento del Estado y de las instituciones".
>
> Ciertamente la Ley Orgánica 15/1999 se refería en su artículo 2.2 c), dentro de los supuestos excluidos de su aplicación a "los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada". Sin embargo, debe indicarse que dicha exclusión, en primer lugar, se contenía en una norma anterior a la

adopción y entrada en vigor del Tratado de Funcionamiento de la Unión Europea y, por consecuencia, a la inclusión dentro de su ámbito de aplicación del denominado Tercer Pilar.

Al propio tiempo, como es obvio, la Ley Orgánica 15/1999 fue aprobada en un momento en que no existía una concreta norma de derecho de la Unión que hubiera de ser traspuesta al derecho de los Estados Miembros que regulase, de forma explícita, el tratamiento de los datos de carácter personal “por parte de las autoridades competentes, con 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 contra la seguridad pública”, siendo así que el tratamiento de datos relacionado con la lucha contra el terrorismo y las formas graves de delincuencia organizada encaja plenamente en la finalidad que acaba de reproducirse y que establece el artículo 1.1 de la Directiva 2016/680.

Ciertamente, como se ha indicado en relación con las materias clasificadas, el considerando 14 permite excluir del régimen de la Directiva los tratamientos relacionados con la “seguridad nacional”. Sin embargo, no existiendo un concepto unívoco de la misma tampoco resulta admisible establece una fórmula genérica que, de facto, pueda excluir de la aplicación de la Directiva y, en consecuencia, de su norma de trasposición el tratamiento de datos relacionado con la lucha contra el terrorismo y la delincuencia organizada, por entender que su objetivo es desestabilizar gravemente el normal funcionamiento del Estado y de las instituciones.

Ello es así por cuanto la generalidad de dichos conceptos, unida al concepto amplio de delincuencia organizada, hace posible que las autoridades competentes puedan determinar casi libremente cuándo aplicar las disposiciones del Anteproyecto y cuándo no aplicarlas.

Al propio tiempo, una interpretación restrictiva de la aplicación de las normas de protección de datos en relación con estos tratamientos llevaría a la conclusión de que no estarían sometidas al derecho de la Unión (al ser ésta la única causa admisible de exclusión) tratamientos como los regulados por la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, dadas las finalidades descritas en el artículo 6 de dicha norma, vinculadas a la lucha contra el terrorismo y la delincuencia organizada. En este sentido, recuerda el considerando 8 de esta última Directiva que “El uso eficaz de los datos PNR, por ejemplo, comparando los datos PNR con diversas bases de datos sobre

personas y objetos buscados, es necesario para, prevenir, detectar, investigar y enjuiciar de modo eficaz delitos de terrorismo y delitos graves, reforzando así la seguridad interior, para reunir pruebas y, en su caso, descubrir a los cómplices de los delincuentes y desmantelar redes delictivas".

Por este motivo, no es posible considerar que los tratamientos incluidos en el artículo 2.4 d) del Anteproyecto sometido a informe se encuentran excluidos de su ámbito de aplicación, por cuanto su finalidad es la 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 contra la seguridad pública". Ello supone que deberá suprimirse del texto sometido a informe la exclusión contenida en el artículo 2.4 d).

En efecto, tal y como se señalaba en el anterior informe, los tratamientos de datos en el ámbito de la lucha contra el terrorismo se encuentran incluidos dentro del ámbito de aplicación de la Directiva, que como se ha indicado, tiene por finalidad garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, siendo el terrorismo uno de los ámbitos delictivos de especial gravedad a los que se refiere el artículo 83 del TFUE.

El nuevo texto circunscribe la exclusión a los tratamientos "relativos a la lucha contra el terrorismo que afecten a la Seguridad Nacional". A este respecto, la Estrategia de Seguridad Nacional de 2017, partiendo de una concepción amplia del concepto de seguridad, incluye entre las "Amenazas y desafíos para la Seguridad Nacional" al terrorismo, fundamentalmente de carácter yihadista, a la vez que destaca la creciente vinculación internacional del crimen organizado con el terrorismo. No obstante, hay que tener en cuenta que también incluye otro tipo de amenazas, como pueden ser, por ejemplo, el crimen organizado y el espionaje, igualmente tipificadas en el Código Penal, que no quedan excluidas del ámbito de aplicación de la Directiva ni así se plantea, con carácter general, en el texto remitido. Precisamente, la Directiva tiene por finalidad regular el tratamiento de datos personales en relación con los diferentes delitos, para lo que permite una mayor flexibilidad en materias tales como finalidades, bases de legitimación, derechos de los interesados o transferencias internacionales de datos.

Por consiguiente, tal y como se ha venido indicando, los tratamientos de datos personales derivados de la lucha contra el terrorismo quedan incluidos, con carácter general, en el ámbito de aplicación de la normativa comunitaria, que incluso ha aprobado normas específicas al respecto, como la ya citada Directiva PNR. Solo en el caso excepcional de que en un supuesto concreto se entendiera que afecta a la Seguridad Nacional, de acuerdo con la interpretación restrictiva anteriormente señalada, quedarían excluidos de la aplicación de la Ley Orgánica en virtud de la exclusión referida a la Seguridad Nacional, del mismo modo que aquellos que quedaran sujetos a la normativa sobre materias

clasificadas quedarían igualmente excluidos de la misma, **por lo que esta Agencia considera que debe suprimirse la letra e) del artículo 2.7. del Anteproyecto.**

VI

Por último, el artículo 2 en su apartado 8 mantiene la previsión, ya incluida en el texto inicial, referente a los sujetos a los que el ordenamiento jurídico imponga un específico deber de colaboración con las autoridades competentes:

> 8. Los tratamientos realizados por los sujetos a los que el ordenamiento jurídico imponga un específico deber de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, se regirán por lo dispuesto en la norma que establezca dicha obligación y por los capítulos III, VII y VIII de esta ley orgánica, siendo de aplicación supletoria lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y sus disposiciones de aplicación".

A este respecto, en el Informe 122/2018, esta Agencia razonaba lo siguiente:

> 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 definitiva, la aceptación de una disposición como la propuesta supondría una limitación de los derechos de los afectados cuyos datos fueran objeto de tratamiento, no sólo por el hecho de que el Reglamento reconoce derechos que no aparecen regulados por la Directiva, sino porque además, se establece en la Directiva un régimen más flexible de limitación de esos derechos, reflejado en el artículo 16 del proyecto, que no es respetuoso con los requisitos establecidos en el artículo 23 del reglamento para que el legislador pueda limitar el ejercicio de los citados derechos, dado que el artículo 23.2 enumera una serie de requisitos que deberá reunir la Ley que no se encuentran previstos en la Directiva.

Por ello, esta Agencia insiste en la necesidad de suprimir el artículo 2.8. del Anteproyecto.

VII

El artículo 3 del Anteproyecto ha recogido la observación formulada por esta Agencia en relación con las definiciones de la Directiva, estableciendo una remisión general a lo establecido en el RGPD.

No obstante, de dicha remisión genérica **debería suprimirse la referencia a la definición de autoridades competentes,** respecto de la que se establece una definición específica en el artículo 2.3 del Anteproyecto, **así como respecto del responsable del tratamiento,** que se define en el apartado 2 del propio artículo 3.

Asimismo, no resulta procedente la remisión a la definición del consentimiento, al no constituir un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes (Considerandos 35 y 37 de la Directiva).

VIII

El artículo 4 recoge los principios del tratamiento de acuerdo con lo señalado por la Directiva. No obstante, tal y como se indicó en el Informe 122/2018, el artículo 4.4. de la misma establece que el responsable del tratamiento "será responsable y capaz de demostrar" el cumplimiento de dichos principios, razón por la cual debe modificarse el apartado 4 del artículo 4 del Anteproyecto para indicar que "El responsable del tratamiento deberá garantizar **y estar en condiciones de demostrar** el cumplimiento de lo establecido en este artículo", dando de este modo cumplimiento al principio de responsabilidad proactiva que se ha constituido en el principio vertebral del nuevo régimen de protección de datos personales en la Unión.

IX

El artículo 5 regula la "Colaboración con las autoridades competentes", tratándose de un precepto que, tal y como se indicaba en el Informe 122/2018, "no traspone precepto alguno de la Directiva, pudiendo considerarse una suerte de cláusula general para la recogida de los datos por parte de las autoridades competentes". A este respecto, el citado informe recordaba la doctrina de la AEPD 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 y concluía que "En consecuencia, se propone la supresión del artículo 4 del Anteproyecto sometido a informe o su modificación, incorporando a las previsiones que actualmente se incluyen los requisitos que esta Agencia Española de Protección de Datos ha venido exigiendo para la transmisión de los datos a las Fuerzas y Cuerpos de Seguridad cuando desarrollen actividades de policía judicial, limitando los supuestos de cesión a este caso".

El nuevo texto remitido ha optado por mantener el precepto, si bien ha procedido a una nueva regulación de dicho deber de colaboración en el que se han recogido parcialmente las observaciones realizadas por esta Agencia:

> Artículo 5. Colaboración con las autoridades competentes.
>
> 1. Las Administraciones públicas, incluidas la tributaria y la de la seguridad social, de acuerdo con su legislación respectiva, 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 o enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la autoridad competente deberá ser concreta y específica.
>
> 2. En los restantes casos, las Administraciones públicas, salvo que sea legalmente exigible la autorización judicial para recabar los datos, informes, antecedentes y justificantes, así como cualquier persona física o jurídica, los proporcionarán a las autoridades competentes que los soliciten, siempre que éstos sean necesarios 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 a los fines del artículo 1.
>
> 4. El interesado no será informado de la transmisión de sus datos a las autoridades competentes en los supuestos de los apartados 1 y 2, a fin de garantizar la actividad investigadora.
>
> 5. Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un específico deber de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1 no informarán al interesado de la transmisión de sus datos a dichas autoridades.

A este respecto, esta Agencia insiste en la conveniencia de suprimir el precepto, que no se corresponde con la Directiva transpuesta y cuya inclusión en el Anteproyecto ocasiona otro tipo de distorsiones, tal y como se verá posteriormente al analizar el régimen sancionador.

No obstante, si se optara por mantenerlo con la nueva redacción, como puede observarse, se ha diferenciado entre el deber de colaboración con las autoridades judiciales, el Ministerio Fiscal o la Policía Judicial, por un lado, y la colaboración con el resto de autoridades competentes por otro, diferenciación que por parte de esta Agencia se valora positivamente, habida cuenta de las

diferentes competencias que el ordenamiento jurídico atribuye a unas y otras autoridades, al actuar las primeras en el ámbito judicial y existir garantías adicionales para la protección del derecho fundamental a la protección de datos personales derivadas de la intervención de la autoridad judicial o del Ministerio Fiscal.

En cuanto a la colaboración con las autoridades judiciales (del orden jurisdiccional penal), el Ministerio Fiscal y la policía judicial (cuando esta última actúa para el cumplimiento de las actuaciones ordenadas por la Autoridad Judicial o el Ministerio Fiscal) deberá estarse, en primer término, a lo establecido en su normativa específica, tal y como se ha analizado anteriormente y se recoge en los apartados 5 y 6 del artículo 2 del Anteproyecto, que establecen normas respecto al contenido y motivación de las resoluciones judiciales y del Ministerio Fiscal.

Sin embargo, tratándose de las funciones encomendadas a la Policía judicial en el artículo 549.1.a) de la LOPJ, 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, siendo obligación de la Policía Judicial poner los hechos en inmediato conocimiento de la Autoridad Judicial o del Ministerio Fiscal, es cuando debe tenerse en cuenta la doctrina de esta Agencia respecto de dichas actuaciones a la que se refería el Informe 122/2018, por lo que se propone la siguiente redacción:

1. Las Administraciones públicas, incluidas la tributaria y la de la seguridad social, de acuerdo con su legislación respectiva, 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 o enjuiciamiento de infracciones penales o para la ejecución de las penas. **La petición de la policía judicial, en el supuesto de ejercicio de las funciones que le encomienda el artículo 549.1.a) de la Ley Orgánica del Poder Judicial, deberá ser concreta y específica.**

Sin embargo, en cuanto a la colaboración con el resto de autoridades competentes regulada en el apartado 2, hay que tener en cuenta que la normativa específica de cada una de ellas regula el deber de colaboración con las mismas, como ocurre, por ejemplo, en el artículo 7 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, los artículos 93 a 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, o el artículo 48 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y

de la financiación del terrorismo, normativa que en ocasiones establece garantías adicionales para el tratamiento de los datos de carácter personal. En ocasiones, esta garantía puede consistir en la necesaria autorización judicial, mientras que en otras ocasiones se establecen otro tipo de garantías ajustadas a los principios de protección de datos personales, para garantizar debidamente la proporcionalidad en el acceso a la información, como pueda ser, por ejemplo, limitar el tipo de datos o la gravedad de los delitos respecto de los que procederá dicho acceso.

En este sentido, existen supuestos en los que el ordenamiento jurídico exige autorización judicial para el acceso a los datos, como ocurre en 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 artículo 1 señala que “esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales”.

Precisamente, la falta de garantía de un control judicial previo fue la que determinó que el TJUE (Sentencia Digital Rights Ireland) 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”.

Invocando dicha doctrina judicial, esta Agencia informó desfavorablemente la modificación del artículo 43.3 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo con el objeto de suprimir la necesaria autorización judicial o del Ministerio Fiscal para el acceso al fichero de titularidades financieras por parte de las Fuerzas y Cuerpos de Seguridad. En el Informe 41/2018 se observaba lo siguiente:

> 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.

Por otro lado, en el Informe 35/2018, referente al Anteproyecto de Ley Orgánica sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, se incorpora al Derecho español la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, que regula, conforme a su artículo 1.1 la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE y el tratamiento de estos datos, incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros, se indicaba lo siguiente:

IX

El artículo 9 del Anteproyecto se refiere a las autoridades competentes, siguiendo lo establecido en el artículo 7 de la Directiva PNR. A tal efecto, el apartado 1 enumera dichas autoridades, el apartado segundo se refiere a los requisitos de las solicitudes que deberán dirigirse a la UIP, el artículo 4 limita las finalidades del tratamiento de los datos y el apartado 5 se refiere al derecho del interesado en relación con las decisiones automatizadas adoptadas por las autoridades competentes.

En relación con este punto, debe hacerse referencia al apartado 2 del artículo 9, a cuyo tenor “Las peticiones de datos realizadas por las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas”.

Ya se ha indicado en un lugar anterior que la sistemática de la Directiva PNR ubica este precepto entre las obligaciones de las UIP, que no deben aceptar solicitudes masivas de datos y que deben valorar la fundamentación de las que se le dirijan. El Anteproyecto, por el contrario, ubica estas previsiones en el artículo dedicado a las autoridades competentes.

La cuestión que no obstante debería plantearse, a la luz de la doctrina del Tribunal de Justicia de la Unión Europea en las sentencias recaídas en los asuntos Digital Rights Ireland y Tele2 Sverige es la de si

los únicos requisitos formales que han de exigirse a las solicitudes son los de que las mismas sean “debidamente motivadas y con suficiente base” o si sería necesaria la existencia de algún tipo de exigencia formal adicional.

A tal efecto, no debe olvidarse que, como se viene indicando a lo largo de este informe, y se desprende de la jurisprudencia que se acaba de mencionar, el tratamiento llevado a cabo por la UIP, que recogerá la información de todos los vuelos internacionales así como de determinados vuelos nacionales que se establezcan supone una clara intromisión en los derechos fundamentales de los pasajeros y tripulantes a los que los datos se refieren y, particularmente, de su derecho fundamental a la protección de datos de carácter personal.

Evidentemente nada cabe objetar de las solicitudes que se lleven a cabo por la autoridad judicial o por el Ministerio Fiscal, amparadas actualmente en el artículo 11.2 d) de la Ley Orgánica 15/1999 y en el nuevo marco normativo en la obligación legal a la que se refiere el artículo 6.1 c) del Reglamento 2016/679.

La cuestión se plantea en los restantes supuestos, en que sería precisa la existencia de algún tipo de requerimiento adicional previo al acceso a los datos.

Así, esta Agencia, en lo que se refiere a las Fuerzas y Cuerpos de Seguridad, tanto estatales como autonómicos, ha venido señalando que podría ser posible sin necesidad de autorización judicial expresa el acceso a los datos de carácter personal que resulte necesario para el desempeño por los mismos de sus funciones de policía judicial, siempre y cuando se cumplan una serie de requisitos que reiteradamente se han venido señalando, entre los que resulta esencial la comunicación posterior de los datos a los órganos judiciales o al Ministerio Fiscal.

Teniendo en cuenta lo antedicho, debería plantearse si no sería necesario el establecimiento de algún requisito adicional para que pueda llevarse a cabo una solicitud de datos PNR por las Fuerzas y Cuerpos de Seguridad.

Por lo tanto, de admitirse la redacción propuesta, supondría reconocer un genérico deber de colaboración que dejaría sin efecto las garantías, distintas de la autorización judicial, que el legislador nacional pueda haber establecido en la normativa para garantizar la efectividad del derecho a la protección de datos de carácter personal.

Por consiguiente, se considera necesario que el deber de colaboración se ponga en relación con lo previsto en la normativa específica. Asimismo, debería suprimirse la referencia a la exigencia de autorización judicial, al recogerse en el apartado 3, proponiéndose la siguiente redacción:

2. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán al resto de autoridades competentes los datos, informes, antecedentes y justificantes que les soliciten, siempre que éstos sean necesarios 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, en los términos y respetando las garantías previstas en la normativa específica que resulte de aplicación. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

Por último, y atendiendo a lo ya informado respecto al tratamiento de los datos personales por los sujetos a los que el ordenamiento jurídico imponga un específico deber de colaboración con las autoridades competentes al analizar el artículo 2.8. del Anteproyecto, procedería la supresión del apartado 5 del artículo 5 del mismo.

Por consiguiente, a juicio de esta Agencia, el artículo 5 debería suprimirse y, en el supuesto de mantenerse, debería tener la siguiente redacción:

Artículo 5. *Colaboración con las autoridades competentes.*

1. Las Administraciones públicas, incluidas la tributaria y la de la seguridad social, de acuerdo con su legislación respectiva, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judiciallos datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación o enjuiciamiento de infracciones penales o para la ejecución de las penas. **La petición de la policía judicial, en el supuesto de ejercicio de las funciones que le encomienda el artículo 549.1.a) de la Ley Orgánica del Poder Judicial, deberá ser concreta y específica y estar debidamente motivada".**

2. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán al resto de autoridades competentes los datos, informes, antecedentes y justificantes que les soliciten, siempre que éstos sean necesarios 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, en los términos y respetando las garantías previstas en la normativa específica que resulte de aplicación. 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 a los fines del artículo 1.

4. El interesado no será informado de la transmisión de sus datos a las autoridades competentes en los supuestos de los apartados 1 y 2, a fin de garantizar la actividad investigadora.

X

El artículo 6 procede a la transposición del artículo 5 de la Directiva, relativo a la conservación de los datos personales, habiéndose recogido en el mismo las observaciones realizadas por esta Agencia respecto al bloqueo de los datos y estableciendo un plazo concreto para la revisión de los datos cuando se haya considerado procedente dicha conservación más allá de los plazos establecidos con carácter general en el Anteproyecto.

Sin embargo, no se ha recogido la observación relativa a la necesidad de establecer criterios de conservación de los datos objeto de tratamiento por las autoridades competentes que desempeñan funciones policiales ni de adaptar los criterios de conservación de los ficheros jurisdiccionales a la normativa que, conjuntamente con el Anteproyecto, les será de aplicación, habiéndose optado por suprimir los criterios que se establecían en la redacción inicial respecto a los ficheros jurisdiccionales.

A este respecto, tal y como se indicaba en el Informe 122/2018, “del tenor del precepto de la Unión parece desprenderse un mandato a los Estados para que establezcan los criterios de conservación de los datos personales sometidos a tratamiento para los fines previstos en la Directiva”. Además, hay que tener en cuenta que en los últimos años se están incrementando el número de sentencias de la Audiencia Nacional que estiman los recursos interpuestos por particulares respecto de la cancelación de sus antecedentes policiales, siendo este momento una buena ocasión para clarificar los criterios que pueden resultar aplicables.

Al objeto de establecer dichos criterios, singularmente en cuanto a los ficheros policiales, podría partirse de lo establecido en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Asimismo, en cuanto a las actuaciones de la Policía Judicial, puede seguirse igualmente el criterio mantenido por esta Agencia, según el cual, 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.

Por tanto, debería modificarse el artículo 6 del Anteproyecto para incluir criterios específicos sobre el plazo de conservación de los datos personales.

Por otro lado, el apartado 2 del artículo 6 prevé que “Excepcionalmente, cumplidos los plazos a los que se refiere el apartado anterior, el responsable del tratamiento podrá acordar motivadamente la necesidad de conservar los datos por más tiempo. De no adoptarse decisión expresa al respecto, los datos serán suprimidos o, en su caso, bloqueados.”

En opinión de esta Agencia, la redacción del citado precepto, que no se corresponde con ninguna previsión de la Directiva, añade incertidumbre al plazo de conservación de los datos, desconociéndose cuáles son las razones que pueden motivar la prolongación del plazo y si se refiere a la misma finalidad para la que se obtuvieron los datos a para una finalidad ulterior, debiendo, en todo caso, quedar limitado a los fines previstos en el artículo 1. En principio, dicho previsión parece ir referida a la conservación de los datos para su tratamiento para una finalidad ulterior, lo que requeriría la concurrencia de las condiciones a las que se refiere el artículo 4.2 al regular los tratamientos ulteriores, lo que debería clarificarse en el precepto. Asimismo, debería contemplarse la información al interesado de dicha conservación, salvo que existan razones que justifiquen lo contrario.

XI

En relación con el artículo 7 del Anteproyecto, el mismo se refiere, en su nueva redacción a los supuestos de “infracción penal o relativa a la protección y prevención frente a las amenazas contra la seguridad pública”.

A este respecto, procede traer a colación lo ya manifestado en el Informe 122/2018:

> El artículo 6 tiene por objeto trasponer el artículo 7 de la Directiva, referido a la obligación del responsable del tratamiento de diferenciar en la medida que ello sea posible, las distintas categorías de datos objeto de tratamiento para los fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública.
>
> El precepto responde con carácter general a lo establecido en la norma objeto de trasposición. No obstante, se detecta una omisión reiterada a lo largo de todo el precepto, por cuanto el mismo se refiere a “infracciones”, mientras que el ámbito de la Directiva se refiere a “infracciones penales”.
>
> La omisión no es baladí si se tiene en cuenta que dentro de los objetivos del tratamiento, según el artículo 1 del Anteproyecto, se encuentra la prevención y persecución de amenazas contra la seguridad pública, que puedan dar lugar a la existencia de conductas tipificadas como infracciones administrativas. La omisión de la referencia a la naturaleza penal de las infracciones podría permitir una interpretación extensiva del precepto que habilitase el tratamiento de datos de afectados distintos de los propios infractores más allá de lo permitido por el ordenamiento español, al habilitarse una norma para su tratamiento diferenciado.
>
> Por este motivo, debería añadirse el término “penal” o “penales” a las referencias reiteradas que el artículo 6 realiza de las “infracciones” a las que el mismo se refiere.

Atendiendo a esos mismos argumentos, y para evitar interpretaciones extensivas a las infracciones administrativas, **debería limitarse la referencia del artículo 7.a) del Anteproyecto, exclusivamente, a las “infracciones penales”.**

XII

En relación con el artículo 8.2, relativo a la verificación de la calidad de los datos, se ha añadido un segundo párrafo en el que se recoge lo indicado en

el artículo 7.2 de la Directiva: “En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar en qué medida los datos personales son exactos, completos y fiables y en qué medida están actualizados”.

Sin embargo, se mantiene inalterada la redacción del párrafo primero del apartado 2 de dicho artículo 8, respecto de la que el Informe 122/2018 señaló lo siguiente:

> 2.Quiere ello decir que la norma de derecho de la Unión establece un mandato claro, preciso e incondicional de que los datos inexactos, incompletos o que no estén actualizados “no se transmitan ni se pongan a disposición de terceros”.
>
> Frente a ello, el Anteproyecto prevé que dichos datos no serán puestos a disposición de terceros “sin transmitir al mismo tiempo la valoración de su calidad, exactitud y actualización”.
>
> Sin perjuicio de que dicha valoración habrá de ser puesta en conocimiento del destinatario en todo caso, por imperativo del artículo 7.2 de la Directiva, la norma interna implicaría, en una interpretación literal de la misma, una extralimitación sobre la norma de derecho de la Unión, por cuanto de ella parece desprenderse que sí sería posible la transmisión que la Directiva prohíbe siempre y cuando se aporte una valoración acerca de la exactitud y actualización de los datos.
>
> Por este motivo, debería darse una nueva redacción al artículo 7.2 del Proyecto de la que se desprenda inequívocamente que en caso de que la evaluación de los datos determine que los mismos son inexactos, incompletos o no actualizados no se procederá a la comunicación de los mismos a terceros, sin que sea posible dicha comunicación por el mero hecho de que se aporte el análisis al que se refiere el precepto”.

Por los motivos expuestos en el citado informe, y teniendo en cuenta la inclusión del nuevo párrafo en el artículo 8.2, **debería suprimirse del párrafo primero la referencia a “sin trasladar al mismo tiempo la valoración de su calidad, exactitud y actualización”.**

No obstante, con el fin de conciliar el adecuado cumplimiento de lo previsto en la Directiva en garantía del derecho del afectado con el debido cumplimiento de los fines objeto de la misma, se propone la siguiente redacción alternativa, que recoge literalmente lo previsto en la Directiva al tiempo que establece una mayor garantía para el interesado evitando posibles errores:

> **2. Las autoridades competentes adoptarán todas las medidas razonables para garantizar que los datos personales que sean**

inexactos, incompletos o no estén actualizados no se transmitan ni se pongan a disposición de terceros. En toda transmisión de datos se trasladará al mismo tiempo la valoración de su calidad, exactitud y actualización.

XIII

El artículo 9.2 del Anteproyecto ha quedado redactado de la siguiente forma:

> 2. Cualquier ley que regule el tratamiento de categorías de datos personales para los fines incluidos en el ámbito de aplicación de esta ley orgánica deberá, al menos, identificar las categorías de datos personales y los objetivos y fines del tratamiento.

En la nueva redacción, se ha sustituido la referencia que se contenía en el texto inicial, a “datos personales” por “categorías de datos personales”. Dicha previsión no se corresponde con lo estipulado en la Directiva, cuyo artículo 8.2. señala que “El Derecho del Estado miembro que regule el tratamiento dentro del ámbito de aplicación de la presente Directiva, deberá indicar al menos los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento”. En este punto, hay que tener en cuenta que el Derecho Europeo, tanto en la Directiva como en el RGPD, trata diferentemente los conceptos de “categorías de datos” y de “datos”, de modo que, cuando quiere referirse a las “categorías de datos” lo hace expresamente, tal y como se recoge, por ejemplo, en los artículos 14.b) y 24.1.d) y h) de la Directiva.

En este caso, la Directiva contiene un mandato explícito y concreto, que no debería ser modificado, en sentido restrictivo, por la legislación de trasposición, por lo que debería volverse a la redacción inicialmente recogida en el Anteproyecto:

> **“Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta ley orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento”**

XIV

El artículo 10, sobre “condiciones específicas de tratamiento”, procede a la transposición de lo previsto en el artículo 9 de la Directiva, si bien no recoge lo previsto en los dos primeros apartados de la misma. En cuanto al segundo

de los apartados, relativo a los tratamientos relativos a funciones que no coincidan con los fines del artículo 1, quedaría recogido en el artículo 2 sobre el ámbito de aplicación de la ley.

Sin embargo, el apartado primero no se limita exclusivamente a determinar el régimen jurídico aplicable a los tratamientos que el mismo comprende, sino que añade requisitos adicionales que no se recogen en otros lugares del Anteproyecto y que se refieren a la prohibición de tratamientos ulteriores para fines distintos de los previstos en el Anteproyecto salvo disposición legal habilitante y la obligación de que esos tratamientos, si se desarrollan, se sometan al RGPD:

> "Los datos personales recogidos por las autoridades competentes para los fines establecidos en el artículo 1, apartado 1, no serán tratados para otros fines distintos de los establecidos en el artículo 1, apartado 1 salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento (UE) 2016/679 a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión".

Por consiguiente, debe procederse a la transposición del artículo 9.1 de la Directiva, considerando esta Agencia que el lugar adecuado podría ser el artículo 4 del Anteproyecto.

Por otro lado, el apartado 2 ha sido redacto siguiendo la sugerencia realizada por esta Agencia, al objeto de ejemplificar, siguiendo los Considerandos de la Directiva, cuáles pueden ser las condiciones específicas a las que se refiere el precepto:

> "2. Las condiciones específicas de tratamiento podrán ser, entre otras, la prohibición de transmisión de datos o de su utilización para fines distintos para los que fueron transmitidos o, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora".

No obstante, tal y como señala la Directiva, esas condiciones específicas solo pueden ser las que se prevean por el Derecho de la Unión o del Estado miembro que se aplica a la autoridad competente que ha de transmitir los datos,

Por consiguiente, el apartado 2 del artículo 10 debería quedar redactado de la siguiente forma:

"2. Las condiciones específicas de tratamiento deberán estar previstas en el Derecho de la Unión o en la legislación español y podrán ser, entre otras, la prohibición de transmisión de datos o de su utilización

para fines distintos para los que fueron transmitidos o, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora".

XV

El artículo 11.1, al definir las categorías especiales de datos, se aparta de la dicción literal del artículo 10 de la Directiva y del artículo 9.1 del RGPD, introduciendo una modificación que, a juicio de esta Agencia, resulta sustancial. Así, se refiere a los "datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física", mientras que las normas europeas lo hacen a "datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física". La sustitución de la coma de la norma europea por la conjunción disyuntiva "o" supone una modificación del concepto europeo de categorías especiales de datos, ya que los datos genéticos lo son en todo caso, mientras que los datos biométricos lo son únicamente en los supuestos en que su tratamiento esté dirigido a identificar de manera unívoca a una persona física.

Por ello, se propone modificar la redacción del artículo 11.1 para recoger lo previsto en la normativa europea: "datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física"

XVI

El artículo 12 procede a la transposición del artículo 11 de la Directiva, pero apartándose de la redacción original, con el siguiente texto:

> 1. No se adoptarán decisiones individuales automatizadas que produzcan efectos jurídicos negativos para el interesado o le repercutan significativamente de forma adversa. Estas decisiones no se basarán, únicamente, en un tratamiento automatizado de datos personales que comprenda la elaboración de perfiles, salvo que se autorice expresamente por una norma con rango de ley o por una norma del Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

La redacción es confusa, concluyendo que "No se adoptaran decisiones individuales automatizas… basadas, únicamente, en un tratamiento automatizado que comprenda la elaboración de perfiles". Se podría entender que sí están permitidas decisiones automatizadas no basadas en un

tratamiento automático y sí están permitidas las que no se basan en un tratamiento de perfiles. También permite la elaboración de perfiles de forma automática que tengan efectos jurídicos (mientras no se tomen decisiones automatizadas). De hecho, en la Directiva se hace distinción en el art. 11.2 y 11.3 entre decisiones automatizas y perfiles.

La redacción de la Directiva es mucho más clara, por lo que el artículo 12.1 debería redactarse de la siguiente forma:

> **"Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por una norma del Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada".**

Por otro lado, en el artículo 12 no se ha traspuesto el apartado 2 del correspondiente artículo 11 de la Directiva y que exige que las decisiones automatizadas que se basen en categorías especiales de datos requieren de unas medidas de salvaguarda específicas, que se diferencian, por el mero hecho de que se mencionen separadamente, de las generales que han de aplicarse ante cualquier decisión automatizada, teniendo en cuenta que, en el presente caso, no se refiere solo a los derechos y libertades sino que incluye "los intereses legítimos del interesado".

Por ello, debe introducirse un nuevo apartado con la siguiente redacción:

"Las decisiones a que se refiere el apartado 1 del presente artículo no se basarán en las categorías especiales de datos personales contempladas en el artículo 10, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado."

XVII

En relación con el artículo 13, relativo a las condiciones generales para el ejercicio de los derechos de los interesados, se han recogido las distintas observaciones realizadas por esta Agencia, si bien se ha modificado el

apartado 6 relativo a la solicitud de información complementaria cuando el interesado tenga dudas respecto a la identidad de la persona física que formule la solicitud, añadiendo que “Si no se proporciona esa información en el plazo de diez días, se le tendrá por desistido de su petición sin necesidad de dictar resolución a tal efecto”.

A este respecto, procede traer a colación lo ya manifestado en el Informe 122/2018 respecto a la regulación del derecho de acceso en el entonces artículo 14 y la posibilidad de tener por desistido de la solicitud en el caso de que no se concretara la información a la que se refiere, y que ha sido aceptada en el artículo 15.2 del nuevo texto remitido, suprimiendo la referencia al desistimiento:

> “Esta Agencia Española de Protección de Datos ha señalado reiteradamente que el ejercicio por el afectado de los derechos establecidos en la normativa de protección de datos trae directamente causa del reconocimiento del citado derecho por el artículo 18.4 de la Constitución y la jurisprudencia del Tribunal Constitucional, apareciendo ahora consagrado igualmente el derecho en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.
>
> De este modo, salvo en determinados supuestos, en que la normativa aplicable a un tratamiento concreto prevé un régimen especial de acceso, no cabe matizar el ejercicio del derecho a través de la normativa de protección de datos ni, aún en menor medida, aplicar las normas propias del procedimiento administrativo al ejercicio y atención de los citados derechos”.

Por consiguiente, aplicando idéntico criterio, debe suprimirse, en el artículo 13.6, la frase “Si no se proporciona esa información en el plazo de diez días, se le tendrá por desistido de su petición sin necesidad de dictar resolución a tal efecto”.

No obstante, teniendo en cuenta que, en este caso, las dudas acerca de la identidad impediría acceder a lo solicitado, se propone la inclusión del apartado siguiente:

> **“El plazo de que dispone el responsable del tratamiento para proporcionar la información solicitada por interesado no comenzará a contar sino desde que el interesado le facilite la información adicional complementaria necesaria solicitada por el responsable”.**

XVIII

La siguiente observación debe realizarse al artículo 14.2., relativo a La información adicional que, en casos concretos, debe facilitarse al interesado, habiéndose señalado en el Informe 122/2018 lo siguiente:

> No obstante, el apartado 2 del citado artículo dispone que la información a la que se refiere el artículo 13.2 de la Directiva "podrá" proporcionarse "atendiendo a las circunstancias del caso concreto".
>
> El artículo 13.2 de la Directiva establece claramente que "Además de la información indicada en el apartado 1, los Estados miembros dispondrán por ley que el responsable del tratamiento de los datos proporcione al interesado, en casos concretos, la siguiente información adicional, a fin de permitir el ejercicio de sus derechos". Quiere ello decir que el legislador de la Unión impone a los Estados miembros la obligación de establecer los supuestos en los que deberá facilitarse de forma obligatoria, y no meramente potestativa, la información adicional citada.
>
> Sin embargo, el texto informado se limita a decir que la información se podrá facilitar atendiendo a las circunstancias del caso concreto, sin establecer, en beneficio de los afectados los supuestos en que deberá inequívocamente facilitarse la información. Por ello, deberían especificarse los supuestos en los que la obligación a la que se refiere el artículo 13.1 del Proyecto habrá de facilitarse obligatoriamente.

Sin embargo, en el nuevo texto remitido no sólo no se identifican los supuestos, en beneficio de los afectados, sino que dicha carga se hace recaer en el propio afectado, al introducirse exigencia de que se trate de una "petición motivada".

Por ello, debería modificarse el artículo 14.2., siendo el legislador el que especifique los supuestos (esto es, los "casos concretos") en los que la información adicional debe facilitarse obligatoriamente. Ello supone asimismo la necesidad de suprimir la obligación de la "petición motivada", porque habrá sido el legislador quien habrá establecido que en determinados casos concretos "habrá que" proporcionar dicha información adicional.

XIX

En relación con la puesta a disposición de los afectados de medios de acceso remoto a sus datos a la que se refiere el artículo 15.3, no se ha recogido la observación realizada en el Informe 12272018, en el que se consideraba necesario, si se optaba por mantener esta posibilidad, garantizar que en caso de que el acceso remoto no ofrezca la totalidad de la información

exigida por el artículo 15.1. del Anteproyecto, el interesado tenga derecho a solicitarla .

Por lo tanto, incluyendo el deber de información no sólo el acceso a los datos personales que se están tratando, sino también al resto de información que establece **el propio precepto, debe completarse el artículo 15.3 a fin de garantizar que en caso de que el acceso remoto no ofrezca la totalidad de la información exigida por el artículo 15.1. del Anteproyecto, el interesado tenga derecho a solicitarla**

XX

En el artículo 16.3.b se añade como uno de los motivos para no suprimir los datos personales y, en cambio, limitar su tratamiento, que los datos personales deban ser conservados “en particular, por razones de seguridad”. Esas razones de seguridad, que no se determinan, se entienden como una especificación de la conservación necesaria a efectos probatorios. **La Directiva no contempla esa excepción, por lo la misma debe quedar limitada a los supuestos en que los datos personales hayan de conservarse a efectos probatorios, debiendo suprimirse del apartado b) del artículo 16.3 la frase “o, en particular, por razones de seguridad”.**

XXI

Por otro lado, en relación con los supuestos en que, legítimamente, se aprecien limitaciones al ejercicio de los derechos de los afectados, el artículo 17 de la Directiva prevé que los mismos puedan ejercitarse “a través” de la autoridad de control. Esta garantía, que no se prevé en el RGPD y que deriva de las especiales restricciones que se establecen en la Directiva, se ha transpuesto en el artículo 18 del Anteproyecto, si bien existe un error en el mismo en la remisión a los artículos respecto de los que resultaría de aplicación, ya que no se corresponden en el texto actual con los artículos.

Además, esta Agencia considera necesario fijar con precisión los supuestos en que procede su aplicación, tal y como realiza la Directiva, al objeto de evitar equívocos que permitan considerar que un interesado puede acceder directamente a la autoridad de control para ejercitar “a través” de ella, sus derechos en todo caso. En este punto, la transposición de la Directiva recogiendo los supuestos legales que van a permitir limitar los derechos de manera genérica, requerirá en todo caso una valoración previa por la autoridad competente atendiendo a las circunstancias del caso, de modo que ni el interesado ni la autoridad de control pueden saber, a priori, si concurren las circunstancias que legitiman la limitación.

Al objeto de definir con precisión los supuestos en que resultará de aplicación, evitando equívocos que puedan llevar a pensar a los afectados que pueden ejercitar directamente sus derechos a través de la autoridad de control, sin que previamente se haya pronunciado la autoridad competente, **se considera que la redacción del artículo 18 debería ser la siguiente**:

Artículo 18. Ejercicio de los derechos del interesado a través de la autoridad de protección de datos.

1. **En los casos en que se produzca un aplazamiento, limitación u omisión de la información a que se refiere el artículo 14, una denegación del ejercicio del derecho de acceso en los términos previstos en el apartado 17.1 o una limitación en la información que deberá proporcionarse al interesado en los casos de denegación de los derechos de rectificación y supresión contemplados en el artículo 16**, el interesado podrá ejercer sus derechos a través de la autoridad de control. El responsable del tratamiento informará al interesado de esta posibilidad.

2. Cuando, en virtud de lo establecido en el apartado anterior, sea la autoridad de protección de datos la que ejercite los derechos, ésta deberá informar al interesado, al menos, de la realización de todas las comprobaciones necesarias o la revisión correspondiente y de su derecho a interponer recurso contencioso-administrativo.

XXII

El artículo 20 de la Directiva, relativo a la “Protección de datos desde el diseño y por defecto” se refiere a “las medidas técnicas y organizativas apropiadas, como por ejemplo la seudonimización, concebidas para aplicar los principios de protección de datos, como por ejemplo la minimización de datos, de forma efectiva y para integrar las garantías necesarias en el tratamiento, de tal manera que este cumpla los requisitos de la presente Directiva y se protejan los derechos de los interesados”.

Transponiendo dicho precepto, el artículo 21.1 del Anteproyecto ha incluido una frase final en la que se señala que “En la medida de lo posible, se podrá adoptar la seudonimización o la minimización de los datos personales”.

No obstante, dicha frase no se corresponde con lo establecido en la Directiva. La seudonimización, que el RGPD define como “el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a

garantizar que los datos personales no se atribuyan a una persona física identificada o identificable" es una de las garantías adecuadas que el responsable puede adoptar para que el tratamiento se ajuste a los principios de la Directiva, entre los que se encuentra el principio de minimización. En este sentido, cuando el artículo 20 de la Directiva se refiere a la seudonimización, lo hace como ejemplo de "las medidas técnicas y organizativas apropiadas concebidas para cumplir los principios de protección de datos" y cuando se refiere a la minimización de datos, es como ejemplo de esos principios.

Esta distinción tiene una especial trascendencia, ya que el principio de minimización de datos, no es disponible para el responsable, no es algo que "en la medida de lo posible, se podrá adoptar", sino que su observancia es en todo caso imperativa para el mismo, como resulta del artículo 4 del Anteproyecto, y su inobservancia, una infracción muy grave, según el artículo 50.1.a) del mismo.

Por ello, debe modificarse la última frase del artículo 21.1 del Anteproyecto, proponiéndose la siguiente redacción:

> "En la medida de lo posible, se podrá adoptar la seudonimización de los datos personales a los efectos de contribuir a la aplicación de los principios establecidos en la presente Ley y, en particular, el de minimización de datos personales".

XXIII

En cuanto a la necesidad de realizar una evaluación de impacto relativa a la protección de datos, la redacción contenida en el artículo 28.1 del Anteproyecto (Cuando sea probable que un tipo de tratamiento suponga un alto nivel de riesgo para los derechos y libertades de las personas físicas, como consecuencia de la utilización de nuevas tecnologías o por razón de su naturaleza, alcance, contexto o fines, el responsable del tratamiento llevará a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento) no se corresponde exactamente con la contenida en el artículo 27 de la Directiva, que a su vez es copia literal de la recogida en el artículo 35.1 del RGPD (Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales).

Teniendo en cuenta que el RGPD es de aplicación directa a los tratamientos sometidos a su ámbito de aplicación, y con el fin de evitar

problemas interpretativos que puedan llevar a inferir alguna diferencia respecto a la necesidad de evaluación de impacto, **sería conveniente unificar ambas redacciones, de modo que el artículo 28.1 quede redactado de igual modo que la Directiva y el RGPD:**

> **"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales".**

XXIV

El artículo 30.1, siguiendo la recomendación realizada por esta Agencia, ha incluido una referencia al Esquema Nacional de Seguridad:

> 1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 11. En particular, deberán cumplir con las medidas incluidas en el Esquema Nacional de Seguridad con arreglo a sus disponibilidades técnicas y presupuestarias.

Teniendo en cuenta que las autoridades competentes a efectos de la Directiva están incluidas en el artículo 77 de la LOPDGDD, las mismas ya están sujetas a la obligación que establece la disposición adicional primera.2 de la misma:

> 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

Por otro lado, las medidas a adoptar no serán solo las del Esquema Nacional de Seguridad, sino las que resulten del correspondiente análisis de riesgos al que se refiere el propio precepto. En este sentido, en el Informe de esta Agencia 170/2018, de 12 de noviembre de 2018, relativo a la compatibilidad funcional del delegado de protección de datos del RGPD y el

responsable de seguridad del Esquema Nacional de Seguridad, se señalaba lo siguiente:

> "Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio".

Y tal y como ha venido informando reiteradamente esta Agencia al analizar las políticas de seguridad de la información de los diferentes ministerios, en el caso de que las medidas a implantar como consecuencia del análisis de riesgos previsto en la normativa sobre protección de datos personales, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberían prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por dicha normativa.

Por ello, la última frase del artículo 30.1 debería redactarse de la siguiente manera:

"En particular, deberán aplicar a los tratamientos de datos personales, al menos, las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad".

XXV

De acuerdo con el artículo 31.1 "Los responsables del tratamiento designarán un delegado de protección de datos. No será obligatorio designarlo cuando el tratamiento de datos personales tenga fines jurisdiccionales".

No obstante, el artículo 32.1. de la Directiva, que se transpone en el citado precepto, lo que prevé es que "Los Estados miembros podrán eximir de esa obligación a los tribunales y demás autoridades judiciales independientes cuando actúen en ejercicio de sus competencias judiciales.

Por consiguiente, la redacción de la última frase del artículo 31.1 del Anteproyecto debería ser la siguiente:

"No estarán obligados a designarlo los órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales lo realicen con fines jurisdiccionales".

XXVI

El Capítulo V del Anteproyecto procede a la regulación de las "Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea u organizaciones internacionales" acomodándose, con carácter general, a lo previsto en la Directiva, tal y como se señaló en nuestro Informe 122/2018.

No obstante, es de destacar que es el único Capítulo en el que, apartándose de las disposiciones de la Directiva que se refiere a las autoridades competentes, se introduce la distinción entre autoridad y funcionario público. Dicha diferenciación, a juicio de esta Agencia, puede introducir distorsiones que puedan dar lugar a transferencias no autorizadas por la Directiva. El funcionario púbico, o es autoridad competente por reunir los requisitos establecidos por la Directiva y el Anteproyecto, o no lo es, en cuyo caso no le resultan de aplicación sus preceptos. Esta diferenciación puede tener aún mas relevancia si tenemos en cuenta que se trata de transferencias a terceros países, cuyas estructuras administrativas pueden diferir notoriamente de las nuestras.

Por todo ello, se considera necesario que en el Anteproyecto se sustituyan las referencias recogidas en los artículos 36, 37, 39 y 40 a autoridades y funcionarios públicos, españoles o extranjeros, por "autoridades competentes".

Por otro lado, la redacción dada al apartado c) del artículo 40.1 del Anteproyecto no se corresponde con la de la letra c) del artículo 39.1 de la Directiva, y puede dar lugar a problemas interpretativos. El Anteproyecto exige como uno de los requisitos para que se puedan realizar, con carácter excepcional, las transferencias directamente a los destinatarios (que no tienen por qué ser autoridades competentes) "Que la autoridad competente que realiza la transferencia a una autoridad competente de un tercer país a los fines que contempla el artículo 1 considere que dicha transferencia resultaría ineficaz o inadecuada, en particular, cuando la transferencia no pueda efectuarse dentro de plazo.". Sin embargo, lo que contempla la Directiva como condición para proceder a la transferencia es el supuesto de que el responsable que las realiza considere que no sería eficaz hacerlo por la vía habitual, que sería a través de la autoridad competente en el país tercero receptor:

> "la autoridad competente de la transferencia considere que la transferencia a una autoridad competente del tercer país a los fines que contempla el artículo 1, apartado 1, resulta ineficaz o inadecuada, sobre todo porque no pueda efectuarse dentro de plazo".

Por ello, la letra c) del artículo 40.1 del Anteproyecto debería redactarse de la siguiente forma:

> **"Que la autoridad competente que realiza la transferencia considere que la transferencia a una autoridad competente de un tercer país a los fines que contempla el artículo 1 resultaría ineficaz o inadecuada, en particular, cuando la transferencia no pueda efectuarse dentro de plazo."**

XXVII

El Capítulo VI del Anteproyecto se refiere a la Autoridades de protección de datos, transponiendo el Capítulo VI de la Directiva, que lleva por rúbrica "Autoridades de control independientes". Teniendo en cuenta que una de las características esenciales sobre las que pivota el régimen europeo de protección de datos personales es la garantía de la independencia de las autoridades de control, tal y como detenidamente se regula en el artículo 42 de la Directiva, **se considera imprescindible que se recoja dicha circunstancia en el propio título del Capítulo VI, de modo que se refiere a las "Autoridades de control independientes**".

Partiendo de lo anterior, el artículo 41 comienza con la enumeración de dichas autoridades a los efectos de la presente Ley Orgánica, en la que siguiendo las observaciones formuladas por esta Agencia se limita a la Agencia Española de Protección de Datos y a las autoridades autonómicas de protección de datos.

A este respecto, y en relación con el régimen jurídico aplicable a las autoridades de control, el Informe 122/2018 señalaba lo siguiente:

> Partiendo de lo anterior, el régimen de las dos autoridades de control a los efectos de la Directiva; es decir, la Agencia Española de Protección de datos y las autoridades autonómicas de protección de datos, incluyendo las obligaciones de cooperación entre las mismas, aparece ya recogido en el Título VII del Proyecto de Ley Orgánica de protección de datos de carácter personal y, en el caso de las autoridades autonómicas, en sus normas de creación y regulación.
>
> Asimismo, tanto la Agencia Española como las autoridades autonómicas están sometidas a lo establecido en el artículo 59 del Reglamento general de protección de datos, conforme al cual "Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las

demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité".

De este modo, no sería preciso establecer más especialidades en el citado artículo 51 que las referidas a la aplicación de lo establecido en el Título VII del Proyecto y la normativa autonómica que sea de aplicación a las autoridades autonómicas.

A este respecto, se proponía la siguiente redacción: "Dichas autoridades se someterán a lo establecido en el Título VII de la Ley Orgánica xxx/2018, de XX de XX y en sus normas de creación, así como en las que desarrollen las mismas" Sin embargo, el nuevo texto remitido no ha recogido dicha observación, estableciendo disposiciones específicas respecto del régimen jurídico aplicable a las mismas:

> Estas autoridades se regirán por esta ley orgánica, por su normativa específica, por los artículos 52 a 54 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por sus disposiciones de aplicación.
>
> Estas autoridades cooperarán en el ejercicio de sus funciones de acuerdo con lo previsto en los artículos 58 y 59 de la Ley Orgánica 3/2018, de 5 de diciembre.
>
> La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.
>
> 3. Las autoridades de protección de datos deberán realizar un informe anual sobre su actividad, de carácter público y que deberá ponerse en conocimiento de las Cortes Generales, del Gobierno y, en su caso, de las Asambleas Legislativas y de los Gobiernos de las Comunidades Autónomas, de la Comisión Europea y del Comité Europeo de Protección de Datos, así como del Defensor del Pueblo e instituciones autonómicas análogas.

En cuanto a la referencia a la propia Ley Orgánica -esto es, a la que desarrolla la Directiva 2016/680, esta ley orgánica resultará de aplicación en cuanto a los tratamientos sometidos a la misma, como ocurre, por ejemplo, en relación con las funciones y potestades reguladas en sus artículos 42 y 43, en los cuales se han tenido en cuenta las observaciones realizadas por esta Agencia, **si bien se estima conveniente modificar el artículo 43.b) incluyendo la referencia a la orden de comunicación al interesado de la**

violación de la seguridad de los datos personales, con el objeto de incorporar a las funciones de las autoridades de control la competencia atribuida a las mismas por el artículo 32.4 del Anteproyecto.

Sin embargo, en relación con el resto de su régimen jurídico, existiendo una norma general (la LOPDGDD) que procede a su regulación, incluida la necesaria garantía de su independencia a la que anteriormente se hacía referencia, y al objeto de evitar duplicidades e, incluso, problemas de interpretación, se insiste en la conveniencia de que en el artículo 41 se recoja únicamente la remisión a dicha norma general (la LOPDGDD) y, en cuanto a las autoridades autonómicas, a sus normas de creación, proponiéndose la siguiente redacción:

> **"Dichas autoridades se regirán por esta Ley Orgánica respecto de los tratamientos sometidos a la misma, y por lo establecido en el Título VII de la Ley Orgánica 3/2018, de 5 de diciembre, y en sus normas de creación, así como por lo que establezcan las normas que a su vez desarrollen éstas".**

Por último, deben recordarse los comentarios que, en cuanto a las competencias atribuidas al Consejo General del Poder Judicial por la LOPJ se realizaban en nuestro Informe 122/2018,:

> Es preciso, ante todo llevar a cabo una clarificación en relación con la enumeración llevada a cabo por el Anteproyecto, teniendo en cuenta que el artículo 45.2 de la Directiva establece que "Los Estados miembros dispondrán que cada autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función judicial. Los Estados miembros podrán disponer que su autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por otras autoridades judiciales independientes en el ejercicio de su función judicial"
>
> Así, recuerda el considerando 80 de la Directiva que "Aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales y otras autoridades judiciales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los órganos jurisdiccionales actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones. Esta excepción debe limitarse a actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho del Estado miembro. Los Estados miembros pueden disponer también que la competencia de la autoridad de control no abarque el

tratamiento de datos personales realizado por otras autoridades judiciales independientes en el ejercicio de su función jurisdiccional, por ejemplo la fiscalía. En todo caso, el cumplimiento de las normas de la presente Directiva por los órganos jurisdiccionales y otras autoridades judiciales independientes debe estar sujeto siempre a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta".

Quiere ello decir que sin perjuicio de las competencias que al Consejo General del Poder Judicial atribuye el artículo 236 nonies de la Ley Orgánica del Poder Judicial, dicho Consejo no puede ser considerado como autoridad competente a los efectos de la Directiva objeto de trasposición por el Anteproyecto sometido a informe.

Ello exige que el precepto que enumera las autoridades de protección de datos a los efectos de la Ley debería tener en cuenta esta previsión, a fin de no someter al Consejo general del Poder Judicial al régimen general de la Ley sino establecer en todo caso que la enumeración de las autoridades de control se lleva a cabo sin perjuicio de las competencias que al Consejo General del Poder Judicial otorga la Ley Orgánica del Poder Judicial.

Por ello, y al objeto de clarificar el régimen competencial, sería conveniente añadir un último apartado en el que se indicara que "Lo dispuesto en el apartado anterior se entiende sin perjuicio de las competencias que respecto de los tratamientos de datos con fines jurisdiccionales atribuye al Consejo General del Poder Judicial el artículo 236 nonies de la Ley Orgánica 6/1985, de 1 de julio."

XXVIII

El artículo 56 de la Directiva establece que "Los Estados miembros dispondrán que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una operación de tratamiento ilícito o de cualquier acto que vulnere las disposiciones nacionales adoptadas con arreglo a la presente Directiva tenga derecho a recibir una indemnización del responsable o de cualquier autoridad competente en virtud del Derecho del Estado miembro por los daños y perjuicios sufridos".

El artículo 46 del Anteproyecto, transponiendo dicho mandato, ha incluido en el mismo el régimen de responsabilidad de las autoridades de control, que ya está establecido en las normas que regulan las mismas y a las que debería remitirse el Anteproyecto, conforme a lo ya indicado en el apartado anterior, teniendo en cuenta que el citado precepto de la Directa se está refiriendo a los tratamientos ilícitos y actos contrarios a la Directiva que se realicen por responsables y autoridades competentes.

Por ello, debería suprimirse del artículo 46 del Anteproyecto la referencia a las autoridades de control.

XXIX

El Capítulo VIII del Anteproyecto regula el régimen sancionador, comenzando en su artículo 48 con la enumeración de los sujetos responsables. A este respecto, el Informe 122/2018 ya señalaba lo siguiente:

> En cuanto a la delimitación de los sujetos obligados, el artículo 50 del Proyecto se refiere, además de a los responsable y encargados de los tratamientos a "los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea" y "el resto de las personas físicas o jurídicas obligadas por esta Ley Orgánica".
>
> En cuanto a los representantes, si bien es cierto que excepcionalmente podría darse la circunstancia de que un encargado del tratamiento no se encontrase establecido en el territorio de la Unión, esta circunstancia no será nunca posible en el caso de los responsables, por cuanto sólo tendrán esta consideración las autoridades competentes, que por definición sí se encuentran en dicho territorio, perteneciendo en todo caso al sector público.
>
> Asimismo, en cuanto a los restantes sujetos, no se alcanza a determinar quiénes podrían ser éstos, dado que las disposiciones de la Directiva, y en consecuencia del Anteproyecto se aplicarían a las autoridades competentes conforme a su artículo 2.2 y, a lo sumo a sus encargados del tratamiento.
>
> Por todo ello, procedería suprimir la letra d) del artículo 50 de Proyecto, así como la referencia al responsable del tratamiento en el caso de la letra c).

Sin embargo, dicha observación no se ha recogido en el nuevo texto, por lo que debe insistirse en la misma, dado que la Directiva no se aplica extraterritorialmente, por lo que los responsables o encargados no establecidos no tienen que nombrar representante, que en el supuesto contemplado en el RGPD y en la LOPDGDD. Además, y más importante, los responsables a los que se dirige la Directiva son autoridades públicas de cada uno de los Estados miembros. En todo caso, podría darse el supuesto de encargados privados que puedan no estar establecidos en la UE.

Y siendo los únicos sujetos obligados por la Directiva los responsables y encargados del tratamiento, debe suprimirse la referencia que se hace al resto de personas físicas y jurídicas en su letra d), que tal y como se ha indicado al analizar el artículo 5 y se volverá posteriormente a tratar, derivan exclusivamente de la introducción en una normativa de protección de datos personales de un deber de colaboración ajeno a la misma que produce distorsiones en cuanto a su aplicación.

Por ello, debe procederse a la supresión de la letra d) del artículo 48 así como la referencia al responsable del tratamiento en el caso de la letra c)

XXX

En cuanto a la tipificación de las conductas infractoras, el nuevo texto remitido no ha aceptado la observación de esta Agencia relativa a la conveniencia de remitirse a las conductas tipificadas en la Ley Orgánica 3/2018, estableciendo un régimen uniforme y garantizando la seguridad jurídica de los operadores.

Aunque esta Agencia mantiene la conveniencia de recoger en el Anteproyecto una remisión a la Ley Orgánica 3/2018, la posibilidad de tipificar conductas específicas aparece expresamente recogida en el artículo 57 de la Directiva, a cuyo tenor “Los Estados miembros establecerán las normas en materia de sanciones aplicables a las infracciones de las disposiciones adoptadas con arreglo a la presente Directiva y tomarán todas las medidas necesarias para garantizar su cumplimiento. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias”.

No obstante, en dicha tipificación debería mantenerse una homogeneidad respecto de las conductas tipificadas en el régimen general de protección de datos, pudiendo modularse en atención a las singularidades de los tratamientos objeto de la misma y teniendo especialmente en cuenta, tal y como se ha señalado en los sucesivos informes de esta Agencia, que el régimen de la Directiva es más restrictivo que el previsto en el RGPD.

En este sentido, en relación con las infracciones muy graves del artículo 50, atendiendo a la mayor limitación del derecho fundamental a la protección de datos que supone el régimen de la Directiva, su régimen no puede resultar más benévolo para el infractor que el establecido con carácter general. A este respecto, siendo los principios y garantías que se establecen en el artículo 4 del Anteproyecto y que se corresponden con los del Artículo 5 del RGPD, su vulneración debe suponer, con carácter general, una infracción muy grave, tal y como se recoge en el artículo 72.1. de la Ley Orgánica 3/2018**, debiendo suprimirse el adverbio “gravemente” del artículo 50.a) del Anteproyecto**. Por la misma razón en caso de no cumplirse el principio de licitud al faltar la

base jurídica que legitime el tratamiento, **debe suprimirse de la letra b) del artículo 50 la frase "siempre que causen perjuicios de carácter muy grave a los interesados"**. **Asimismo, respecto de la letra q) del artículo 50, relativa a la obligación de bloqueo, debe suprimirse la frase "y se causen perjuicios de carácter muy grave a los interesados".**

Igualmente, si en el régimen general se tipifica como infracción muy grave, en el artículo 72.1 k) el impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, con mayor razón dicha conducta debe considerarse infracción muy grave en el anteproyecto, teniendo en cuenta que el mismo establece la posibilidad de adoptar mayores limitaciones y restricciones respecto del ejercicio de dichos derechos, **debiendo suprimirse de la letra ñ) del artículo 50 la frase "siempre que se causen perjuicios de carácter muy grave para los interesados" así como suprimirse la letra h) del artículo 51 que tipifica como infracción grave "El impedimento, la falta de atención o la obstaculización de los derechos de acceso, rectificación, supresión o limitación del interesado, siempre que no concurra alguna de las causas de restricción de estos derechos y no constituya infracción muy grave" ya que, salvo en los casos en que sea ilícito penal, su infracción debe considerarse en todo caso como muy grave.**

Por otro lado, atendiendo a las importantes competencias que tanto el RGPD como la Directiva atribuyen a las autoridades de protección de datos, deben, asimismo, homogeneizarse las infracciones relacionadas con la actuación de las mismas, sin rebajarse la gravedad de las infracciones, por lo que al igual que hace el artículo 72, letras m, ñ y o, de la Ley Orgánica 3/2018, **deben tipificarse como infracción muy grave:**

- **El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de las potestades que le confiere el artículo 43 de esta Ley Orgánica.**
- **No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.**
- **La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.**

Asimismo, debe modificarse la letra o) del artículo 51.1 del Anteproyecto, que tipifica como infracción grave "La falta de cooperación, la actuación negligente o el impedimento de la función inspectora de la autoridad de protección de datos" añadiendo la frase "en los supuestos no contemplados en el artículo 50 de esta Ley Orgánica".

Por otro lado, en cuanto a las infracciones graves, **debe tipificarse como infracción en el artículo 51.1, además del incumplimiento de la obligación de designar un delegado de protección de datos, prevista en su letra e), el "no posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones". Asimismo, deberá tipificarse como infracción grave "el tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 29 de esta Ley Orgánica".**

En relación con las infracciones leves tipificadas en el artículo 52, la letra c) se refiere al "incumplimiento de los plazos de revisión exigibles en virtud del artículo 6". Tal y como se ha indicado en otro apartado de este informe, el artículo 6 procede a la transposición del artículo 5 de la Directiva, relativo a la conservación de los datos personales, que establece una obligación específica, en este ámbito, de fijar plazos apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación de los datos personales. Tratándose de una previsión específica, que viene a incrementar las garantías de los afectados atendiendo al régimen más restrictivo de la Directiva, esta Agencia considera que su incumplimiento no debería tipificarse como infracción leve, sino, al menos, como infracción grave. **Por tanto, debe modificarse el artículo 51 para incluir como infracción grave "el incumplimiento de los plazos de revisión exigibles en virtud del artículo 6", suprimiéndose la letra c) del artículo 52.**

Por otro lado, deben suprimirse de las conductas tipificadas aquellas que, estando previstas en el régimen general, no se corresponden con las especialidades del régimen especial contenido en el Anteproyecto. Así, **debe suprimirse la letra c) del artículo 50 relativa al "incumplimiento de los requisitos para la validez del consentimiento exigidos por el artículo 72 de la Ley Orgánica 3/2018, de 5 de diciembre, siempre que se causen perjuicios de carácter muy grave a los interesados",** ya que como señalan los Considerandos 35 y 37 de la Directiva el consentimiento del interesado no debe constituir en sí mismo un fundamento jurídico para que las autoridades competentes procedan al tratamiento de datos personales conforme a la misma. Por la misma razón, **debe suprimirse la referencia al consentimiento del interesado que se contiene en la letra e) del artículo 50 y en la letra d) del artículo 51.**

XXXI

Especial referencia debe realizarse a la tipificación de las conductas relativas al incumplimiento del deber de colaboración establecido en el artículo

5 del Anteproyecto, y que se tipifican como infracción muy grave en la letra o) del artículo 50 (La negativa a proporcionar a las autoridades competentes la información necesaria para la prevención, detección, investigación o enjuiciamiento de infracciones penales, para la ejecución de sanciones penales o para la protección y prevención frente a las amenazas contra la seguridad pública, siempre que se deriven perjuicios o riesgos de carácter muy grave para los interesados) y como infracción grave en la letra n) del artículo 51 (La negativa a proporcionar a las autoridades competentes la información necesaria para la prevención, detección, investigación o enjuiciamiento de infracciones penales, la ejecución de sanciones penales o para la protección y prevención frente a las amenazas contra la seguridad pública).

Al margen de tipificarse idéntica conducta con diferente gravedad, y tal y como ha venido incidiendo reiteradamente esta Agencia, el citado artículo 5 del Anteproyecto no supone transposición de artículo alguno de la Directiva, debiendo tenerse en cuenta las observaciones que al mismo se realizan en el apartado X del presente, en el que se incide en la relevancia que al efecto tiene la normativa específica que regula el deber de colaboración con las diferentes autoridades competentes. Por todo ello, teniendo en cuenta que tanto el Código Penal como dichas normas especiales tipifican diferentes conductas derivadas del incumplimiento del deber de colaboración y que el mismo no guarda relación directa con el régimen de protección de datos personales contenido en la Directiva y en el Anteproyecto, el régimen sancionador debería ser el previsto en la citada normativa especial.

Por consiguiente, se considera necesario suprimir la letra o) del artículo 50 y la letra n) del artículo 51.

Asimismo, y tal y como se ha indicado anteriormente, teniendo en cuenta que el presente supuesto es el único que ampararía la aplicación del régimen sancionador, al "resto de las personas físicas o jurídicas obligadas por esta ley orgánica" previsto en el artículo 48 relativo a los sujetos responsables, **debe procederse a la supresión de la letra d) del artículo 48**.

Y del mismo modo, la inclusión de dichas conductas es la que justificaría, una vez salvada la aplicación de la normativa general de protección de datos personales, la referencia a otras leyes que se contiene en el artículo 49, así como las normas de conflicto que el mismo establece, por lo que debería procederse igualmente a la supresión en dicho precepto de la referencia en otras leyes, **limitándose el artículo 49, tal y como se indicó en el Informe 122/2018 a establecer que cuando la conducta fuese constitutiva de infracción tanto de la Ley general como del Anteproyecto se aplicarán las disposiciones sancionadoras de la Ley general; es decir, de la Ley Orgánica 3/2018, de 5 de diciembre.**

En otro caso, el mantenimiento de preceptos que establecen responsables y tipifican y sancionan conductas ajenas al ámbito propio de la norma y que no implican tratamientos de datos personales (más bien al contrario, el incumplimiento del deber de colaboración supondría que no ha habido dicho tratamiento), solo produce distorsiones en cuanto a su aplicación, debiendo tenerse en cuenta que las únicas autoridades competentes para sancionar las conductas contrarias a lo previsto en el Anteproyecto son las autoridades de control.

XXXII

Por último, en cuanto a las conductas típicas, deben corregirse algunos errores materiales, como es la reiteración de la misma conducta en las letras f) y l) del artículo 50 o la errata del apartado d) del artículo 52 sustituyendo “y a los destinatarios” por “de los destinatarios”.

XXXIII

En relación con las sanciones el artículo 53.1 ha recogido la observación formulada por esta Agencia, remitiendo respecto de los responsables incluidos en el artículo 77.1 de la Ley Orgánica 3/2018, a lo previsto en dicho precepto.

Asimismo, en su apartado 2 ha recogido la remisión a la normativa general de protección de datos al objeto de determinar la cuantía de la sanción al resto de sujetos infractores. Sin embargo, se ha mantenido la cuantía de las sanciones establecidas en el texto anterior, por lo que se considera conveniente reiterar lo ya señalado en el Informe 122/2018:

> Respecto de los restantes sujetos, el Anteproyecto establece unas cuantías de 6.000 a 24.000 euros para las infracciones leves, de 24.001 a 60.000 euros para las graves y de 60.001 a 240.000 euros para las muy graves.
>
> No consta en el Proyecto remitido justificación alguna de las cuantías establecidas por este precepto, que por otra parte no coinciden ni con las establecidas en la vigente Ley Orgánica 15/1999 ni con las que preveía el Anteproyecto de Ley Orgánica sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, por el que se trasponía la Directiva (UE) 2016/681, que ya fue objeto de informe por esta Agencia.
>
> Por otra parte, la reducción de los límites establecidos en el Anteproyecto respecto de los previstos en la Ley Orgánica 15/1999 genera la paradójica consecuencia de que, habiéndose adoptado una norma de la Unión Europea encaminada a reforzar las garantías de los derechos fundamentales de los afectados en relación con los

tratamientos de datos sometidos a la misma, la entrada en vigor de la Ley de trasposición al derecho interno de dicha norma implicaría automáticamente una drástica reducción de las cuantías de las sanciones que podrían imponerse en caso de incumplimiento de dicha disposición, que en algunos casos se reducirían en un 80% respecto de las recogidas en la Ley Orgánica, como sucedería en el caso de las sanciones por la comisión e infracciones leves.

Por este motivo, y a fin de garantizar adecuadamente los mencionados derechos deberían revisarse las cuantías de las sanciones a las que se refiere el artículo 56.2 del Proyecto manteniendo, cuando menos, las cuantías previstas actualmente en la Ley Orgánica 15/1999, si bien sí sería posible incrementar la cuantía mínima de las sanciones por la comisión de infracciones leves hasta los 6.000 euros que recoge la norma.

XXXIV

El artículo 54 del Anteproyecto regula la prescripción de las infracciones y sanciones, apartándose en la nueva redacción del régimen general contenido en la Ley Orgánica 3/2018. Teniendo en cuenta que la esencia de la presente disposición es transponer una Directiva en materia de protección de datos personales, razones de seguridad jurídica y la necesidad de no establecer un régimen más benévolo en un ámbito más restrictivo con los derechos de los afectados que el previsto con carácter general hacen necesario, tal y como se viene argumentando en el presente informe, su equiparación a lo previsto en la Ley Orgánica 3/2018.

En este sentido, si bien el texto inicialmente informado por esta Agencia recogía unos plazos de prescripción de las infracciones que se correspondían con los contemplados en los artículos 72 a 74 de la Ley Orgánica 3/2018 (tres años para las infracciones muy graves, dos años para las infracciones graves y uno para las leves), la nueva redacción del artículo 54 ha reducido dichos plazos:

1. Las infracciones administrativas tipificadas en esta ley prescribirán a los seis meses, al año o a los dos años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

Por consiguiente, es necesario modificar el apartado 1 del artículo 54, adecuando los plazos de prescripción a lo previsto en la normativa general, de modo que las infracciones administrativas tipificadas en esta ley prescribirán al año, a los dos años o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

Por las mismas razones, la interrupción de la prescripción debe seguir el mismo régimen que en la normativa general, previendo el artículo 75 de la Ley

Orgánica 3/2018 la reanudación del plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor, y no de un mes tal y como se establece en el segundo párrafo del artículo 54.1 del Anteproyecto. Además, hay que tener en cuenta que los procedimientos tramitados por las autoridades de protección de datos en el ámbito del Anteproyecto, se rigen por lo dispuesto en el Título VIII de la Ley Orgánica 3/2018, al que se remite el artículo 45 del Anteproyecto.

Por ello, debe modificarse la redacción del tercer párrafo del artículo 54.1 del Anteproyecto para ajustarlo a lo previsto en el artículo 75 de la Ley Orgánica 3/2018:

"Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor."

Por la misma razón debe modificarse el régimen de la prescripción de las sanciones, ya que si bien en este caso los plazos se acomodan a lo previsto en el artículo 78 de la Ley Orgánica 3/2018, en la reanudación del cómputo del plazo interrumpido se reduce el plazo a un mes desde que se paraliza el procedimiento, en lugar de los seis meses previstos en la normativa general.

Por ello, debe modificarse la redacción del segundo párrafo del artículo 54.2 del Anteproyecto para ajustarlo a lo previsto en el artículo 78.3 de la Ley Orgánica 3/2018:

> **"La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor."**

Por otro lado, el artículo 55 regula la caducidad del procedimiento, cuya supresión ya se propuso en el Informe 122/2018, teniendo en cuenta que la normativa aplicable a los procedimientos tramitados por las autoridades de protección de datos es la contemplada en el Título VIII de la Ley Orgánica 3/2018, al que se remite el artículo 45 del Anteproyecto, y cuyo artículo 64 contiene normas específicas relativas a las formas de iniciación de los procedimientos y a su duración.

Procede, por consiguiente, suprimir el artículo 55 del Anteproyecto.

XXXV

Procede, a continuación, analizar la disposición adicional segunda introducida en el nuevo texto remitido, relativa a los ficheros y registros de población:

> Disposición adicional segunda. Ficheros y Registro de Población de las Administraciones Públicas.
> 1. Las autoridades competentes podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias.
>
> 2. Los datos obtenidos tendrán como único propósito el cumplimiento de los fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública y la comunicación de estas autoridades con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas.

En primer lugar, hay que destacar que pese a la unificación en el precepto, el apartado 1 contempla el acceso a datos de diferente naturaleza sometidos a diferentes regímenes jurídicos en cuanto al acceso a los mismos por su normativa específica: los datos de habitantes y los datos del censo electoral.

En cuanto al acceso a los datos de los padrones municipales, el Padrón Municipal de habitantes es un registro administrativo que se encuentra regulado por la Ley 7/1985, de 2 de abril, de Bases del Régimen Local, cuyo artículo 16, apartado primero, señala que “El Padrón municipal es el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. Las certificaciones que de dichos datos se expidan tendrán carácter de documento público y fehaciente para todos los efectos administrativos”.

En cuanto al carácter de los datos que obran en el Padrón municipal, la jurisprudencia ha declarado de manera reiterada que: “Los datos del padrón son confidenciales pues contienen datos propios del ámbito de privacidad de los empadronados como se infiere de la simple lectura del artículo 16.2 de la Ley de Bases de Régimen Local donde se exponen los datos que obligatoriamente constan en el Padrón y que están sometidos a la Ley Orgánica de Protección de Datos de Carácter Personal con la única excepción contenida en el artículo 16.3 de dicha Ley de Bases”.

En relación con la posible cesión de sus datos, el apartado tercero del precepto citado recoge los principios que rigen la transmisión y utilización de los datos del Padrón Municipal, al disponer que “Los datos del Padrón Municipal se cederán a otras Administraciones públicas que lo soliciten sin

consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia".

Dicho precepto se desarrolla por el artículo 53 del Real Decreto 1690/1986, de 11 de julio, por el que se aprueba el Reglamento de Población y Demarcación Territorial de las Entidades Locales.

"1. El padrón municipal es el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. Las certificaciones que de dichos datos se expidan tendrán carácter de documento público y fehaciente para todos los efectos administrativos.

2. Los datos del padrón municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

Fuera de estos supuestos, los datos del padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. En todo caso, el padrón municipal está sujeto al ejercicio por parte de los vecinos de los derechos de acceso y de rectificación y cancelación regulados en los artículos 14 y 15 de la Ley Orgánica 5/1992, de 29 de octubre."

El artículo 16.3 de la Ley de Bases de Régimen Local fue extensamente interpretado por el Tribunal Constitucional en su sentencia 17/2013, de 31 de enero de 2013, en la que determinó la constitucionalidad del mismo.

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).

Partiendo de dicha normativa y jurisprudencia, durante la vigencia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter

Personal, la Agencia Española de Protección de Datos ha venido diferenciando dos supuestos posibles de cesión de datos, en función de que el cesionario tuviera o no la condición de Administración Pública.

En el caso de que el cesionario tuviera la condición de Administración Pública, esta Agencia ha considerado que la expresión “datos del Padrón municipal” que se emplea en el artículo 16.3 de la LBRL se refiere únicamente a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio, por lo que la cesión de los datos contenidos en el Padrón municipal de habitantes amparada en la normativa reguladora del mismo únicamente será posible en caso de que concurran dos requisitos acumulativos:

- En primer lugar, que la misma tenga por finalidad el ejercicio por la administración cesionaria de sus competencias.

- En segundo lugar, que el dato correspondiente a la residencia o domicilio del afectado resulte relevante para el citado ejercicio.

Por ello, cualquier cesión de los datos del Padrón deberá fundarse en la necesidad por la Administración cesionaria, en el ejercicio de sus competencias, de conocer el dato del domicilio de la persona afectada, dado que del artículo 4.2 de la LOPD de 1999, y hoy en el art. 5.1.b) RGPD, se deriva la imposibilidad del tratamiento de los datos para fines diferentes de los que motivaron su recogida, salvo que así lo consienta el afectado o la Ley lo prescriba.

En relación con la necesidad de acreditar la competencia, debía atenderse igualmente a lo dispuesto en la Disposición adicional segunda, apartado segundo de la Ley Orgánica 15/1999:

“Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones Públicas”.

En relación con dicho precepto la Sala de lo Contencioso-Administrativo de la Audiencia Nacional en su sentencia de 21 de abril de 2004 señalaba que “De este precepto de la Ley de Protección de Datos de Carácter Personal se conciben los ficheros o registros de población, entre los que cabe incluir al Padrón municipal, como un elemento de comunicación entre los distintos órganos de las administraciones públicas y de los ciudadanos, y que su uso

vendrá determinado en el cumplimiento de las competencias que por el ordenamiento jurídico le viene atribuido".

Por último, esta Agencia también ha venido requiriendo que dicha cesión no se produjera de manera masiva, sino con carácter parcial, en el marco de una solicitud y para el mantenimiento de una determinada relación jurídico-administrativa.

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 acces**o, 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."

Por consiguiente, esta Agencia entiende que, estando debidamente legitimado el acceso a los datos del padrón por parte de las autoridades competentes, debe respetarse, no obstante, los criterios de proporcionalidad y las garantías establecidas por el Tribunal Constitucional, teniendo en cuenta que la fórmula propuesta en la disposición adicional segunda del Anteproyecto, consistente en la entrega de una copia actualizada de los datos obrantes en los padrones municipales del ámbito territorial en el que ejerzan sus competencias supondría un acceso masivo, indiscriminado y no motivado a los mismos

Por otro lado, en cuanto a los datos del censo electoral, el legislador nacional ha sido mucho más riguroso al regular el acceso a los mismos, estableciendo garantías adicionales que implican la intervención de la autoridad judicial cuando se trate de acceso a dichos datos fuera de los supuestos expresamente contemplados en la normativa electoral para fines electorales. Así resulta de lo dispuesto en el artículo 41 de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, que después de señalar en su apartado 1 que "Por real decreto se regularán los datos personales de los electores, necesarios para su inscripción en el censo electoral, así como los de las listas y copias del censo electoral" añade en su apartado segundo que "Queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial".

La referencia al conducto judicial y no a la autorización judicial ha planteado dudas interpretativas del citado precepto en relación al acceso a los datos del censo por parte del Ministerio Fiscal y de la Policía Judicial en el ejercicio de las funciones de averiguación de delitos que les atribuyen la LOPJ y el EOMF, siendo la interpretación de esta Agencia restrictiva al tratarse de un límite a un derecho fundamental, considerando necesaria, mientras no se modifique el precepto, la intervención judicial.

La propuesta del Anteproyecto supondría una modificación sustancial respecto al régimen tradicional de acceso a los datos del censo electoral, suprimiendo la intervención de la autoridad judicial en todos los casos de acceso por parte de cualesquiera de las autoridades competentes. A juicio de esta Agencia, dicho modificación se considera excesiva, no motivándose adecuadamente en la memoria las razones de un cambio tan significativo, y no existiendo, por otra parte, razones diferentes a las que justificarían, en su caso,

un acceso a los datos del padrón, por lo que serían aplicables en este caso los mismos requisitos de concreción, proporcionalidad, individualidad, motivación para el acceso, y control ya requeridos por el TC para los datos del padrón. Por ello, al igual que se ha planteado respecto al artículo 5 del Anteproyecto, debería diferenciarse entre los supuestos de acceso por parte de los órganos jurisdiccionales del orden penal, el Ministerio Fiscal y la Policía Judicial y el resto de autoridades competentes, respecto de las cuales debería mantenerse, en todo caso, además, la necesaria autorización judicial. En cuanto a la Policía Judicial, debe valorarse por el legislador si admite también el acceso en los casos en que actúa al amparo de lo dispuesto en el artículo 549.1.a) de la LOPJ sin una previa decisión de la autoridad judicial o fiscal, atendiendo a la obligación existente de dar cuenta a las mismas en el plazo máximo de 24 horas previsto en el artículo 295 de la Ley de Enjuiciamiento Criminal. Asimismo, se reitera, en todos estos supuestos debería detenerse en cuenta la doctrina del Tribunal Constitucional anteriormente enunciada respecto al acceso de los datos del padrón, evitando un acceso masivo, indiscriminado y no motivado a los datos del censo electoral e incluirse una disposición final que modifique el citado artículo 41.2 de la LOREG.

XXXVI

La disposición final cuarta modifica la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, (LGP) introduciendo un nuevo artículo 15 bis relativo al tratamiento de datos de carácter personal, con la siguiente redacción:

> «Artículo 15 bis. Tratamientos de datos de carácter personal.
>
> 1. Admitido en el establecimiento un recluso, se procederá a verificar su identidad personal, efectuando la reseña alfabética, dactilar y fotográfica, así como a la inscripción en el libro de ingresos y la apertura de un expediente personal relativo a su situación procesal y penitenciaria, de la que tendrá derecho a ser informado.
>
> 2. Asimismo podrán tratarse datos personales de los reclusos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como sus datos genéticos y biométricos dirigidos a identificarlo de manera unívoca, los datos relativos a su salud o a su vida sexual o a su orientación sexual, siempre que sea estrictamente necesario.
>
> 3. El tratamiento de los datos personales de los reclusos se regirá por lo previsto en la 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 de prevención frente a las amenazas contra la seguridad pública.
>
> 4. Igualmente se procederá al cacheo de su persona y al registro de sus efectos, retirándose los enseres y objetos no autorizados.

> 5. En el momento del ingreso se adoptarán las medidas de higiene personal necesarias, entregándose al recluso las prendas de vestir adecuadas que precise, firmando el mismo su recepción.

La normativa sobre instituciones penitenciarias afecta a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, por lo que queda excluida de la aplicación de la normativa general de protección de datos de carácter personal, rigiéndose por su normativa específica y supletoriamente, por dicha normativa general, tal y como ha establecido el artículo 2.3. de la Ley Orgánica 3/2018:

> 3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

En el momento actual, la Ley General Penitenciaria no contenía una disposición específica respecto del tratamiento de los datos de carácter personal de los internos, cuya normativa específica se contiene en el Capítulo III del Título I del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario, artículos 6 a 9, valorándose por esta Agencia que dicha reglamentación específica se recoja en una norma con rango de ley, cuyo apartado 3 sujeta dichos tratamientos a lo establecido en el presente Anteproyecto.

A este respecto, el artículo 1 de la Ley Orgánica General Penitenciaria señala que:

> “Las instituciones penitenciarias reguladas en la presente Ley tienen como fin primordial la reeducación y la reinserción social de los sentenciados a penas y medidas penales privativas de libertad, así como la retención y custodia de detenidos, presos y penados.
> Igualmente tienen a su cargo una labor asistencial y de ayuda para internos y liberados.”

Por lo tanto, la mayoría de los tratamientos de datos de carácter personal de los internos llevados a cabo por las instituciones penitenciarias entrarán dentro del ámbito objetivo del presente Anteproyecto y de la Directiva que transpone.

Sin embargo, puede existir tratamiento de datos personales de los internos cuya finalidad no sea la prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, algunos de los cuales aparecen específicamente previstos en el artículo 7 del Reglamento General Penitenciario, como la comunicación a otras Administraciones Públicas al objeto de que ejerzan sus funciones en materia de servicios sociales, Seguridad Social, custodia de menores u otras análogas, a la que se refiere su apartado 2, o los tratamiento con el fin de realizar estudios epidemiológicos de su apartado 3.

En este sentido se pronunció esta Agencia en su Informe 59/2019, en relación con la comunicación, por las instituciones penitenciarias a la Comunidad Autónoma correspondiente, encargada de la tramitación de las rentas mínimas de inserción, del dato relativo al ingreso en un centro penitenciario de las personas afectadas por dicha circunstancia, teniendo en cuenta que la suspensión en el pago de la rentas mínimas de inserción no forma parte de la ejecución de la pena sino que es consecuencia de la normativa autonómica que regula los requisitos de dicha prestación. Tal y como queda expuesto, dichos tratamientos, de acuerdo con lo previsto por el artículo 2.3 de la LOPDGDD, se rigen por su normativa específica, aplicándose de manera supletoria lo establecido en el RGPD y en la Ley Orgánica 3/2018.

Por consiguiente, respecto a los tratamientos que no entran dentro del ámbito de aplicación de la Directiva y del presente Anteproyecto, la normativa penitenciaria puede establecer especialidades, ajustadas a la doctrina del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal, especialmente, respecto a la proporcionalidad de los límites que puedan imponerse, sin que sea aplicable, sin más, un régimen más restrictivo para el derecho fundamental como el previsto en el Directiva. Y en lo no previsto específicamente, se aplicará de forma supletoria el RGPD y la Ley Orgánica 3/2018.

Por consiguiente, debe modificarse el apartado 3 del artículo 15 bis del Ley Orgánica General Penitenciaria, introducido por la disposición final cuarta del Anteproyecto, de modo que se especifique que los tratamientos de datos personales que se realicen por las instituciones penitenciarias para fines distintos de los previstos en la 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 de prevención frente a las amenazas contra la seguridad pública, se regirán por su normativa específica y, supletoriamente, por el RGPD y la Ley Orgánica 3/2018.

Por otro lado, en relación con los tratamientos de categorías especiales de datos a los que se refiere el apartado 2, hay que recordar que el artículo 10

de la Directiva permite tratar categorías especiales de datos personales sólo cuando sea estrictamente necesario, y ello siempre que concurra alguna de las causas a), b) o c) a que se refiere dicho artículo, pero en todo caso se requiere la "sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado", garantías o salvaguardias que el presente artículo no establece y que debería contener a la vista de la doctrina establecida en la sentencia del Tribunal Constitucional 76/2019, de 22 mayo, sobre el apartado 1 del art. 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a esta por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales:

> "El reglamento [aquí, la Directiva] contiene, por tanto, una obligación concreta de los Estados miembros de establecer tales garantías, en el caso de que habiliten para tratar los datos personales especialmente protegidos".
>
> (…)
>
> 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).
>
> (…)
>
> - La mera inexistencia de "garantías adecuadas" o de las "mínimas exigibles a la Ley" constituye de por sí una injerencia en el derecho fundamental, de gravedad similar a la que causarían intromisiones directas en su contenido nuclear.
>
> - La exigencia de "garantías adecuadas" se fundamenta, por tanto, en el respeto del contenido esencial del derecho fundamental.
>
> (…)
>
> b) Esta doctrina sobre las garantías adecuadas es también la que sigue la jurisprudencia del Tribunal de Justicia de la Unión Europea. En la sentencia de la Gran Sala de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd, apartado 54, el Tribunal de Justicia señaló lo siguiente: "la normativa de la Unión de que se trate

debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y 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 de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos (véanse, por analogía, en lo que respecta al artículo 8 del Convenio Europeo de Derechos Humanos, las sentencias del Tribunal Europeo de Derechos Humanos, Liberty y otros c. Reino Unido de 1 de julio de 2008, núm. 58243/00, §§62 y 63; Rotaru c. Rumanía, antes citada, §§57 a 59, y S y Marper c. Reino Unido, antes citada, §§99).”

(…)

7. Sentado lo anterior, estamos en situación de enjuiciar los tres elementos que aglutina la impugnación central del recurso de inconstitucionalidad y que confluyen en una doble vulneración de los arts. 18.4 y 53.1 CE: (i) que la disposición legal recurrida no haya determinado por sí misma la finalidad del tratamiento de datos personales que revelen opiniones políticas, más allá de la genérica mención al “interés público”; (ii) que no haya limitado el tratamiento regulando pormenorizadamente las restricciones al derecho fundamental; y (iii) que no haya establecido ella misma las garantías adecuadas para proteger los derechos fundamentales afectados.

(…)

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 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.

(…)

(iv) Por último, debemos recordar que el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí. El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que el Derecho del Estado miembro establezca "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD] y que "se ofrezcan garantías adecuadas" (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas, no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.

Por consiguiente, debería modificarse el apartado 2 para incorporar las garantías que se estimen adecuadas para salvaguardar el derecho a la protección de datos personales de los internos, atendiendo al tipo de datos que se tratan y a las finalidades de los distintos tratamientos.

XXXVII

Para concluir, se insiste en la conveniencia, ya adelantada en el informe 122/2018, de adaptar la terminología empleada en el Anteproyecto, cuya esencia, como se ha señalado, es transponer una Directiva en materia de protección de datos, a la terminología específica empleada en la normativa general, constituida tanto por el RGPD como por la Ley Orgánica 3/2018.

En este sentido, debería de recogerse el concepto de "interés vital" y sustituirse conceptos no recogidos en la normativa de protección de datos, como el de "peligro" o "nivel de riesgo", por el de "riesgo" o "alto riesgo", que son los que emplean las tres normas citadas. Asimismo, debe tenerse en

cuenta que la nueva normativa ya no gira, a diferencia de lo que ocurría en la anterior, sobre el concepto de fichero sino sobre el de tratamiento.