



## INFORME DEL CONSEJO FISCAL SOBRE EL ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES TRATADOS PARA FINES DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN O ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES, ASÍ COMO DE PROTECCIÓN Y PREVENCIÓN FRENTE A LAS AMENAZAS CONTRA LA SEGURIDAD PÚBLICA

1. CONSIDERACIONES PREVIAS. 2. OBSERVACIONES SOBRE LA FUNCIÓN CONSULTIVA DEL CONSEJO FISCAL Y LAS FUNCIONES DEL MINISTERIO FISCAL. 3. ESTRUCTURA Y FUNDAMENTO DEL ANTEPROYECTO DE LEY ORGÁNICA. 4. CONSIDERACIONES SOBRE EL OBJETO DEL ANTEPROYECTO. 5. OBSERVACIONES SOBRE EL TEXTO REMITIDO. 6. CONCLUSIONES.

### 1. CONSIDERACIONES PREVIAS.

En fecha 2 de abril de 2020 tuvo su entrada en la Fiscalía General del Estado la comunicación del Sr. Secretario de Estado de Justicia remitiendo el *Anteproyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública*, (en adelante, el Anteproyecto), solicitando el informe del Consejo Fiscal con carácter urgente e improrrogable. El Anteproyecto se acompaña de su correspondiente Memoria de análisis de impacto normativo.

El oficio justifica su remisión en el cumplimiento de lo previsto en el art. 14.4.j) de la Ley 50/1981, de 30 de diciembre, por la que se aprueba el Estatuto Orgánico del Ministerio Fiscal (en adelante, EOMF) y la urgencia e improrrogabilidad en el Acuerdo del Consejo de Ministros de 3 de marzo de



2020, por el que se autoriza la tramitación administrativa urgente del expediente.

## **2. OBSERVACIONES SOBRE LA FUNCIÓN CONSULTIVA DEL CONSEJO FISCAL Y LAS FUNCIONES DEL MINISTERIO FISCAL.**

De acuerdo con lo dispuesto en el art. 14.4.j) del EOMF corresponde al Consejo Fiscal informar los proyectos de ley o normas reglamentarias que afecten a la estructura, organización y funciones del Ministerio Fiscal.

El Ministerio Fiscal es un órgano de relevancia constitucional que tiene por misión promover la acción de la justicia en defensa de la legalidad, de los derechos de los ciudadanos y del interés público tutelado por la ley, de oficio o a petición de los interesados, así como velar por la independencia de los Tribunales y procurar ante éstos la satisfacción del interés social (art. 124 CE y art. 1 EOMF).

Para el cumplimiento de esta misión, corresponde al Ministerio Fiscal, entre otras funciones, velar por el respeto de los derechos fundamentales y libertades públicas con cuantas actuaciones exija su defensa (art. 3.3 EOMF); ejercitar las acciones penales y civiles dimanantes de delitos y faltas u oponerse a las ejercitadas por otros, cuando proceda (art. 3.4 EOMF); intervenir en el proceso penal, instando de la autoridad judicial la adopción de las medidas cautelares que procedan y la práctica de las diligencias encaminadas al esclarecimiento de los hechos o instruyendo directamente el procedimiento en el ámbito de lo dispuesto en la Ley Orgánica reguladora de la Responsabilidad Penal de los Menores, pudiendo ordenar a la Policía Judicial aquellas diligencias que estime oportunas (art. 3.5 EOMF); tomar parte, en defensa de la legalidad y del interés público o social, en los procesos relativos al estado civil y en los demás que establezca la ley (art. 3.6 EOMF), intervenir en los procesos civiles que determine la ley cuando esté comprometido el interés social o cuando puedan



afectar a personas menores, incapaces o desvalidas, en tanto se provee los mecanismos ordinarios de representación (art. 3.7 EOMF); y defender la legalidad en los procesos contencioso-administrativos que prevén su intervención (art. 3.14 EOMF).

No obstante la aludida limitación material de la potestad de informe, la función consultiva de este órgano viene siendo interpretada en términos amplios, habiéndose expresado en otras ocasiones el Consejo Fiscal en el sentido de entender que, con arreglo al principio de colaboración entre los órganos constitucionales, han de ser expresadas sus consideraciones sobre aspectos que afecten a derechos y libertades fundamentales, así como en relación a cuestiones de técnica legislativa o de orden terminológico, y todo ello con el fin de contribuir a mejorar la corrección de los textos normativos y, por consiguiente, a su efectiva aplicabilidad, una vez aprobados, en los procesos judiciales en los que el Ministerio Fiscal ejercita las funciones que legalmente tiene encomendadas.

El Anteproyecto sometido a informe, si bien no afecta a la organización y estructura del Ministerio Fiscal, está relacionado con sus funciones, al reconocer al Ministerio Fiscal como una de las autoridades competentes para el tratamiento de datos personales llevados a cabo con 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, así como destinatario del principio de colaboración de las Administraciones Públicas y personas físicas y jurídicas a los mismos fines citados previamente, e igualmente se relaciona con las funciones encomendadas por los artículos 4 y 5 del EOMF.

El presente texto da cumplimiento al preceptivo trámite de informe previsto en la indicada legislación orgánica del Ministerio Fiscal, expresando el parecer del



Consejo Fiscal sobre el mencionado proyecto.

### 3. ESTRUCTURA Y FUNDAMENTO DEL ANTEPROYECTO DE LEY ORGÁNICA.

El Anteproyecto de Ley Orgánica se compone de una Exposición de Motivos, cincuenta y cinco artículos distribuidos en ocho títulos, así como de dos disposiciones adicionales, y nueve disposiciones finales.

La Exposición de Motivos se divide en cuatro secciones. La primera se refiere al marco normativo europeo y nacional vigente, y a la necesidad de adaptar el marco normativo nacional a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativo a la protección de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos* y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

La segunda analiza las razones que han hecho necesaria la modificación del marco legal hasta ahora vigente, entre otras, el hecho de que la norma fuera anterior al Tratado de Lisboa y su necesidad de adaptación al artículo 16, apartado 2 del Tratado de funcionamiento de la Unión Europea, asimismo que el ámbito de aplicación de la misma no alcanzaba los tratamientos de carácter nacional, por lo que debía buscarse una armonización en la protección de datos de carácter personal en la materia, conforme a los considerandos 6 y 8 de la Directiva UE 2016/680.

La tercera asume la necesidad de regular los datos genéticos (considerando 23) y la distinción entre datos personales según su grado de exactitud y fiabilidad (considerando 30) y las categorías de interesados (art. 6), haciendo mención al carácter precursor de la Constitución Española en el tratamiento del



derecho a la protección de datos (art. 18.4), reconocido como un derecho fundamental y que supone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar, y el pleno ejercicio de sus derechos y la necesidad de dicho marco jurídico en el ámbito de la cooperación policial y judicial penal y en el sistema judicial penal.

Finalmente, la cuarta hace un breve resumen del contenido de los Capítulos I, II, III, IV, V, VI, VII y VIII del Anteproyecto.

El Capítulo I, relativo a las *Disposiciones generales*, comienza regulando el objeto de la ley orgánica (art. 1), su ámbito de aplicación (art. 2), define el concepto de autoridad competente para el tratamiento a efectos de la ley orgánica, tratamientos realizados por los órganos jurisdiccionales y el Ministerio Fiscal, tratamientos excluidos del ámbito de aplicación y la sujeción de los supuestos de deber de colaboración, y finalmente establece por remisión al Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, las definiciones en la materia (art.3 ).

El Capítulo II regula los *Principios de protección de datos*, remitiéndose a los definidos en la Directiva (UE)/2016/680, y así se citan los principios relativos al tratamiento de los datos personales (art. 4), se introduce el principio de colaboración con las autoridades competentes por parte de administraciones públicas y particulares (art. 5), los plazos de conservación y revisión (art. 6), la distinción de categorías de interesados en el tratamiento (art.7), verificación de los datos personales y distinción de datos basados en hechos (art. 8), licitud del tratamiento (art. 9), condiciones específicas de tratamiento (art. 10), tratamiento de categorías especiales de datos personales (art.11) y mecanismo de decisión individual automatizada (art. 12). Como única diferencia con la normativa comunitaria, ha de mencionarse el principio de colaboración con las autoridades competentes por parte de las autoridades y las personas privadas a los fines del artículo 1 mediante la aportación de los datos que figuran en el



precepto.

El Capítulo III se dedica a los *derechos de las personas*, distinguiendo un régimen general que abarca las condiciones generales del ejercicio de los derechos (art. 13), derecho a la información (art. 14), derecho de acceso (art. 15), derecho de rectificación, supresión o limitación (art. 16), restricciones al ejercicio de los derechos antes citados (art. 17), posibilidad del ejercicio de los derechos a través de la autoridad de control, y en segundo lugar, se establecen las condiciones especiales en el ejercicio de dichos derechos cuando nos encontremos en investigaciones y procesos penales (art. 19).

El Capítulo IV se refiere al *responsable y al encargado del tratamiento*. Dentro del mismo se establecen en primer lugar las obligaciones generales del responsable y encargado del tratamiento (arts. 20 y 23), la protección de datos desde el diseño y por defecto (art. 21), la corresponsabilidad (art. 22) y las obligaciones en el tratamiento derivadas de la protección de datos, entre las que cabe citar la obligación de llevar un registro de actividades de tratamiento (art. 25), un registro de operaciones de tratamiento (art. 26), la cooperación con la autoridad de protección de datos (art. 27) y la evaluación de impacto y consulta previa con la autoridad de protección de datos antes de proceder a tratar los datos (arts. 28 y 29). En segundo lugar y en materia de seguridad de los datos personales, se fijan los criterios de seguridad del tratamiento (art. 30), la notificación de las violaciones de seguridad a la autoridad de protección de datos (art. 31) y al interesado (art. 32). Finalmente se menciona la figura del delegado de protección de datos, definiendo su designación (art. 33), posición (art. 34) y funciones (art. 35).

El Capítulo V establece los criterios aplicables a las *transferencias internacionales de datos*, partiendo de los principios generales aplicables (art. 36), las transferencias, bien a través de decisión de adecuación (art. 37), o de garantías apropiadas (art. 38), las excepciones para situaciones específicas



(art. 39) y finalmente las realizadas a destinatarios que no sean miembros de la Unión Europea (art.40).

El Capítulo VI se dedica a las *autoridades de protección de datos*, definiendo las existentes en España (art. 41), funciones (art. 42), potestades (art. 43) y la asistencia entre autoridades de protección de los estados miembros (art. 44).

El Capítulo VII regula el *Procedimiento en caso de reclamaciones tramitadas por las autoridades de protección de datos*, su régimen aplicable (art. 45) y el derecho a indemnización, ya sea en los supuestos de tratamiento realizado por ente del sector público (art. 46) o del sector privado (art. 47).

El Capítulo VIII contempla el *régimen sancionador*, definiendo los sujetos responsables (art. 48), las normas de conflicto (art. 49), las infracciones (arts. 50 a 52), las sanciones (art. 53), la prescripción de las infracciones y sanciones (art. 54) y la caducidad del procedimiento (art. 55).

Las Disposiciones adicionales aluden, entre otras, a cuestiones como la regulación de los acuerdos internacionales firmados en la materia antes de la entrada en vigor de la presente ley y la utilización de los ficheros del Instituto Nacional de Estadística en cumplimiento de los fines de esta ley.

Las Disposiciones finales describen la naturaleza de la ley (primera), sobre el título competencial de la ley (segunda), la modificación de preceptos normativos afectados por la ley (tercera a séptima), la incorporación del derecho comunitario a la normativa española mediante la aprobación de la presente norma (octava) y la entrada en vigor de la ley (novena).

#### **4. CONSIDERACIONES SOBRE EL OBJETO DEL ANTEPROYECTO.**

El Anteproyecto de Ley Orgánica de protección de datos personales



tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública, tiene por objeto, esencialmente, la incorporación al Ordenamiento español de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativa a la protección de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.*

Esta finalidad se plasma en la Disposición final octava, siendo igualmente relevante el artículo 63 de la Directiva, en el que se dispone que los Estados miembros adoptarán y publicarán las disposiciones legales reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, e igualmente cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial.

Dicho Anteproyecto tiene su origen en la reforma de la normativa europea de protección de datos generada por la rápida evolución de la tecnología y la globalización, y sobre cuya necesidad se pronunció la Comunicación de la Comisión Europea *“Un enfoque global de la protección de los datos personales en la Unión Europea”*, de 4 de noviembre de 2010, que en su sugerencia 5, y con relación a la Directiva 95/46/CE sobre protección de datos, decía *“que había conducido a un marco jurídico fragmentado debido a los diferentes enfoques de aplicación adoptados en los diferentes Estados miembros, y que los avances de las nuevas tecnologías han conducido a nuevos retos en lo que se refiere a la protección de datos; está de acuerdo, por lo tanto, en que se ha confirmado la necesidad de un nuevo marco jurídico”*.



Por lo tanto, nos hallamos ante un nuevo marco jurídico en materia de protección de datos, que desde el punto de vista de la normativa europea, está compuesto 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* (en adelante, RGPD), aplicable desde el pasado 25 de mayo de 2018, de alcance general, obligatorio y directamente aplicable en cada Estado miembro; y para el “*ámbito penal*”, la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales y a la libre circulación de dichos datos* (en adelante, Directiva 2016/680), norma cuyo proyecto de trasposición se somete a examen, conteniendo las anteriores normas, disposiciones referidas tanto al sector público como al sector privado de los Estados miembros.

Igualmente dentro de ese paquete de reformas y en la misma fecha se aprobó la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, relativa a la utilización de datos del registro de nombres de 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 los 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 en dichos Estados miembros, y que en el momento actual está también pendiente de su trasposición al ordenamiento jurídico español.

Finalmente, y para el tratamiento efectuado por las instituciones, órganos y organismos de la Unión, se aplica el Reglamento (UE) 2018/1725 del



Parlamento Europeo y del Consejo de 23 de octubre de 2018, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE.*

Por lo tanto, nos encontramos ante tres normas que fueron publicadas en el Diario oficial de la Unión Europea del 4 de mayo de 2016, y que conforman un bloque normativo en materia de tratamiento de protección de datos con origen en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, y en el artículo 16, apartado 1º del Tratado de Funcionamiento de la Unión Europea (TFUE), que configuran el derecho fundamental de protección de datos de carácter personal, en el que la disciplina general se lleva a cabo en el RGPD, mientras la específica se complementa a través de las directivas antes citadas y con las disposiciones de los Estados miembros a través de la normativa de trasposición que llevan a cabo, sin que ello influya en una interpretación conjunta de las normas citadas, ya que como se establece en los considerandos 9, 10 y 11 de la Directiva, es necesario diferenciar que el RGPD establece las normas generales en la materia, mientras que la Directiva establece las normas específicas relativas al tratamiento de datos personales basados en los ámbitos de la cooperación judicial y policial en materia penal basada en el artículo 16 TFUE.

En nuestro ordenamiento interno, y con carácter general, la Ley Orgánica 3/2018, de 5 de diciembre, de *Protección de Datos Personales y garantía de los derechos digitales* (en adelante, LOPDGDD) se dictó con el objetivo de adaptar nuestro ordenamiento jurídico al RGPD, manteniendo la vigencia de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de *Protección de Datos de Carácter Personal* (en adelante, LOPD) exclusivamente para los tratamientos sometidos a la mencionada Directiva 2016/680, en tanto no entre en vigor la norma que trasponga al derecho español lo dispuesto en la misma.



Igualmente se busca crear una normativa que consagre el respeto al derecho fundamental al que se refiere el artículo 18.4 de la CE, es decir, conforme a lo establecido en la STC 292/2000, *“el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”*, estableciendo mediante dicho Anteproyecto unas garantías necesarias que aseguren su legalidad, ya que como dice la STC 76/2019, de 22 de mayo, *“el derecho fundamental a la protección de datos personales no tiene carácter absoluto. Puede ser restringido por medio de la ley, siempre que ello responda a un fin de interés general, y los requisitos y el alcance de la restricción estén suficientemente precisados en la ley y respeten el principio de proporcionalidad”*.

En consecuencia, la ley orgánica que definitivamente emane de este Anteproyecto se constituirá, a su vez, en norma especial frente a la LO 3/2018 y al RGPD, debiendo recordarse, en este punto, que los Reglamentos, a diferencia del resto del derecho derivado comunitario, tienen alcance general, obligatorio y directamente aplicable en cada Estado miembro (art. 288 del Tratado de Funcionamiento de la Unión Europea).

Por otro lado, resulta conveniente apuntar que la Directiva, en su art. 63, fija como plazo de trasposición al derecho interno el 6 de mayo de 2018, término que, al no haberse cumplido, dio lugar a que, de conformidad con el art. 260.3 del Tratado de Funcionamiento de la Unión Europea, la Comisión Europea iniciase un procedimiento de infracción solicitando, en julio de 2019, al Tribunal de Justicia de la Unión Europea la imposición de sanciones a España por incumplir la obligación de transponer una Directiva adoptada por el legislador



europeo al derecho interno dentro del plazo establecido.

En este sentido, se ha de tener en cuenta que las directivas no incorporadas al derecho nacional en el plazo correspondiente, al igual que aquellas que hayan sido incorrectamente transpuestas, pueden generar ciertos efectos; el primero sería el efecto directo vertical que supone la aplicación directa de las mismas respecto de las disposiciones que contemplen derechos de los ciudadanos frente a los poderes públicos siempre que sean incondicionales y suficientemente claras y precisas y, por otro, el principio de interpretación conforme que supone la interpretación del derecho nacional atendiendo al contenido de la Directiva.

De todo ello deriva la trascendencia de efectuar no solo una trasposición en plazo sino la importancia de una correcta trasposición.

Por lo demás, la exposición de motivos del Anteproyecto dispone la adecuación a los principios de la buena regulación, y en este sentido es evidente que la norma era necesaria ya que, como se ha explicado anteriormente, el artículo 63 de la Directiva había impuesto a los Estados miembros la obligación de adoptar y publicar las disposiciones legales, reglamentarias y administrativas tendentes a la trasposición de ésta.

En cuanto al principio de seguridad jurídica, la contenida en el Anteproyecto es una norma con rango de ley orgánica prevista en el artículo 81.1 CE a la que corresponde el desarrollo directo del derecho fundamental, esto es, *“la regulación de determinados aspectos esenciales para la definición del derecho, la previsión de su ámbito y la fijación de sus límites en relación con otras libertades constitucionalmente protegidas”* (STC 132/1989 de 18 de julio, STC 135/2006 de 27 de Abril y STC 173/1998, de 18 de Agosto), en tanto que a la ordinaria le atañe todo cuanto se refiere al ejercicio del derecho.



También sobre el principio de proporcionalidad, se fijan una serie de garantías a lo largo del articulado, basadas no solo en la aplicación de los principios del tratamiento de datos del Capítulo II, sino fundamentalmente, como establece el artículo 1, en que todo tratamiento no puede ser realizado con fines distintos de los establecidos en la norma, con la aplicación del RGPD en tal caso y salvo las exclusiones en el supuesto de que el tratamiento se efectúe como parte de una actividad que esté fuera del ámbito de aplicación del Derecho de la Unión, conforme a lo establecido en el Considerando 11 de la Directiva.

El principio de transparencia se entiende cumplido a la vista del listado de informes recabados que obra en la Memoria de análisis de impacto normativo, y del cumplimiento del trámite de audiencia pública.

Sobre la valoración del análisis de impacto, entendemos que, en cuanto al orden competencial, la ley orgánica se dicta al amparo de la competencia exclusiva del Estado en el artículo 149 1º, 6º y 29º de la Constitución Española, que atribuye al estado la competencia exclusiva en la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales, así como en materia de seguridad pública y de la legislación procesal.

Por lo tanto, procede realizar un estudio del contenido del Anteproyecto, teniendo en cuenta que la materia sobre la que trata la normativa comunitaria es una actividad sumamente específica, y que no puede ser abordada con los instrumentos de control previstos para los tratamientos privados de datos. Ocurre que, al entrar en conflicto distintos intereses, de una parte, los derechos de los ciudadanos sobre sus datos personales y, de otra, las necesidades de tratamiento de esos datos personales para fines de prevención, detección, investigación o represión de los delitos, ambos han de encontrarse en una situación de equilibrio perfecto, para evitar que los derechos de los ciudadanos puedan resultar lesionados o vulnerados o que se limite tanto el tratamiento de



datos, que se haga imposible su uso en la prevención, investigación o represión de las infracciones penales.

Por otra parte, y desde la perspectiva del Ministerio Fiscal, dado que el objeto del Anteproyecto, según su artículo 1.1 (y art. 1.1 de la Directiva), lo constituye la regulación del tratamiento de datos personales por parte de las autoridades competentes para los fines en ella descritos, y siendo indiscutible la condición del Ministerio Fiscal como autoridad competente y responsable del tratamiento, la efectiva plasmación legal de este Anteproyecto pudiera llegar a comprometer su autonomía funcional y el ejercicio de su misión por medio de órganos propios.

## **5. OBSERVACIONES SOBRE EL TEXTO REMITIDO.**

La mayor parte de las disposiciones previstas en los Capítulos I a VIII del Anteproyecto recogen las disposiciones de la Directiva 2016/680, sin perjuicio de que en aspectos puntuales el Anteproyecto regule la materia con mayor amplitud.

Sobre ello hay que hacer las siguientes consideraciones:

En primer lugar, dado que uno de los objetivos del Anteproyecto es trasponer la Directiva con la que se pretende asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas entre las autoridades competentes de los Estados miembros (Considerando 7), se habría de procurar en su redacción una mayor precisión terminológica.

Así, por ejemplo (y sin perjuicio de lo que se irá apuntando a lo largo de este informe), la propia denominación del Anteproyecto resulta imprecisa ya que omite la mención a las “autoridades competentes” cuando lo que precisamente regula es el tratamiento de datos personales por parte de aquellas con unas finalidades específicas.



Por otro lado, sería recomendable que, ya que la misma afecta a un derecho fundamental, y al igual que hace la Directiva, la denominación de la ley debería incidir en que la protección recaerá sobre las personas físicas en lo que respecta al tratamiento de sus datos personales.

Sobre el articulado se pueden indicar las siguientes consideraciones:

### Exposición de motivos

Con carácter previo, y ya desde la exposición de motivos, hay que señalar que llama la atención que el Anteproyecto sometido a informe no utilice un lenguaje inclusivo. Así, por ejemplo, a palabra “*ciudadanos*” deber ser sustituida por la palabra “*ciudadanía*”, la palabra “*interesado*” debe ser sustituida por “*persona interesada*” y, una vez sustituido el vocablo “*interesado*”, por ejemplo, en el folio 6, por “*persona interesada*”, irá en cascada la sustitución de las palabras sospechoso o condenados, por sospechosas y condenadas (personas).

En cuanto al contenido de la Exposición de Motivos y respecto a la definición de autoridades competentes, y la posterior concreción de éstas, no se menciona al Ministerio Fiscal, siendo necesaria su inclusión, del mismo modo que se menciona en la exposición de motivos y en el articulado a los órganos jurisdiccionales, sin que existan razones que justifiquen dicha omisión. Igualmente deben explicarse las consecuencias jurídicas de la redacción de los párrafos 5º y 6º del artículo 2º con relación a los tratamientos de datos efectuados por los órganos jurisdiccionales y el Ministerio Fiscal, de conformidad con lo establecido en el artículo 45.2 de la Directiva.

En segundo lugar, en las menciones que realiza al contenido del capítulo V debe procederse a la modificación de su redacción ya que, aunque es cierto que la palabra “*transferencia*” admite la posibilidad del término “*trasferencia*” (DRAE), sin embargo, no deberían utilizarse indistintamente ambas formas



dentro del texto (página 9), con el fin de dar una uniformidad de estilo”.

## Capítulo I. Disposiciones generales

### Artículo 1

El artículo 1 dispone que la ley tiene por objeto “*regular el derecho fundamental a la protección de datos personales*”, y precisa los fines del tratamiento, “*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, así como de protección y de prevención frente a las amenazas contra la seguridad pública*”. De este modo se precisa el carácter especial de la regulación, frente al general del RGPD, como regulan el artículo 2.2 d) del RGPD y el artículo 2.2 a) de la LOPDGDD, introduciendo el contenido del derecho fundamental previsto en el artículo 18.4 de la CE y según los criterios expresados en los considerandos 2 y 14 de la Directiva.

Ahora bien, este precepto regula el objeto introduciendo el concepto “*seguridad pública*”, que es un concepto que, si bien se recoge en la Directiva objeto de trasposición, no ha sido convenientemente adaptado a los conceptos empleados en el ordenamiento jurídico español.

Partimos de que la “*seguridad pública*” es un concepto distinto al de “*seguridad nacional*”, pero lo que no es tan evidente es que lo sea del de “*seguridad ciudadana*”. En todo caso, queda perfectamente diferenciado del de “*infracción penal*”. Así, además de en el artículo 1, en el artículo 7.a), sobre las categorías de interesados, viene a distinguir entre infracción penal por un lado y protección y prevención frente a las amenazas contra la seguridad pública por otro.

Esta distinción es más evidente en el artículo 17.1 en el que se distinguen además las categorías en distintos apartados. En el apartado c), se habla de



seguridad pública y en el apartado d) se habla de seguridad nacional.

Parece que el concepto "*seguridad pública*", por exclusión, nos remite al ámbito administrativo sancionador. No en vano el artículo 7.b) distingue entre condenados (infracción penal) y sancionados (infracción administrativa). Por lo que, en este ámbito, podría pensarse que se está empleando el concepto "*seguridad pública*" como sinónimo de "*seguridad ciudadana*", algo que nos reconduce a la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

Ahora bien, debemos llamar la atención sobre la dicción del propio artículo, que solo habla de momentos anteriores a la amenaza (protección y prevención) por lo que la norma analizada no sería nunca de aplicación a las labores de punición de las infracciones o ejecución de las sanciones impuestas en aplicación de la Ley de Seguridad Ciudadana.

En definitiva, recomendamos que si el concepto "*seguridad pública*" se quiere emplear como sinónimo de "*seguridad ciudadana*" se utilice este término. Si, por el contrario, el legislador maneja un concepto de "*seguridad pública*" distinto, sería menester en aras a la seguridad jurídica que lo aclarare.

Por otra parte, es aconsejable una redacción más clara, estableciendo el objeto de la ley en la regulación del derecho fundamental a la protección de los datos personales en relación a dos tipos de tratamientos llevados a cabo por autoridades competentes:

- 1º.- Con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
- 2º.- Con fines de protección y prevención frente a las amenazas contra la seguridad pública.

Al tratarse del derecho fundamental a la protección de los datos que las



autoridades competentes tienen con motivo de lo dicho en los apartados anteriores, no es necesario, en este punto, detallar los tipos de infracciones. Sin embargo, la apreciación de las consecuencias accesorias del delito las consideramos necesarias para determinar de manera clara el alcance de los derechos del ciudadano en ese aspecto de la ejecución penal.

El concepto de seguridad pública es un concepto oscuro en nuestro ordenamiento, siendo necesaria una concreción respecto a su alcance, habida cuenta, además, que en el artículo siguiente la ley excluye expresamente el tratamiento de datos personales (apartados d y e) relativos a materias clasificadas: Defensa, Seguridad Nacional, terrorismo, delincuencia organizada dirigida a desestabilizar gravemente el normal funcionamiento del Estado, etc.

Por su parte el artículo 2.4 utiliza la expresión *“protección y prevención frente a las amenazas contra las infraestructuras críticas”*, mientras que el artículo 5.2 utiliza la expresión *“prevención y protección frente a un peligro real y grave para la seguridad pública”*, algo difícilmente cuantificable.

Así, pues, es necesario delimitar el concepto y alcance del concepto seguridad pública.

La definición del concepto de infracciones o sanciones penales debe interpretarse de conformidad con los considerandos 12 y 13 de la Directiva, que precisan que el concepto de infracción penal es autónomo del Derecho de la Unión, y fijan los criterios para considerar aquellas actividades de la Policía y Cuerpos de Seguridad incluidas en el fin de la norma.

Finalmente dispone que las personas pueden ejercer el derecho fundamental a la protección de datos personales conforme a las normas de la LOPDGDD siempre que el resultado de dicha aplicación no sea contrario a los fines del tratamiento, dando respuesta a dicho ejercicio en la regulación de los derechos



de las personas, que es objeto del Capítulo III del Anteproyecto.

## Artículo 2

El artículo 2, establece en los párrafos 1 y 2 su *ámbito de aplicación* ampliando el concepto de tratamiento de datos personales, ya que incluye los procedentes de las imágenes y sonidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado, y los órganos competentes para el control y vigilancia en los centros penitenciarios y el control, regulación, vigilancia y disciplina del tráfico con los fines previstos en la Directiva, dejando dentro de su regulación específica, aquellos supuestos en los que no se cumplen los fines de esta norma, o aplicando supletoriamente el RGPD.

Esta regulación no coincide con las previsiones del considerando 26 de la Directiva, puesto que este se refiere a que *“las autoridades policiales puedan llevar a cabo actividades tales como las investigaciones encubiertas o la videovigilancia”*, con los fines específicos previstos en la ley y con fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas las de protección y prevención frente a las amenazas para la seguridad pública, siempre que estén previstas en la legislación y constituyan una medida necesaria y proporcionada en una sociedad democrática. De otro lado, el artículo 22.6 de la LOPDGDD admite *“ el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por los Cuerpos y Fuerzas de Seguridad y por los órganos competentes para la vigilancia y control de los centros penitenciarios,*

La normativa legal española en materia de videovigilancia se encuentra en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y RD 596/1999, de 16 de abril. Los artículos 1 y 2 de la primera precisan su objeto y ámbito de aplicación, el artículo 10 regula el régimen de infracciones y



sanciones, en su disposición adicional séptima define las faltas graves y muy graves y la disposición adicional octava textualmente dice *“La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia”*.

Pues bien, en esta materia, pese a disponer de una regulación específica, el Anteproyecto no distingue cuándo el uso de las cámaras tiene como finalidad la prevención, detección, investigación de delitos, en cuyo caso debe de estar incluido en esta ley orgánica, o cuando ese uso tiene una finalidad puramente administrativa sancionadora, fundamentalmente en materia de tráfico, u otros aspectos de vigilancia o de policía más propios de la seguridad ciudadana.

A esta captación de imágenes mediante sistemas de videovigilancia también hace expresa referencia el artículo 588 quinquies a) de la Ley de Enjuiciamiento Criminal y, como bien establece la Circular de la Fiscalía General del Estado 3/2019, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la regulación de la LECrim, que se analiza, tiene por objeto la utilización de dispositivos electrónicos de captación o grabación de sonido, y eventualmente de la imagen, en el marco de la investigación criminal de determinados delitos. No están sujetos, por lo tanto, a esta regulación, los supuestos previstos en la Ley Orgánica 4/1997, de 4 de agosto, *por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos* que, conforme a lo previsto en su art. 1.1 tiene, esencialmente, *una finalidad preventiva*, ni tampoco la colocación de cámaras de videovigilancia por particulares, que deberá ajustarse a la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales*. La captación y grabación de imágenes y



sonido en estos casos se regirá por las leyes indicadas y la eventual incorporación al proceso de archivos de imagen o sonido captados entrará dentro de las facultades y obligaciones de la Policía Judicial que regula el art. 282 LECrim, siendo la prueba así aportada perfectamente valorable por el Tribunal (STS nº 134/2017, de 2 de marzo).

En otro orden de cosas, el artículo 2.3 considera autoridad competente, *a los efectos de esta ley orgánica, a “toda autoridad pública que tenga competencias encomendadas legalmente, para la consecución de los fines del artículo 1”*.

El término “consecución” no resulta correcto ya que, a los efectos de lo que aquí se trata, las autoridades competentes no buscan conseguir alguno de los fines recogidos en el artículo 1, sino que lo que hacen es tratar datos con alguna de esas finalidades.

Por tanto, *se propone* que la frase “para la consecución de los fines del artículo 1” se sustituya por “para el tratamiento de datos personales en base a alguno de los fines previstos en el artículo 1”.

Además, al tratar en particular de cuáles son las autoridades competentes para realizar los tratamientos de datos personales referidos en el artículo 1, no se alcanza a comprender por qué junto a la Agencia Estatal de Administración Tributaria no figura la Tesorería General de la Seguridad Social, cuando el tratamiento de ambas instituciones públicas es mimético. No sólo a nivel de protección penal (regulación conjunta de los delitos contra la Hacienda Pública y los delitos contra la Seguridad Social) sino también de régimen de cesión de datos y funciones de cooperación y auxilio de la AEAT y la TGSS con el Ministerio Fiscal y el Poder Judicial (véase el redactado del art. 95 de la LGT y 66 de la LGTGSS).

Las mismas funciones y responsabilidades en relación con los fines del art. 1



tienen la AEAT y la TGSS, por lo que no se entiende la inclusión de la primera y no de la segunda. Máxime cuando en el artículo 5.1 incluye entre las Administraciones públicas que debe de proporcionar datos a las autoridades judiciales, Ministerio Fiscal y Policía Judicial a la de la seguridad social conjuntamente con la tributaria.

La regulación de los tratamientos realizados por los órganos jurisdiccionales y por el Ministerio Fiscal se contempla en los apartados 5 y 6 del artículo 2 del Anteproyecto, del siguiente modo:

*Según el apartado 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".*

*Y según el apartado 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".*

La 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 (Considerando 20).

No obstante, la opción de remisión normativa por la que se decanta el Anteproyecto en lo que respecta a los tratamientos de datos personales efectuado por el Ministerio Fiscal (y por los órganos judiciales competentes)



merece una valoración muy negativa dado que, en la actualidad, la regulación de esta materia en las normas procesales penales y en el EOMF es prácticamente inexistente, siendo insuficiente y desfasada la que recoge la LOPJ.

En relación a dichos preceptos se ha de apuntar lo siguiente:

a) En primer lugar no se alcanza a comprender la remisión (para lo que no esté regulado en la LOPJ) al Capítulo III del Anteproyecto que se realiza en el apartado 5, cuando lo que se regula en el Capítulo III es el ejercicio de los derechos por parte de los interesados y no las operaciones y procedimientos de tratamiento, y cuando, por otro lado y para mayor confusión, en el art. 19 (inserto en la Sección 2ª de dicho Capítulo III) se realiza un nuevo reenvío a la LOPJ, en este caso respecto del ejercicio de los derechos de los interesados en el marco de investigaciones y procesos penales.

En el supuesto de que la referencia al Capítulo III fuera un error material y el Anteproyecto pretendiera referirse al Capítulo II, se ha de señalar que la regulación que este capítulo contiene no alcanza las exigencias mínimas respecto de los tratamientos de datos en el ámbito de los tratamientos jurisdiccionales efectuados por el Ministerio Fiscal, tal y como se argumentará más adelante [concretamente en el apartado d)].

b) La normativa a la que se remite el Anteproyecto, en relación al Ministerio Fiscal, en la actualidad se reduce a la Disposición Adicional segunda del EOMF, añadida por Ley Orgánica 19/2003, de 23 de diciembre, por la que se modificó la LOPJ, y en la que se establece que el Ministerio Fiscal dispondría de un sistema de información y una red de comunicaciones electrónicas plenamente integrados con el fin de asegurar su unidad de actuación.

En desarrollo de dicha previsión legal se dictó el Real Decreto 93/2006, de 3 de



febrero, por el que se regula el sistema de información del Ministerio Fiscal, el cual, si bien se refiere a ficheros, establece una responsabilidad compartida entre el Fiscal General del Estado respecto del fichero generado por el sistema de información procesal de la Fiscalía General del Estado y las respectivas Fiscalías de aquél generado por el sistema de gestión procesal de cada una de ellas.

Según el RD 93/2006, el sistema de información procesal del Ministerio Fiscal constituye una base de datos centralizada que interconecta los distintos sistemas telemáticos puestos a disposición de las fiscalías a través de una red integrada de comunicaciones electrónicas, el cual está conformado por los sistemas de gestión procesal desarrollados para las distintas fiscalías por las Administraciones competentes y por el sistema único y centralizado de información de la Fiscalía General del Estado (arts. 1 y 2), considerando sistema de gestión procesal a aquel conjunto de aplicaciones informáticas dirigidas a organizar en las distintas fiscalías la información relativa a todas o una clase determinada de procedimientos, diligencias y expedientes de que conoce el Ministerio Fiscal, facilitando su tramitación y la actuación uniforme del Ministerio Público (art.3).

Por otro lado, el art. 48.3 de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores (en adelante LORPM) dispone que la recogida, cesión y tratamiento automatizado de datos de carácter personal de las personas a las que se aplique la presente Ley, sólo podrá realizarse en ficheros informáticos de titularidad pública dependientes de las entidades públicas de protección de menores, Administraciones y Juzgados de Menores competentes o del Ministerio Fiscal, y se regirá por lo dispuesto en la LO 15/1999 y sus normas de desarrollo.

En cuanto a la normativa relativa al tratamiento de datos llevado a cabo con ocasión de la tramitación por los jueces y tribunales de los procesos de los que



sean competentes y que subsidiariamente sería de aplicación al Ministerio Fiscal, se regula, a partir de la reforma operada por la Ley Orgánica 7/2015, de 21 de julio, en el Capítulo I bis del Título III del Libro I de la LOPJ, bajo el título Protección de datos de carácter personal en el ámbito de la Administración de Justicia (artículos 236 bis a 236 decies) así como en el Reglamento 1/2005, *de aspectos accesorios de actuaciones judiciales*.

Respecto de dicha regulación, ya en el informe complementario al emitido sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal (actual Ley 3/2018), aprobado por el Pleno del Consejo General del Poder Judicial de 26 de julio de 2017, y sin que a la fecha actual la situación que se describe haya variado, se afirma que “el marco regulatorio que se contiene en los artículos 236 bis a decies de la LOPJ se antoja claramente insuficiente” considerando conveniente “que por el prelegislador, se contemplase la necesidad de abordar en un determinado plazo la regulación completa y sistemática del singular régimen del tratamiento de datos con fines jurisdiccionales dentro del marco del RGPD, adaptando y desarrollando el régimen general que este contiene a las especificidades del tratamiento de datos con fines jurisdiccionales; regulación que habrá de incluirse en la LOPJ, marco legal propio donde se ha de contener la reglamentación de las competencias y funciones de este órgano constitucional”.

c) El tratamiento de datos jurisdiccionales de naturaleza penal por parte del Ministerio Fiscal tiene su origen en dos fuentes distintas. La primera, sería tributaria de su intervención en los correspondientes procesos incoados por los órganos judiciales, en este caso, de la jurisdicción penal; la segunda devendría del ejercicio de aquellas funciones propias del Ministerio Fiscal que tienen una naturaleza jurisdiccional o cuasi jurisdiccional.

La LOPJ dispone que los tribunales podrán tratar datos de carácter personal con fines jurisdiccionales y no jurisdiccionales, el primero 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, así como los que se precisen para su adecuada gestión (apartados 1 y 2 art. 236 ter LOPJ), siendo el Reglamento 1/2005, aunque refiriéndose a ficheros de datos, el que mejor concreta cuáles se pueden considerar jurisdiccionales y cuáles no, lo que puede servir de referencia a las distintas actividades de tratamiento que efectúa el Ministerio Fiscal, así:

Los ficheros a que se refiere el art. 230.5 (actual art. 236 ter LOPJ) se formarán con los datos de carácter personal que figuren en los procesos de los que conozcan y con los que consten en los procedimientos gubernativos. Los primeros se denominarán ficheros de datos jurisdiccionales y los segundos ficheros de datos no jurisdiccionales (art. 87.1 del Reglamento 1/2005).

En los ficheros de datos jurisdiccionales solamente se contendrán los datos de carácter personal que deriven de las actuaciones jurisdiccionales y, en particular: los que en atención a lo dispuesto en las leyes procesales sean necesarios para el registro e identificación del procedimiento o asunto jurisdiccional con el que se relacionan; los que sean necesarios para la identificación y localización de quienes pudieran tener derecho a intervenir como parte; los necesarios para la identificación de quienes asuman las labores de defensa o representación procesal o intervengan en cualquier otra calidad en el procedimiento o asunto; los que exterioricen las resoluciones dictadas y las actuaciones en él realizadas y los derivados de la instrucción.

Por tanto, cualquier operación o conjunto de operaciones realizadas sobre datos personales, o conjuntos de datos personales, de la naturaleza jurisdiccional antes descrita, ya sea por procedimientos automatizados o no (tales como el registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación,



supresión o destrucción) que realice el Ministerio Fiscal constituirá tratamiento de datos jurisdiccionales. Esta conclusión no se puede tachar de novedosa ya que así se admite por la Sala de lo Contencioso-administrativo de la Audiencia Nacional en Sentencias de 9 de octubre de 2009 y de 25 de marzo de 2011.

Por otro lado, el Ministerio Fiscal lleva a cabo funciones jurisdiccionales o cuasi jurisdiccionales propias, dentro de las cuales se podrían encuadrar, en lo que al ámbito penal se refiere, a la tramitación del procedimiento establecido en la LORPM así como aquellas relativas a las diligencias de investigación (art. 5 y 773.2 LECrim.), dado que no es que el Fiscal tenga atribuida la potestad jurisdiccional, sino que participa de ella al tramitar diligencias que tienen una íntima relación con el proceso (y ello tal como se pronuncia la Consulta FGE 1/2015, sobre el acceso de lo actuado en las Diligencias de Investigación por quien invoca un interés legítimo).

d) El art. 4.2 del RGPD (en términos idénticos al 3.2 de la Directiva), al que se remite el art. 3 del Anteproyecto, define el tratamiento de datos personales como: *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”*.

Tal como antes se ha apuntado, la 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, regulación que no se aborda en el actual Anteproyecto.



Por tanto, el Anteproyecto, para cumplir adecuadamente con el mandato contenido en la Directiva, ante la ausencia en el ordenamiento nacional de disposiciones acordes con la actual normativa europea, debería regular, de modo específico respecto del tratamiento de datos personales por parte del Ministerio Fiscal, entre otras cuestiones:

- El procedimiento para materializar la distinción entre los datos personales de las distintas categorías de interesados, así como los plazos y procedimientos específicos para la supresión y revisión periódica de los mismos.

En este aspecto, constituyen distintas categorías de interesados: las personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal; las personas condenadas por una infracción penal; las víctimas de una infracción penal o personas respecto de las cuales determinados hechos pudieran dar lugar a pensar que puedan ser víctimas de una infracción penal, y terceras partes involucradas en una infracción penal; etc. (art. 5 y 6 de la Directiva).

- Los criterios de distinción entre datos personales basados en hechos y datos personales basados en apreciaciones personales (art. 7.1 y 7.2 de la Directiva).

- El procedimiento o actuaciones para garantizar y controlar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros y las actuaciones a llevar a cabo en caso de que se hubiesen transmitido datos personales incorrectos o se hubieran transmitido ilegalmente (art. 7.3 de la Directiva).

- La identificación, en las correspondientes disposiciones legales que regulen el tratamiento (LOPJ, normas procesales penales, EOMF, etc.), de las distintas categorías de datos personales para los fines incluidos en el ámbito de



aplicación de esta norma, así como los objetivos y finalidades del mismo (art. 8 de la Directiva), debiendo indicarse, al menos, los objetivos del tratamiento, los datos personales que serán objeto del mismo, la finalidad del tratamiento, los procedimientos para el mantenimiento de la integridad y la confidencialidad de los datos personales y los procedimientos para su destrucción, proporcionando con ello garantías suficientes frente a los riesgos de abuso y arbitrariedad (Considerando 33 de la Directiva).

En este sentido la Disposición Final Cuarta del Anteproyecto introduce un nuevo artículo, el 15 bis, en la Ley Orgánica 1/1979, de 26 de septiembre, *General Penitenciaria*, en el que sí que se plasman los datos personales de los internos que serán objeto de tratamiento, aunque se omite la exigible referencia a los objetivos y finalidades de ese tratamiento, aspecto este último que debiera subsanarse.

- La conveniencia de clarificar adecuadamente las condiciones de tratamiento específicas, por lo que se habrá de distinguir entre aquellos que quedan bajo el amparo de la norma de trasposición de la Directiva y aquellos a los que les será de aplicación el RGPD.

Así, en principio, quedaría bajo el marco de la Directiva y debería permitirse el tratamiento (ya se efectúe por el mismo responsable o por otra autoridad competente) con alguno de los fines previstos en el ámbito de aplicación de la Directiva aunque ese tratamiento se efectúe para fines distintos de los originales para los que los datos personales fueron inicialmente recopilados, con la condición de que dichos fines estén autorizado con arreglo a la legislación aplicable y sean necesarios y proporcionados para dicho otro fin (Considerando 29).

Por el contrario, cuando el Derecho del Estado miembro encomiende a las autoridades competentes el desempeño de funciones que no coincidan con los



finés establecidos en el ámbito de aplicación de la Directiva se debería aplicar el RGPD (art. 9.2 de la Directiva).

- La plasmación normativa del principio de minimización del tratamiento de categorías especiales de datos personales [art. 4.1 c) y 10 de la Directiva].
- La prohibición de mecanismos de decisiones basadas únicamente en tratamientos automatizados y, en caso de autorización de las mismas, las medidas para salvaguardar los derechos y libertades de los interesados (art. 11 de la Directiva).
- La adecuada regulación del registro de operaciones a fin de verificar la legalidad del tratamiento, autocontrol, garantizar la integridad y la seguridad de los datos personales en el ámbito de las actuaciones jurisdiccionales y cuasi jurisdiccionales penales del Ministerio Fiscal (art. 25 de la Directiva).

En definitiva, resulta esencial una adecuada, completa e integrada regulación de esta materia en el ámbito jurisdiccional ya que compromete no solo el ejercicio de las funciones del Ministerio Fiscal sino también a un derecho fundamental (18.4 CE), en este caso, el de la protección de datos personales de los ciudadanos, del que también es garante el Ministerio Público, ya que el régimen general que se plasma en el Anteproyecto es insuficiente.

### **Artículo 3**

El artículo 3, se remite a las definiciones del artículo 4 del RGPD, mencionando su aplicación a los efectos de esta ley orgánica. Se entiende que dicha referencia es errónea, ya que las definiciones citadas en el artículo 4 del Anteproyecto, concuerdan con las reguladas en el artículo 3 de la Directiva 2016/680 del Parlamento y del Consejo, de 27 de abril de 2016.



Es por ello por lo que debe modificarse el precepto, en el sentido de hacer constar textualmente en el párrafo final; *“tal y como se establecen en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016”*.

## Capítulo II. Principios

### Artículo 4

El artículo 4 hace referencia a los principios del tratamiento ya definidos en la Directiva, e igualmente en su párrafo 2º menciona la obtención de datos que se obtuvieran de un fichero preexistente como complemento de los obtenidos en la recogida directa de una investigación concreta, aunque con posterioridad en los artículos 6, 8 y 9 desarrolla alguno de los principios citados en este artículo.

Sobre este precepto hay que señalar que el artículo 4.2 b) condiciona el tratamiento por el responsable o por otro, a los fines establecidos en el art. 1, apartado 1, en la medida en que el tratamiento sea necesario y proporcionado *“de acuerdo con el Derecho de la Unión Europea o la legislación española”*, pero no se entiende por qué el apartado a) del mismo artículo no recoge dicha precisión, al igual que lo hace el art. 4.2 a) de la Directiva, cuando el responsable del tratamiento esté autorizado a tratar los datos personales para dicho fin. De no unir ese párrafo parecería como si el responsable del tratamiento no precise estar autorizado legalmente para tratar los datos, sobre todo cuando se trate de un responsable distinto.

Por lo demás, siempre y cuando se cumpla con las finalidades previstas en la norma, cabe el archivo de los datos con fines de interés público, o su uso científico, estadístico e histórico, con garantías para los interesados.

### Artículo 5



El artículo 5 instituye el *deber de colaboración con las autoridades competentes*, y cita en su párrafo 1º como destinatarias del deber de colaboración a las autoridades judiciales, al Ministerio Fiscal y a la Policía Judicial. La mención a esta última sería correcta si en nuestro sistema contásemos con una Policía Judicial dependiente de Jueces y Fiscales. Sin embargo, esto no es así puesto que, de acuerdo con lo que disponen los artículos 547 a 550 de la LOPJ y lo que resulta del contenido del Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial, la dependencia de la Policía Judicial, en nuestro sistema jurídico, de Jueces y Tribunales y del Ministerio Fiscal es funcional, de tal manera que “en las funciones de investigación penal, la Policía Judicial actuará bajo la dirección de juzgados y tribunales y del Ministerio Fiscal”. Son, pues, unidades que, en última instancia, dependen de sus superiores jerárquicos no judiciales y por este motivo, los datos, antecedentes y justificantes que solicite la Policía Judicial de las Administraciones Públicas, tributaria y de la seguridad social en funciones de investigación de los delitos deberían exigir la previa existencia de un procedimiento judicial o del Fiscal abierto o una petición de la autoridad judicial o fiscal que lo respalde. Así, con la cesión de datos por parte de la AEAT, el art. 95 de la Ley General Tributaria consagra el carácter reservado de los datos con trascendencia tributaria en los siguientes términos

*“1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:*

*a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada.*



*b) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea”.*

El precepto establece, pues, dos límites, uno subjetivo y otro objetivo. En virtud del límite objetivo, solo está prevista cuando el destinatario sea un órgano jurisdiccional o el Ministerio Fiscal. Es decir, al contrario de lo que establece el artículo 5.1, no incluye la Policía Judicial. Para la cesión de datos a la Policía Judicial se requiere de autorización judicial, lo que nos reconduciría al apartado segundo del artículo 5, que sí prevé esta posible necesidad de autorización judicial (“2. *En los restantes casos, las Administraciones públicas, salvo que sea legalmente exigible la autorización judicial para recabar los datos, informes, antecedentes y justificantes...*”). Debe igualmente destacarse que las finalidades de cesión del artículo 5.1 (*investigación o enjuiciamiento de infracciones penales o para la ejecución de las penas*) son más amplias que las finalidades del artículo 95 de la LGT (*investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada*).

Otro tanto cabe predicar de la cesión de datos de la TGSS, pues el artículo 66 de su ley reguladora consagra la reserva de datos en los siguientes términos:

*“1. Los datos, informes o antecedentes obtenidos por la Administración de la Seguridad Social en el ejercicio de sus funciones tienen carácter reservado y sólo podrán utilizarse para los fines encomendados a las distintas entidades gestoras y servicios comunes de la Seguridad Social, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión o comunicación tenga por objeto:*

*a) La investigación o persecución de delitos públicos por los órganos jurisdiccionales, el Ministerio Público o la Administración de la Seguridad Social.”*



Vemos que igualmente se incluye a la Autoridad judicial y al Ministerio Fiscal, pero excluye a la Policía Judicial.

También cabría decir lo mismo respecto del Banco de España. El art. 6 del Real Decreto Legislativo 1298/1986, de 28 de junio, ha sido objeto de modificación por el art. 5 de la Ley 2/1999, de 14 de abril, y por la disposición adicional undécima de la Ley 37 /1998, de 14 de noviembre. Con arreglo a esta última modificación, el apartado 2, inciso inicial, dispone que *“los datos, documentos e informaciones que obren en poder del Banco de España en virtud de cuantas funciones le encomienden las leyes tendrán carácter reservado y no podrán ser divulgados a ninguna persona o autoridad”* y el apartado 3, inciso inicial, preceptúa que *“todas las personas que desempeñen o hayan desempeñado una actividad para el Banco de España y hayan tenido conocimiento de datos de carácter reservado están obligadas a guardar secreto”*. Y en el ámbito de las excepciones se incluyen *“las informaciones requeridas por las autoridades judiciales competentes en un proceso penal”*, excepción que se extiende al Ministerio Fiscal según el Dictamen de 22 de mayo de 2.007 sobre la procedencia de que la central de información del Banco de España proporcione determinada información al Banco de España, pero no a la Policía Judicial.

Lo mismo cabe afirmar en relación a la CNMV, regulándose en el artículo 90 Ley 24/1988, de 28 de julio, del Mercado de Valores, el secreto en los siguientes términos:

*“2. Las informaciones o datos confidenciales que la Comisión Nacional del Mercado de Valores u otras autoridades competentes hayan recibido en el ejercicio de sus funciones relacionadas con la supervisión e inspección previstas en esta u otras leyes no podrán ser divulgados a ninguna persona o autoridad.*

*4. Se exceptúan de la obligación de secreto regulado en el presente artículo:*



*c) Las informaciones requeridas por las autoridades judiciales competentes o por el Ministerio Fiscal en un proceso penal, o en un juicio civil, si bien en este último caso la obligación de secreto se mantendrá en todo lo relativo a las exigencias prudenciales de una empresa de servicios de inversión”.*

Vemos que aquí tampoco se incluye a la Policía Judicial

En otros supuestos, si bien la Policía Judicial puede ser destinataria de la información según su regulación sectorial (no hay, pues, límite subjetivo) solo lo puede ser para determinadas actuaciones, de suerte que la dicción literal del art. 5.1 no se compadece con las normas reguladoras de los distintos entes.

Tal es el caso del SEPBLAC, pues el artículo 44 contempla la colaboración con la Policía Judicial, pero lo hace solo en relación con el blanqueo de capitales y la financiación del terrorismo (*colaborar con las Fuerzas y Cuerpos de Seguridad, coordinando las actividades de investigación y prevención llevadas a cabo por los restantes órganos de las Administraciones Públicas que tengan atribuidas competencias en las materias señaladas en la letra precedente*)

En cuanto a la mención específica al Ministerio Fiscal, se incluye, presumiblemente, con el objetivo de garantizar la fluidez en la transmisión de la información y no dificultar las investigaciones de naturaleza penal, no obstante, en la práctica, puede llegar a producir el efecto contrario.

Con carácter previo a entrar en su análisis, se ha de señalar la imprecisión terminológica que contiene su redacción ya que en el apartado 1º (también el 2º) se hace referencia a “datos, informes, antecedentes y justificantes” con carácter general cuando lo correcto sería “datos personales” o “datos de carácter personal” puesto que de no hacerlo así cabría extender el ámbito de aplicación de la norma a supuestos no contemplados en ella (datos no personales).



a) El precedente de este artículo se encuentra en los arts. 11. 2 d) y 22.2 de la LOPD.

El primero de ellos, excluye la exigencia del consentimiento de los interesados cuando los datos personales a comunicar tengan por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas, no siendo tampoco preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

El art. 22.2 de la LOPD, a su vez, dispone que *“la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto (...)”*.

b) No obstante, el apartado 1º del artículo 5 (y en términos similares el apartado 2º) del Anteproyecto no transpone ninguna específica cláusula de la Directiva y básicamente lo que contempla es una presunta autorización a las administraciones públicas y a cualquier persona física o jurídica para proporcionar datos a las autoridades judiciales, a la policía judicial y al Ministerio Fiscal (en el apartado 2º se menciona a otras autoridades competentes ignorándose de quienes se trata, en lo que se refiere prevención, detección e investigación de infracciones penales, que sean distintas a las anteriores), autorización que se considera innecesaria al tiempo que, sin duda, resultará perturbadora en la práctica.



b.1) Resulta *innecesaria* ya que los sujetos a los que se refiere vendrán obligados a cumplir con el correspondiente deber de colaboración, no porque se establezca en esta disposición, sino por ser exigible en virtud de lo que disponga la correspondiente normativa específica (tal como la propia disposición señala) o bien en virtud de un deber genérico de colaboración ya sea con jueces, fiscales o con la policía judicial en base a una obligación legal, ya sea general de denunciar hechos delictivos de los que se tenga conocimiento o de colaborar con las autoridades competentes en este ámbito (tal como explicita el propio Anteproyecto en su art. 2.8), no debiéndose olvidar que de lo que aquí se trata es de la comunicación de datos personales relativos a la prevención, detección e investigación de infracciones penales (haciéndolo extensivo el apartado 2º a los supuestos relativos a la prevención y protección frente a un peligro real y grave para la seguridad pública).

En este sentido se ha de recordar que el derecho fundamental a la protección de los datos no es absoluto. La limitación de su ejercicio viene reconocida, de forma genérica, en el art. 10.1 Constitución Española cuando se residencia en el orden público y la paz social. El Tribunal Constitucional, en la STC 292/2000, señala como límite del derecho fundamental a la protección de los datos personales, entre otros, la averiguación, persecución y castigo del delito, actuando el resto de los derechos fundamentales y bienes jurídicos protegidos constitucionalmente como límite al ejercicio del derecho fundamental, en atención a la necesidad, proporcionalidad y a que sea "respetuoso con el contenido esencial del derecho fundamental restringido".

En el ámbito del proceso penal, los límites a ese derecho se encuentran entre los derechos que protege el art. 24 CE y que comprenden: el derecho a la tutela judicial efectiva, el derecho a un proceso con todas las garantías, el derecho de defensa y el derecho a la prueba.



De igual modo, resulta innecesario ya que la protección de datos personales en este ámbito, no gravita en torno al consentimiento del interesado (tal como sucede en la LO 15/1999), al disponer la Directiva que “el ejercicio de las funciones de prevención, investigación, detección o enjuiciamiento de infracciones penales que la legislación atribuye institucionalmente a las autoridades competentes permite a estas exigir u ordenar a las personas físicas que atiendan a las solicitudes que se les dirijan. En este caso, el consentimiento del interesado, según se define en el RGPD, no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes” ya que “cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad” (Considerando 35), siendo, por tanto, la base del tratamiento de datos el cumplimiento, por la autoridad competente, de una obligación legal ejecutada en el ejercicio de poderes públicos.

En el mismo sentido el RGPD, en lo que respecta a aquellos sujetos que no sean autoridades públicas, dispone que la indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable, estableciéndose como única limitación de esa transmisión la existencia de una obligación de secreto legal, profesional o vinculante por otro concepto (Considerando 50 en relación al 47).

b.2) Por otro lado, en la práctica, esa presunta habilitación que se les otorga a los sujetos obligados a colaborar, resultará *perturbadora* porque puede llegar a ser interpretada como la atribución de una potestad para decidir si los datos que se solicitan, por quienes teniendo autoridad para ello y cumpliendo las exigencias legales, son o no necesarios y/o proporcionados para la



investigación o enjuiciamiento de infracciones penales o para la ejecución de las penas, dando lugar a que aquellos puedan llegar a asumir un control de legalidad que no les corresponde e imponer así injustificadas limitaciones a la autoridad competente en el ejercicio de sus funciones.

En este sentido se ha de tener en cuenta que la Directiva dispone:

*- “Las autoridades públicas a las que se les faciliten datos personales en virtud de una obligación jurídica para el ejercicio de su misión oficial (...) no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros” (Considerando 22). Según el art. 3.10 de la Directiva es destinatario: “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerará destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o del Estado miembro; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento”.*

*“Para la prevención, investigación y enjuiciamiento de las infracciones penales, es necesario que las autoridades competentes traten datos personales recopilados en el contexto de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales concretas más allá de ese contexto específico, con el fin de adquirir un mejor conocimiento de las actividades delictivas y establecer vínculos entre las distintas infracciones penales detectadas” (Considerando 27).*



*“Los datos personales deben recogerse con fines determinados, explícitos y legítimos dentro del ámbito de aplicación de la presente Directiva y no deben ser tratados para fines incompatibles con los fines de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Si el mismo u otro responsable del tratamiento trata datos personales con alguno de los fines previstos en el ámbito de aplicación de la presente Directiva distinto del fin para el que los datos fueron recopilados, dicho tratamiento debe permitirse con la condición de que el mismo esté autorizado con arreglo a la legislación aplicable y sea necesario y proporcionado para dicho otro fin” (Considerando 29).*

“Se permitirá el tratamiento de los datos personales, por el mismo responsable o por otro, para fines establecidos en el artículo 1, apartado 1, distintos de aquel para el que se recojan en la medida en que: a) el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin de conformidad con el Derecho de la Unión o del Estado miembro, y b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión o del Estado miembro (Art. 4.2).

c) En cuanto a la frase que se añade, *in fine*, en el apartado 1º (en sentido similar en el apartado 2º) relativa a que “la petición de la autoridad competente deberá ser concreta y específica”, resulta confusa pudiendo llegar a interpretarse por los sujetos obligados a comunicar la información, por un lado, que esta solo se podrá facilitar a las autoridades competentes previa petición efectuada por las mismas y, por otro, que se les otorga, de nuevo, un control de legalidad (que no les corresponde) al permitirles decidir si se cumple o no con esa exigencia de concreción y especificidad.

d) Por otro lado, en base a lo dispuesto en la Directiva se dispone en el apartado 4 del art. 5 que *“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”, dicha redacción es confusa ya que plantea la duda de si se podrá o no informar al interesado en el caso del apartado 3 (supuestos en los que la comunicación requiere autorización judicial) y ello, cuando, a mayor abundamiento el apartado 5 del referido artículo no contempla esa salvedad.*

En consecuencia, se ha de tener en cuenta el cambio de paradigma que la Directiva ha supuesto en el ámbito del derecho a la protección de datos personales para los fines previstos en la misma por lo que la inclusión de una “autorización” a las administraciones públicas, personas físicas y jurídicas para cumplir con su deber de colaboración con las autoridades competentes resulta innecesaria y nada añade a un deber preexistente fruto de exigencias legales, genéricas o específicas, o vinculado a las normas que legitiman a las autoridades competentes para ejercer sus funciones, no siendo razonable que el examen de legalidad sobre lo solicitado pueda trasladarse a los sujetos requeridos y ello sin perjuicio de que por las autoridades competentes, cumpliendo la normativa vigente, se deban respetar los principios que inspiran el derecho a la protección de datos personales.

En virtud de todo lo expuesto, se propone que el artículo 5 se redacte del siguiente modo:

*Con el objetivo de garantizar la actividad investigadora que se lleve a cabo por las autoridades competentes, a los fines previstos en el art. 1.1 de esta ley, las administraciones públicas y las personas físicas y jurídicas a los que el ordenamiento imponga el correspondiente deber de colaboración, en ningún caso, informarán al interesado de la efectiva transmisión de sus datos personales a las autoridades competentes ni, en su caso, de la solicitud de información efectuada por estas.*



*En el supuesto de que los datos personales sean solicitados por la autoridad competente, la solicitud que esta efectúe atenderá a los principios recogidos en el art. 4.1 b) y c) de esta ley.”*

### **Artículo 6**

El artículo 6 regula los *plazos de conservación y revisión*, desarrollando en el Anteproyecto las previsiones de la Directiva que dejaba en manos de los Estados miembros la fijación de los plazos apropiados para la supresión de datos personales o para una revisión periódica de la necesidad de conservación de los datos personales.

En el Anteproyecto se establecen criterios básicos para la determinación del tiempo necesario de conservación, y se abre la posibilidad de ampliación de dicho periodo de modo excepcional y mediante resolución motivada del responsable que justifique la necesidad de la conservación.

También se regula la supresión o bloqueo de los datos en el caso de que no se motive adecuadamente la necesidad de conservarlos, por lo que se debe establecer qué regulación es aplicable al bloqueo de los datos.

En el texto tampoco se define el bloqueo de datos, por lo que debemos entender que el mismo implica que la cancelación de los datos no se materializa en el borrado físico de los mismos, sino que se mantiene la identificación y reserva de éstos con el fin de impedir su tratamiento. El RGPD no cita expresamente el bloqueo de los datos, pero configura en su artículo 23.1 una limitación de eficacia de los derechos de rectificación y supresión, que según su apartado d), *“se adoptará en los supuestos de prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección de amenazas a la seguridad pública o su prevención”*, así como la finalidad del apartado f) *“la protección de la independencia judicial o de los procedimientos judiciales”*.



Asimismo, el artículo 32 de la LOPDGDD que obliga *“al responsable del tratamiento a bloquear los datos cuando proceda su rectificación o supresión”*.

El apartado 2 del artículo 32 de la LOPDGDD prevé que *“los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas”*.

Por lo tanto, debe establecerse una definición del concepto de bloqueo de datos o remitirse a la legislación aplicable a la misma para definir el ámbito material del bloqueo.

Finalmente, debe constar en la normativa en relación con los datos personales recogidos en los ficheros jurisdiccionales penales de conformidad con los párrafos 5 y 6 del artículo 2, que en los tratamientos llevados a cabo por las autoridades jurisdiccionales y el Ministerio Fiscal haga referencia a los específicos plazos de conservación que respecto a los ficheros jurisdiccionales penales establecen las leyes procesales, a la vista de que son aquellas normas las que rigen el tratamiento de los datos en los órganos jurisdiccionales penales y Ministerio Fiscal.

### **Artículo 7**

El artículo 7, recoge la obligación de diferenciar categorías de interesados, rasgo propio del ámbito de cooperación policial y judicial en el ámbito penal, distinguiendo diversas categorías de interesados.

El artículo 7 a), cita la expresión *“personas que puedan cometer un delito”*, a la que le falta concreción, siendo más correcta la empleada por la Directiva: *“personas que van a cometer una infracción penal (o un delito)”*, refiriéndose a



los actos preparatorios.

El artículo 7 b), alude a las personas “sancionadas”, lo que implica que son aquellas que han cometido o van a cometer alguna amenaza contra la seguridad pública, ya que si no sobra la expresión y basta con habla de personas condenadas.

En el artículo 7 c), y sin perjuicio que entendamos que pueden ser más precisos los términos utilizados por la Directiva en su artículo 6 c), “*víctimas o víctimas respecto de las cuales determinados hechos den lugar a pensar que puedan ser víctimas de una infracción penal*”, que los utilizados en el Anteproyecto, probablemente sería conveniente hacer aquí una remisión a la Ley 4/2015, de 27 de abril, del Estatuto de la Víctima del delito, en cuanto realiza una distinción precisa de las diversas categorías de víctimas y de los derechos de las mismas.

#### **Artículo 8**

El artículo 8 se refiere a la verificación de la calidad de los datos personales y supone una concreción de uno de los principios establecidos en el artículo 4 (exactitud), siendo de especial importancia la diferenciación de la base del dato, entre hechos o apreciaciones personales a los efectos de determinar el tratamiento de éstos.

#### **Artículo 11**

El artículo 11 partiendo de la regla general de la imposibilidad de tratamiento de datos de categorías especiales, cuya definición cita en el párrafo 1 y que se describen en los considerandos 23, 24 y 37 de la Directiva, y en los párrafos 12, 13 y 14 del artículo 4 de la Directiva, permite el tratamiento siempre y cuando se encuentre previsto en una norma, que los haya hecho públicos el interesado, o que resulten necesarios para la protección de los derechos y libertades del interesado u otra persona física y se adopten específicas medidas técnicas y organizativas, con fundamento en los mayores riesgos que conllevan este tipo



de datos.

A este respecto, hay que partir del carácter sensible de estos datos y su entronque con el contenido esencial de los derechos fundamentales al honor, la dignidad y la intimidad de las personas, de tal manera que el artículo 18.4 de la Constitución española dispone que *“la ley limitará el uso de la informática para garantiza el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*. Por este motivo, aunque no se observa ningún obstáculo a que el tratamiento de estos datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, biométricos, relativos a la salud o a la vida u orientación sexual de una persona física pueda realizarse cuando sea estrictamente necesario y cuando *“se encuentre previsto por una norma con rango de ley o de una norma del Derecho de la Unión Europea”* [artículo 11.1 a) del Anteproyecto], sí puede haberlo en el tratamiento de tales datos cuando *“resulte necesario para proteger los derechos y libertades fundamentales del interesado”* (apartado b) del artículo 11.1 del Anteproyecto) o cuando el tratamiento se *“refiera a datos que el interesado haya hecho manifiestamente públicos”*. En primer lugar, porque no se precisan cuáles sean las *“salvaguardas adecuadas”* a las que se refiere el artículo 10 de la Directiva (UE) 2016/580 o las *“garantías adecuadas”* exigidas por el propio artículo 11.1 y, en segundo lugar, porque es difícil justificar un juicio de proporcionalidad para tratamiento de tales datos a los fines establecidos en el artículo 1.1. del Anteproyecto. De aquí que se proponga, en estos supuestos, sujetar el tratamiento de tales datos a las condiciones específicas a las que se refiere el artículo 10 del Anteproyecto, es decir, la de informar al destinatario de las condiciones específicas de tratamiento y de la obligación de respetarlas, la prohibición de transmisión de dichos datos o de su utilización con fines distintos para los que fueron transmitidos y, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora.



En cuanto al tratamiento de los datos de los menores de edad, el artículo 11.2 indica que se hará garantizando “ el interés superior de los mismos y con un nivel adecuado de seguridad”. Al igual que en el caso anterior, es observar una escasa garantía en el tratamiento de datos de los menores de edad.

Igualmente debería haberse incluido en este apartado el tratamiento de los datos de personas con capacidad modificada judicialmente o que estén incurso en un proceso de esta naturaleza.

### **Artículo 12**

El artículo 12 prohíbe la utilización del mecanismo de decisión individual automatizado, que se define en el párrafo 4 del artículo 3 de la Directiva. En este sentido, está prohibido basar únicamente la decisión en el tratamiento de los datos automatizados, o en la elaboración de perfiles, siempre y cuando produzcan efectos negativos o repercutan de forma adversa en el interesado.

En el artículo 22 del RGPD se desarrolla de forma muy similar la regulación, estableciéndose las excepciones que permiten dicho tratamiento y el derecho a obtener la revisión humana en el proceso de revisión de la decisión adoptada.

Como especialidad en relación con el RGPD se incluye la prohibición de los perfiles que sean discriminatorios basándose en las categorías especiales de datos antes citadas.

### **Capítulo III. Derechos de las personas**

El Anteproyecto aborda la regulación del ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento de los datos personales por los interesados distinguiendo entre el régimen general al que dedica la Sección 1ª del Capítulo III (artículos 13 a 18), y el régimen



especial de ejercicio de los derechos cuando el tratamiento de datos personales sea consecuencia de investigaciones y procesos penales, regulado en la Sección 2ª del mismo Capítulo (artículo 19), y que comprende el ejercicio de los derechos de información, acceso, rectificación y supresión cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales, comprendiendo, por tanto, los datos personales que son objeto de tratamiento por el Ministerio Fiscal en el ejercicio de sus funciones, previéndose en tal caso que el ejercicio de los derechos por los interesados se llevará a cabo de conformidad con las normas procesales penales, y en su defecto prevé la aplicación supletoria del régimen general.

Comprende también el régimen especial el ejercicio de tales derechos cuando los datos sean objeto de tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, que se realizará de conformidad con lo previsto en la LOPJ, y en las normas procesales, estableciendo la aplicación supletoria del régimen general, en defecto de regulación del ejercicio de estos derechos en dichas normas.

### **Artículo 13**

El artículo 13 regula las condiciones generales de ejercicio de los derechos de los interesados trasladando las previsiones de la Directiva, estableciendo la obligación del responsable del tratamiento de facilitar al interesado, de forma concisa, inteligible, de fácil acceso y con lenguaje claro y sencillo, la información contemplada en el artículo 14, así como la derivada de los artículos 12, 15 a 19 y 32.

De conformidad con las previsiones del considerando 40 de la Directiva que señala que *“Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos con arreglo a las disposiciones adoptadas de conformidad con la presente Directiva, incluidos los mecanismos para solicitar y, en su caso,*



*obtener, de forma gratuita, el acceso a sus datos personales, así como su rectificación o supresión y la limitación de su tratamiento. El responsable del tratamiento debe estar obligado a responder sin dilación indebida a las solicitudes del interesado, salvo que aplique restricciones a los derechos del interesado de conformidad con la presente Directiva”, se propone que se modifique el apartado 1 del artículo 13, en el sentido de que se añada al final de éste lo siguiente: “salvo que se apliquen restricciones a los derechos de los interesados de conformidad con lo dispuesto en el artículo 17”.*

Se ha optado por la técnica legislativa de recoger en un precepto posterior, artículo 17, las restricciones comunes a los derechos de información, acceso, rectificación o supresión de datos personales y a la limitación de su tratamiento, en lugar de recoger las restricciones al ejercicio de cada uno de los derechos de los interesados en los preceptos que regulan los correspondientes derechos.

Se establece, de conformidad con las previsiones de la Directiva, que la facilitación de la información será gratuita, salvo que las solicitudes de un interesado sean manifiestamente infundadas o excesivas, debido a su carácter repetitivo, restringiendo en este sentido las previsiones recogidas en el artículo 12 de la Directiva, que no limita las solicitudes manifiestamente infundadas o excesivas a las repetitivas, sin que esté justificada esta limitación, toda vez que el responsable, en cualquier caso está obligado a demostrar y justificar el carácter manifiestamente infundado o excesivo de la solicitud.

En caso de solicitudes manifiestamente infundadas o excesivas, *“el responsable del tratamiento podrá inadmitirlas a trámite o, en el caso de que se establezca, percibir una contraprestación económica”*, percepción de tasa o canon que está prevista en el artículo 12 de la Directiva y que habrá de ser objeto de regulación posterior.

#### **Artículo 14**



El artículo 14 aborda el contenido mínimo de la información que debe poner el responsable del tratamiento a disposición del interesado en los términos establecidos en el artículo 13 de la Directiva.

### **Artículo 15**

El artículo 15 regula el derecho de acceso del interesado a sus datos personales en los términos establecidos en el artículo 14 de la Directiva.

Se introducen en el precepto previsiones, no contempladas en la Directiva, en cuanto a la cantidad de información solicitada por el interesado, al modo de facilitar el acceso al interesado a través de un sistema remoto, directo y seguro, y la posibilidad de que el interesado elija un modo distinto de acceso del que se le ofrece por el responsable que suponga un coste desproporcionado, en cuyo caso la solicitud se considera excesiva y el afectado deberá asumir el exceso de costes que su elección comporte.

Tales previsiones se recogen en el artículo 13 de la LOPDGDD que se han trasladado en los mismos términos al presente Anteproyecto.

### **Artículo 16**

El artículo 16 regula el derecho de los interesados a obtener del responsable del tratamiento la rectificación de datos cuando sean inexactos o la supresión de datos personales, a instancia del interesado o a iniciativa del propio responsable, cuando el tratamiento infrinja los artículos 4, 9 u 11, o cuando los datos deban ser suprimidos en virtud de una obligación legal, de conformidad con las previsiones del artículo 16 de la Directiva.

El art. 16.3.b) al hablar de la limitación, en lugar de la supresión, de los datos personales por el responsable del tratamiento, exige la concurrencia de dos circunstancias. Pues bien, las del apartado b), cuando los datos hayan de conservarse a efectos probatorios, añade la siguiente frase "*o, en particular, por*



*razones de seguridad*". Esto supone una ampliación de lo dispuesto en el art. 16.3 b) de la Directiva sin que se justifique las razones por las que el responsable limite el tratamiento de datos personales por razones de seguridad y no exclusivamente a efectos probatorios.

Se recogen asimismo las previsiones de la Directiva en relación con la comunicación de la rectificación a la autoridad competente de la que provengan los datos, así como la notificación de los datos rectificadas o suprimidos o la limitación del tratamiento a los destinatarios para que procedan a la rectificación, supresión de los datos o a la limitación del tratamiento.

### **Artículo 17**

El artículo 17 ha optado por la técnica legislativa de recoger en este precepto las restricciones comunes a los derechos de información, acceso, rectificación o supresión de datos personales y a la limitación de su tratamiento, en lugar de recoger las restricciones al ejercicio de cada uno de los derechos de los interesados en los preceptos que regulan su ejercicio por los particulares, separándose en este punto el Anteproyecto de la Directiva.

*El considerando 44 de la Directiva establece que "Debe permitirse a los Estados miembros adoptar las medidas legislativas que retrasen, limiten u omitan que se facilite información a los interesados o que limiten, total o parcialmente, el acceso de los interesados a sus datos personales, en la medida en que dichas medidas sean necesarias y proporcionadas en una sociedad democrática y mientras sigan siéndolo, con el debido respeto a los derechos fundamentales y los intereses legítimos de la persona física afectada, con el fin de no entorpecer las indagaciones, investigaciones o procedimientos oficiales o judiciales, de no perjudicar la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, de proteger la seguridad pública o la seguridad nacional o de salvaguardar los derechos y las libertades de terceros. El responsable del tratamiento debe evaluar, mediante*



*un análisis individual y específico de cada caso, si procede o no restringir, total o parcialmente, el derecho de acceso”.*

Se cumple así el objetivo de garantizar la protección de datos personales en el marco de la investigación penal, reforzando la protección de los interesados mediante el reconocimiento específico de sus derechos, pero también el de impedir que las limitaciones al tratamiento de datos personales perjudiquen en definitiva los fines de prevención, investigación o represión de las infracciones penales, impedir que se obstaculicen investigaciones o procedimientos, proteger la seguridad pública, la Seguridad Nacional y los derechos y las libertades de otras personas.

En el apartado 2 del artículo 17 del Anteproyecto se recoge la obligación del responsable de informar por escrito al interesado de cualquier restricción de sus derechos en los casos contemplados en los artículos 14 y 15, de las razones de la restricción, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta ley orgánica. En el segundo párrafo del referido apartado se prevé que *“las razones de la restricción puedan ser omitidas cuando la aportación de dicha información pueda poner en riesgo los fines a los que se refiere el apartado 1”*.

Si bien la remisión del artículo 17 comprende los artículos 14 (derecho de información) y 15 (derecho de acceso), la Directiva prevé la obligación de informar (y su omisión cuando la aportación de la información pueda poner en riesgo los fines previstos en la misma) en relación a los supuestos de denegación o limitación del derecho de acceso y en el supuesto de denegación de rectificación o supresión de datos personales o de limitación del tratamiento regulado en el artículo 16 del Anteproyecto.

Sin embargo, el artículo 17 del Anteproyecto no recoge la posibilidad de



restringir la obligación del responsable de tratamiento de proporcionar información al interesado en los casos de denegación de rectificación o supresión de datos personales o de limitación de su tratamiento regulado en el artículo 16, omisión que no está justificada en modo alguno, toda vez que el título del artículo 17 hace referencia a las *“restricciones a los derechos de información, acceso, rectificación o supresión de datos personales y a la limitación de su tratamiento”* y que la restricción de la obligación de proporcionar información está prevista en el apartado 4 del artículo 16 de la Directiva que establece que:

*“Los Estados miembros dispondrán que el responsable del tratamiento informe al interesado por escrito de cualquier denegación de rectificación o supresión de los datos personales, o de limitación de su tratamiento, y de las razones de la denegación. Los Estados miembros podrán adoptar medidas legislativas por las que se restrinja, total o parcialmente, la obligación de proporcionar tal información, siempre y cuando dicha limitación del tratamiento constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:*

- a) Evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;*
- b) Evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o la ejecución de sanciones penales;*
- c) Proteger la seguridad pública;*
- d) Proteger la Seguridad Nacional;*
- e) Proteger los derechos y libertades de otras personas”.*

En consecuencia, procede la modificación del artículo 17 añadiendo la previsión del apartado 4 del artículo 16 de la Directiva.

Por último, se pone de manifiesto que existe un error en la numeración de los



apartados de este precepto, por omisión de un párrafo 3º.

### **Artículo 18**

El artículo 18 recoge la posibilidad de ejercicio de los derechos del interesado a través de la autoridad de protección de datos de conformidad con lo establecido en el artículo 17 de la Directiva, y del responsable del tratamiento de informar en tal sentido al interesado, si bien se remite a los casos contemplados en el artículo 15.3 y 16.1 del Anteproyecto, (probablemente por error en las remisiones al variar la numeración en la redacción del articulado del Anteproyecto) que no coinciden en modo alguno con lo dispuesto en la Directiva. No obstante, ello, por las razones que se expondrán más adelante, en el apartado 6 de este informe (relativo a los capítulos VI, VII y VIII), se propone la siguiente redacción del artículo 18:

*1. En los casos contemplados en los artículos 15.3 y 16.1, el responsable del tratamiento informará al interesado de la posibilidad de que sus derechos sean ejercitados a través de la autoridad de protección de datos o en su caso, y en su respectivo ámbito, ante el Consejo General del Poder Judicial y la Unidad de Protección de Datos del Ministerio Fiscal.*

*2. Cuando, en virtud de lo establecido en el apartado anterior, sea la autoridad de protección de datos o, en su respectivo ámbito, los organismos mencionados en el apartado anterior, los que ejerciten los derechos, éstos deberán 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.*

### **Artículo 19**

El artículo 19 establece un régimen especial para el ejercicio de los derechos de los interesados como consecuencia de investigaciones y procesos penales,



distinguiendo en distintos apartados entre el ejercicio de los derechos de información, acceso, rectificación y supresión cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales, lo cual se llevará a cabo de conformidad con las normas procesales penales, y el ejercicio de tales derechos cuando los datos sean objeto de tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, en cuyo caso el ejercicio de los derechos de información, acceso, rectificación y supresión se realizará de conformidad con lo previsto en la LOPJ, y en las normas procesales. El apartado 3 establece que en defecto de regulación del ejercicio de estos derechos en dichas normas se aplicará lo dispuesto en esta ley orgánica.

Dicho régimen especial deriva del art. 18 de la Directiva, el cual establece que los estados miembros podrán disponer que el ejercicio de los derechos a los que se hace referencia en los artículos 13, 14 y 16 (acceso, rectificación o supresión y la limitación al tratamiento) se lleve a cabo de conformidad con el Derecho del Estado miembro cuando los datos personales figuren en una resolución judicial o en un registro o expediente tramitado en el curso de investigaciones y procesos penales”, estableciendo el art. 15, por su lado, una serie de limitaciones al derecho de acceso dirigidas a evitar que se obstaculice o se cause perjuicio a la investigaciones o enjuiciamiento de infracciones penales o para proteger los derechos y libertades de otras personas.

No obstante, la plasmación de dicho régimen especial en el Anteproyecto no solo es confusa, sino que establece injustificadamente distintos cauces para el ejercicio de los derechos relativos a la protección de datos, así:

En el apartado 1º remite a las normas procesales penales para el ejercicio de los derechos relativos a datos personales que figuren en una resolución judicial, en un registro, en diligencias o expedientes tramitados en el curso de



investigaciones y procesos penales, y, dado que no menciona a ningún responsable de tratamiento, a diferencia de lo que sucede en el apartado 2º en el que se menciona expresamente a los órganos judiciales, habrá de interpretarse que se refiere a cualquier otra autoridad competente, por lo que indirectamente se está incluyendo, entre otros, al Ministerio Fiscal.

Por otro lado, en el apartado 1º, pese a que los datos personales a que se refiere se encuentren incluidos en una resolución judicial, en un registro, en diligencias o expedientes tramitados en el curso de investigaciones y procesos penales para el prelegislador no parece que los mismos sean objeto de tratamiento con fines jurisdiccionales, ya que esa naturaleza parece reservada, según el apartado 2º, al tratamiento efectuado por los órganos judiciales, en cuyo caso se ejercitará según lo dispuesto en la LOPJ y en las normas procesales.

En relación a ello se han de hacer las siguientes consideraciones:

a) El carácter jurisdiccional de un tratamiento no estriba en que se lleve a cabo por un órgano judicial ya que la propia Directiva considera como jurisdiccionales los tratamientos de datos realizados por el Ministerio Fiscal.

Por tanto, el Ministerio Fiscal, tal como parece que se pretende en el Anteproyecto, no debe tener un tratamiento distinto al de los órganos judiciales dada su condición de autoridad judicial a los efectos de la Directiva y del RGPD, ya que se ha de aceptar que el mismo, por las razones que ya se han explicado, además de tratamientos de datos personales no jurisdiccionales, lleva a cabo otros de naturaleza jurisdiccional.

b) El Anteproyecto parece ignorar la existencia, en la actualidad, de aplicaciones informáticas de gestión procesal (en este caso penal y penitenciaria) integradas y/o de uso compartido entre los órganos judiciales y el Ministerio Fiscal por lo



que, con el fin de evitar incongruencias en los registros, resultará inviable el tratamiento diferenciado que se pretende en lo que al ejercicio de los derechos de los interesados se refiere.

c) A la luz de la actual regulación, en el supuesto de que se trate de datos derivados de procedimientos judiciales, el ejercicio de derechos de protección de datos ante el Ministerio Fiscal inevitablemente se habrán de tramitar, a la vista de lo dispuesto en el art. 236 octies 1 de la LOPJ, conforme a las normas que resulten de aplicación al correspondiente proceso penal en el que fueron recabados, razón por la que, en caso de que los referidos derechos pretendan ser ejercidos ante él, no tendrá opción distinta a la de resolver motivadamente indicando a los interesados que carece de competencia para ello e informar a los mismos que podrán efectuar esa solicitud ante los correspondientes órganos judiciales.

El art. 236 octies 1 también sería de aplicación en lo que se refiere al ejercicio de los derechos relacionados con los tratamientos de datos jurisdiccionales derivados de una actividad jurisdiccional propia del Ministerio Fiscal, como es la que desarrolla en virtud de la LORPM, asumiendo en este caso el Ministerio Fiscal, como responsable del tratamiento, la condición de autoridad competente.

No obstante, y pese a lo dispuesto en dicho artículo, se ha de tener presente que las normas procesales no solamente son anteriores a la normativa de protección de datos actual, sino que tampoco contienen una regulación específica respecto del ejercicio de derechos relativos a la protección de datos personales, por lo que será la autoridad competente la que deberá realizar el esfuerzo para localizar algún precepto procesal que permita el ejercicio de cada uno de esos derechos, siendo la LOPJ y no las normas procesales penales la que, aunque de modo insuficiente, recogen determinados artículos relacionados con el ejercicio de derechos.



Por otro lado, y respecto a las otras actividades de naturaleza jurisdiccional o cuasi jurisdiccional derivadas de la tramitación y resolución de diligencias de investigación, el cauce al ejercicio de los derechos de los interesados se lleva a cabo en base a lo dispuesto en los instrumentos legales que emanan de la Fiscalía General del Estado, tales como la Circular 4/2013, de 30 de diciembre, *sobre las diligencias de investigación* y la Consulta 1/2015, *sobre el acceso a lo actuado en las diligencias de investigación por quien invoca un interés legítimo*, en las cuales se establecen los criterios, que analógicamente a lo dispuesto en el art. 236 octies 1 de la LOPJ, servirían de cauce y, en su caso, limitación al ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con los datos personales tratados como consecuencia de su tramitación.

Sin duda el ejercicio de los derechos reconocidos en la normativa de protección de datos por parte de las distintas categorías de interesados es una materia compleja que hubiera requerido de un mayor esfuerzo que el que se aprecia en el art. 19 del Anteproyecto, ya que, básicamente, lo que hace dicho precepto es remitirse a una normativa que en la actualidad no brinda suficiente cobertura legal al ejercicio de la totalidad de esos derechos.

Por otro lado, la remisión supletoria al propio Anteproyecto (art. 19.3) ofrece una muy precaria y confusa solución, ya no solo por las singularidades de los procesos penales y el ejercicio de la actividad jurisdiccional, sino por el hecho de que, contrariamente a lo que ahí se dispone, la LOPJ establece que a las solicitudes de ejercicio de los derechos por los interesados en materia de protección de datos tratados con fines jurisdiccionales no le son de aplicación las disposiciones establecidas al efecto por la legislación vigente en materia de protección de datos de carácter personal (art. 236 octies 1).

En virtud de todo lo expuesto, y en la confianza de una próxima, completa e integrada regulación en la legislación procesal del ejercicio de los derechos



relativos a la protección de datos, y de manera semejante a como se regula esta cuestión en el art. 12.5 de la LO 3/2018, se propone la siguiente redacción del art. 19:

*“El ejercicio de los derechos contemplados en los artículos anteriores, en relación con el tratamiento de datos personales realizado con fines jurisdiccionales, se tramitará de conformidad con lo dispuesto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y, en su caso, conforme a las normas que resulten de aplicación al proceso, diligencias o expedientes en que esos datos figuren”.*

#### **Capítulo IV. Responsable y encargado del tratamiento**

En el Capítulo IV del Anteproyecto se plasma la trasposición del derecho nacional de las obligaciones de responsabilidad activa establecidos en la Directiva, las cuales, en términos generales, se han reproducido fielmente, por lo que únicamente cabe señalar que las mismas son de aplicación al Ministerio Fiscal, como autoridad competente y responsable del tratamiento, no suponiendo ninguna novedad a la vista de lo dispuesto de modo similar en el RGPD y en la L.O. 3/2018, así como en base a lo regulado por la Instrucción de la FGE 2/2019, sobre protección de datos en el ámbito del Ministerio Fiscal.

#### **Artículo 20**

El artículo 20 recoge, de conformidad con las previsiones del artículo 19 de la Directiva, la obligación del responsable del tratamiento de aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme a la propia ley orgánica, a lo previsto en la legislación sectorial y en sus normas de desarrollo, así como a lo dispuesto en la LOPJ o en la legislación procesal que resulte de aplicación, en los supuestos previstos en el artículo 19, si bien por error se remite al artículo 18, de modo que debe procederse a su modificación.



### Artículo 25

El artículo 25 regula la obligación del responsable del tratamiento de conservar un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad, así como la obligación del encargado del tratamiento de llevar un registro de todas las actividades de tratamiento de datos personales que efectúe en nombre de un responsable y el contenido del registro en los términos previstos en el artículo 24 de la Directiva.

El art. 25.1 f) presenta una diferencia en comparación con al art. 24.1 f), correspondiente al de la Directiva, ya que esta no limita las categorías de transferencias de datos personales “a un tercer país que no sea miembro de la UE...”, sino que se refiere en sentido amplio a terceros países.

### Artículo 28

El artículo 28 regula la obligación del responsable de efectuar una evaluación de impacto relativa a la protección de datos, contemplada en el artículo 27 de la Directiva, cuando sea probable que un tipo de tratamiento, como consecuencia de la utilización de nuevas tecnologías, o por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas.

A este respecto, el anteproyecto dice: *“La evaluación incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros...”*

Conforme al artículo 27 de la Directiva resulta más correcto hablar de “riesgos”, por lo que sería procedente eliminar la referencia a “peligros” para sustituirla por la empleada en la Directiva.

### Artículo 29



El artículo 29 establece la obligación del responsable y encargado del tratamiento de consultar a la autoridad de protección de datos antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo fichero en los casos en que el tratamiento entrañe o pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, estableciendo que la autoridad de protección de datos debe asesorar al responsable o al encargado del tratamiento, los plazos y la posibilidad de que la autoridad de protección ejerza sus potestades de investigación, corrección o consulta, de conformidad con las previsiones del artículo 28 de la Directiva.

### **Artículo 30**

El artículo 30 aborda la regulación de la seguridad del tratamiento, estableciendo la obligación del responsable y del encargado del tratamiento de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías especiales de datos, especificando las medidas de control que deben ser aplicadas por el responsable o encargado del tratamiento, en cuanto al tratamiento automatizado, a raíz de una evaluación de los riesgos, recogiendo las medidas establecidas en el artículo 29 de la Directiva.

### **Artículo 31**

El artículo 31 recoge la obligación del responsable del tratamiento de notificar a la autoridad de protección de datos una violación de la seguridad de los datos personales, los supuestos dispensados, el plazo, el contenido de la notificación y la necesidad de su documentación, siguiendo las previsiones del artículo 30 de la Directiva.

*Al respecto del artículo 31 de la Directiva, 1, donde dice: "Cualquier violación de la seguridad de los datos personales será notificada por el responsable del tratamiento a la autoridad de protección de datos, a menos que sea improbable que la violación de la seguridad de los datos personales constituya un peligro*



*para los derechos y las libertades de las personas físicas. La notificación deberá realizarse en las setenta y dos horas siguientes.”*

Por idénticas razones a las expuestas más arriba, proponemos sustituir la palabra “*peligro*” por “*riesgo*” (Art 30 de la Directiva).

### **Artículo 33**

El artículo 33 afronta la regulación de la designación del delegado de protección de datos, estableciendo la no obligatoriedad de su designación por el responsable del tratamiento cuando el tratamiento tenga fines jurisdiccionales.

El apartado 1 del artículo 32 de la Directiva, se refiere a la posibilidad de que los Estados miembros eximan de esa obligación “*a los tribunales y demás autoridades judiciales independientes cuando actúen en ejercicio de sus competencias judiciales*” y en términos parecidos se recoge en el considerando 63 de la Directiva.

Al respecto cabe señalar lo dispuesto en el considerando 80 al señalar que “*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*”.

## **Capítulo V. Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea u organizaciones internacionales**

### **Artículo 36**

El artículo 36 parte de la necesidad de establecer normas jurídicas para el intercambio de información entre las autoridades españolas y terceros países



que no sean miembros de la Unión Europea u organizaciones internacionales, con el fin de facilitar la cooperación transfronteriza de las autoridades competentes en el ejercicio de las funciones de prevención, investigación, detección o enjuiciamiento de las infracciones penales, así como su libre circulación entre las autoridades competentes, respetando el núcleo de dicho derecho por parte de las autoridades encargadas de la transmisión de datos personales en un proceso penal, o en materia de prevención, de conformidad con los principios establecidos en los considerandos 64 a 66 de la Directiva .

Se establecen las condiciones generales necesarias para que se consideren válidas las transmisiones en el párrafo primero, las circunstancias que permiten las transferencias por parte de las autoridades españolas sin autorización de otro Estado miembro (prevención de amenaza inmediata y grave para la seguridad pública de un Estado miembro o de un tercer país), en el caso de que la autorización no se consiguiera a su debido tiempo.

Finalmente, se añade el establecimiento de mecanismos de cooperación internacional y asistencia mutua para fomentar la aplicación efectiva de la legislación sobre datos personales.

Entendemos que deben definirse o fijarse con claridad los términos a los que se refiere la Directiva, tales como “amenaza”, “gravedad” y “nivel adecuado”, al generar inseguridad, ya que por citar un concepto no especificado, se desconoce cómo valorar la adecuación en el supuesto de que el Estado miembro tenga un nivel superior de garantías al que la Unión considere como “nivel adecuado”, por lo que podría considerarse la adecuación como “un nivel mínimo de protección” que deberían cumplir todos los terceros países a los que se transfieren datos personales.

## Capítulo VI. Autoridades de protección de datos



#### Artículo 41

El artículo 41 regula la “*autoridad de protección de datos*” frente al concepto “*autoridad de control*”, que establece la normativa europea, entendida como autoridad pública independiente que supervisa la aplicación de la presente Directiva.

El legislador español ha optado por la Agencia Española de Protección de Datos como autoridad de control, de conformidad con el párrafo 3º del artículo 41 de la Directiva, al disponer que la AEPD, que es la autoridad de control creada en la LOPDGDD para la protección de datos en desarrollo de las previsiones del RGPD, sea quien asuma la responsabilidad de las funciones de control de protección de los datos tratados de conformidad con el artículo 1 de la presente ley.

El problema de la redacción del párrafo 1º de este artículo 41, es que no se ha tenido en cuenta lo establecido en el artículo 45 de la Directiva cuyo párrafo 2º dice “*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*”. Es por ello, que la actuación de la Agencia Española de Protección de Datos y de las agencias de protección de datos definidas en el presente artículo no puede extenderse a los ficheros jurisdiccionales.

Por lo tanto, la Directiva habla en primer lugar de “*órganos jurisdiccionales en el ejercicio de su función judicial*”, que el artículo 2 apartado 5º del Anteproyecto considera que, en cuanto al tratamiento de datos, se rigen por lo dispuesto en la Ley Orgánica 6/1985, de 1 de Julio, del Poder Judicial, por las leyes procesales penales, y subsidiariamente por el capítulo III de la presente



ley, relativa a los derechos de las personas, y en segundo lugar, de "*otras autoridades judiciales independientes*", para referirse al Ministerio Fiscal, cuyos tratamientos se regulan por lo dispuesto en el artículo anterior y el EOMF.

En cuanto a los órganos jurisdiccionales en el ejercicio de su función judicial, la propia Directiva establece una limitación a la autoridad de control, ya que impone a los Estados miembros la exclusión de control de aquellos tratamientos de datos personales efectuados por órganos jurisdiccionales en el ejercicio de su función judicial, del mismo modo que lo hacen el artículo 55.3 del RGPD, o los artículos 2.4 y 44.3 de la LOPDGDD, que separan el ámbito de control de ambos y el artículo 10.1 de la LOPDGDD que establece que solo se tratarán por la AEPD los datos penales que no gocen de la condición de los establecidos en la Directiva.

En cuanto a "*otras autoridades judiciales independientes*", de conformidad con lo establecido en el artículo 45.2 de la Directiva, y en los considerandos 20, 49 y 80, el Ministerio Fiscal es autoridad judicial independiente y el legislador se ha inclinado, al introducir el artículo 2, apartado 6º del Anteproyecto, por disponer que las operaciones de tratamiento en ella citadas queden excluidas del control de la autoridad de control prevista en el artículo 41 del Anteproyecto. No obstante, el cumplimiento de las normas de la presente Directiva por los órganos jurisdiccionales y otras autoridades judiciales independientes debe estar siempre sujeto a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta (considerando 80).

Es por ello por lo que deben llevarse a cabo las modificaciones normativas pertinentes que determinen la creación de las autoridades de control independientes en ambos tipos de órganos, que en el caso del Ministerio Fiscal debería llevarse a cabo mediante la modificación del EOMF.



Por otro lado, entendemos que la mención que se hace a la sujeción a los artículos 52 a 54 del Reglamento (UE) 2016/679 del Parlamento y del Consejo no es ajustada, ya que la propia Directiva tiene establecidas sus normas en los artículos 42 a 44, que regulan la independencia, las condiciones generales aplicables a los miembros de la autoridad de control y las normas relativas a la autoridad de control.

## Capítulo VII. Reclamaciones

### Artículo 46

El artículo 46 se remite al artículo 56 de la Directiva que establece “*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 de cualquier autoridad competente en virtud del Derecho del Estado miembro por los daños y perjuicios sufridos*”.

En la trasposición de la Directiva se regula el derecho a indemnización a los interesados basado en dos criterios, por un lado, la existencia de daño o lesión, y, por otro lado, que su origen sea el incumplimiento de lo dispuesto en el Anteproyecto.

El presente artículo regula la indemnización a cargo de *entes del sector público*, refiriendo como obligados a la indemnización a los responsables y encargados o las autoridades de protección de datos en los supuestos en que se den las circunstancias que permiten la indemnización. Asimismo, se establece la normativa que regula el régimen de exigencia de responsabilidad en función de que se trate de ficheros de una autoridad administrativa o de una autoridad judicial.



Sin embargo, deberían establecerse unas normas más claras para delimitar la responsabilidad en cada caso concreto del responsable y encargado a los efectos de la indemnización, como las que aparecen previstas en el artículo 82 del RGPD.

## Capítulo VIII. Régimen sancionador

### Artículo 50

El artículo 50 a diferencia del correlativo de la LOPDGDD, únicamente define las infracciones muy graves dejando fuera de su ámbito los plazos de prescripción de las infracciones y sanciones penales que se regulan en el artículo 54.

Los criterios utilizados para distinguir la infracción muy grave de la infracción grave se basan en el carácter grave de la vulneración, o en la causación de perjuicios de carácter muy grave a los interesados, puesto que muchas de las infracciones previstas son susceptibles de ser catalogadas en una u otra categoría.

Respecto al catálogo de infracciones muy graves, entendemos que las sanciones previstas en los apartados f y l son coincidentes, ya que en ambos casos se requiere para la sanción que se haga al margen de las circunstancias previstas en el artículo 11, por lo que podría refundirse el precepto en un único apartado.

Igualmente, cabe destacar cierta similitud con algunas de las establecidas en la LOPDGDD, añadiéndose de nuevo cuño únicamente las letras o y p.

### Artículo 52

Respecto de la letra p) de este precepto, donde dice: *“La falta de notificación a la autoridad de protección de datos competente acerca de una violación de la*



*seguridad de los datos personales, cuando sea exigible, así como la ausencia de comunicación al interesado del peligro de producirse una violación de la seguridad de los datos personales, siempre que se deriven perjuicios de carácter muy grave para el interesado”, por las razones expuestas con reiteración estimamos que “peligro” ha de sustituirse por “riesgo”.*

### **Artículo 53**

El artículo 53 en materia de sanciones se remite a las sanciones establecidas en el artículo 77.2 de la LOPDGDD, que establece *“que cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones tipificadas en los artículos 72 a 74 ALOPD, “la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido”.*

En segundo lugar, y para el supuesto de que el infractor no sea alguno de los señalados en el art 77.1, se establece una sanción de multa, cuya cuantía se refleja en el precepto.

En tercer lugar, y para la graduación de la multa se recurre a lo establecido en el artículo 83.2 del RGPD, que establece los criterios de graduación, que han sido incorporados en el artículo 76.2 de la LOPDGDD.

De lo dicho se deduce que la AEPD podría imponer al Ministerio Fiscal, como consecuencia del tratamiento de datos con fines jurisdiccionales y por alguna de las infracciones contempladas en el régimen sancionador, la sanción de apercibimiento y, en su caso, la sanción de amonestación cuando existieran informes técnicos que no hubieran sido atendidos, sanción que incluirá la denominación del cargo del responsable, la cual será publicada en el BOE (art. 77 2 y 3 LO 3/2018).



Por todo ello y dado que el Anteproyecto no excluye al Ministerio Fiscal del ámbito de actuación y competencias de la AEPD, se han de realizar las siguientes consideraciones:

a) En primer lugar, la nueva normativa de protección de datos se ha de integrar, como cualquier otra, en el ordenamiento jurídico existente el cual, respecto de lo que aquí se trata, define al Ministerio Fiscal como órgano de relevancia constitucional con personalidad jurídica propia, independiente en el ejercicio de sus funciones de los distintos poderes del estado (art. 7 EOMF) e integrado con autonomía funcional en el Poder Judicial y que ejerce su misión por medio de órganos propios (art. 2.1 EOMF).

b) Respecto de las autoridades de control, la Directiva que se traspone, en el apartado 2º del art. 45, 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”*.

Por otro lado, el Considerando 80 de la Directiva, como ya se ha señalado, además de equiparar al Ministerio Fiscal con las autoridades judiciales establece que los Estados miembros pueden disponer 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.

El referido Considerando subraya que, en todo caso, el cumplimiento de las normas de la presente Directiva por los órganos judiciales independientes debe



estar sujeto siempre a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta de los Derechos Fundamentales de la Unión Europea.

A su vez, el Considerando 82 de la Directiva, establece que las competencias de la autoridad de control no deben afectar a las normas específicas previstas para los procesos penales, incluidos la investigación y el enjuiciamiento de infracciones penales, ni a la independencia del Poder Judicial.

c) A diferencia de lo dispuesto en la LO 3/2018, en el capítulo VI del Anteproyecto se omite cualquier referencia a la distribución de competencias entre la AEPD y el CGPJ.

No obstante, según dispone el art. 236 nonies de la LOPJ, las competencias que la LO 15/1999 atribuye a la Agencia Española de Protección de Datos serán ejercidas, respecto de los tratamientos efectuados con fines jurisdiccionales y los ficheros de esta naturaleza, por el CGPJ.

La referencia que se realiza en dicho artículo de la LOPJ a la LO 15/1999 habrá de entenderse que se refiere tanto a la LO 3/2018 como a la ley que sea fruto de este Anteproyecto, y ello pese a que este no contemple, en ese aspecto, la "actualización" del art. 236 nonies LOPJ, ni contenga cláusula derogatoria alguna en relación a la LO 15/1999 en aquellos aspectos en los que se mantenía vigente según la Disposición Transitoria Cuarta de la LO 3/2018, y que no eran otros que los que ahora regula este Anteproyecto.

d) La función de autoridad de protección de datos de la AEPD respecto del Ministerio Fiscal ha de quedar restringida al tratamiento de datos con fines no jurisdiccionales, no pudiendo extenderse a los tratamientos de datos con fines jurisdiccionales y ello no solo por la necesidad de salvaguardar la independencia del Ministerio Fiscal respecto de actuaciones jurisdiccionales y



de aquellas derivadas de su intervención en los procesos judiciales, sino también para evitar que, indirectamente y a través del Ministerio Público, por la AEPD se lleve a cabo una supervisión de los órganos judiciales competentes ya que, como antes se ha apuntado, en la actualidad existen aplicaciones integradas que no solo dan soporte a la gestión procesal efectuada por el Ministerio Fiscal sino que conectan o contienen los expedientes judiciales en sí mismos.

Por otro lado, y como ya se ha dicho, el derecho a la protección de datos (art. 18.4 CE) no es un derecho absoluto pudiendo entrar en conflicto con otros derechos fundamentales que se proyectan en el proceso judicial, entre los que se encuentran el derecho a la tutela judicial efectiva y el adecuado ejercicio del derecho de defensa (art. 24 CE) debiendo tenerse en cuenta que si la AEPD tiene encomendada la supervisión del derecho de protección de datos personales es el Ministerio Fiscal, en el ámbito jurisdiccional, el garante tanto de ese como de otros derechos fundamentales (art. 124 CE, 1 y 3.3 EOMF) los cuales no se deben ver comprometidos en el ejercicio de las facultades de inspección encomendadas a una entidad administrativa cuando, además, en el curso de la misma, se podría llegar a conocer no solo los datos personales objeto de protección sino también la naturaleza del conflicto que se dirime.

En este aspecto, el Anteproyecto, al igual que ha sucedido en otros países de nuestro entorno, ha de trasponer correctamente la normativa europea garantizando la separación de poderes y la independencia en el ejercicio de funciones jurisdiccionales, en este caso del Ministerio Fiscal, por lo que la supervisión de los tratamientos de datos de esa naturaleza deberá ser realizada, en su caso, por organismos específicos establecidos dentro del sistema judicial del estado miembro y no por entidades de control vinculadas al poder ejecutivo (aunque de ellas se predique su independencia).



Es de lamentar que se desaproveche de nuevo (ya que tampoco se contempló en la LO 3/2018) la oportunidad para incluir en el EOMF la creación de un “organismo específico de protección de datos” que, por las mismas razones que lo requiere el Poder Judicial, resulta imprescindible que se encuentre incardinado, con garantías de independencia, dentro del organigrama del Ministerio Fiscal.

Ese “organismo específico” no tiene necesariamente que reunir las condiciones que se exigen (en los artículos 41 y ss. de la Directiva 51 y ss. del RGPD) para la constitución y configuración de las autoridades de control, no solo porque no se exige expresamente que así sea sino porque la actual regulación de la LOPJ y de la LO 3/2018 no impone esas condiciones al CGPJ, único “organismo específico” actualmente existente.

En base a lo expuesto, se propone que se añada en el art. 41 del Anteproyecto un cuarto apartado:

*“4º. Las competencias y facultades que la presente ley atribuye a la Agencia de Protección de Datos serán ejercidas, respectivamente, por el Consejo General del Poder Judicial y por la Unidad de Protección de Datos del Ministerio Fiscal, en relación al tratamiento de datos personales con fines jurisdiccionales, al ejercicio de los derechos de los interesados en los tratamientos realizados con esa finalidad y al régimen sancionador en ese ámbito.*

*La Agencia Española de Protección de Datos y los mencionados organismos colaborarán en aras del adecuado ejercicio de las respectivas competencias que les atribuye la normativa de protección de datos personales, la Ley Orgánica del Poder Judicial y el Estatuto Orgánico del Ministerio Fiscal”.*

Como consecuencia de lo anterior, de igual modo se propone se añadan al Anteproyecto dos nuevas disposiciones finales.



*La primera con el siguiente contenido:*

*“Modificación de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal.*

*Se modifica el art. 12 para incluir en nuevo apartado n):*

*n) La Unidad de Protección de Datos.*

*Se modifica el art. 20 y se incluye un nuevo apartado 4 con la siguiente redacción:*

*4. En la Fiscalía General del Estado, de igual modo, existirá la Unidad de Protección de Datos que, respecto del tratamiento de datos con fines jurisdiccionales realizado por el Ministerio Fiscal, del ejercicio de los derechos de los interesados en el tratamiento realizado con esa finalidad y del régimen sancionador en ese ámbito, ejercerá con autonomía las competencias y facultades que por la normativa de protección de datos se atribuya a la Agencia Española de Protección de Datos.”*

*La segunda con el siguiente contenido:*

*“Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

*Se incluye un nuevo apartado 5 en el artículo 1 con la siguiente redacción:*

*5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial y de las normas procesales que le sean aplicables.*

*Se modifica el apartado 3 del artículo 44 que pasará a tener la siguiente redacción:*



*3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y la Unidad de Protección de Datos del Ministerio Fiscal colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial y la Ley 50/1981, de 30 de diciembre reguladora del Estatuto Orgánico del Ministerio Fiscal les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.”*

#### **Artículo 54**

El artículo 54 respecto a la prescripción de las infracciones, establece que 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.

Igualmente, y para el caso de la prescripción de las sanciones el plazo de prescripción será de un año, dos años o tres años, según sean leves, graves o muy graves.

Como quiera que la Directiva no contempla un plazo de prescripción de las infracciones y dicho plazo debe fijarse por razones de seguridad jurídica, debe ser el legislador español el competente para su fijación, estableciéndose los criterios en el artículo 30.1 de la LRJSP, que dice que *“las sanciones prescribirán según lo dispuesto en las leyes que las establezcan. Si éstas no fijan plazos de prescripción, las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año”*

Finalmente, y en cuanto al cómputo del plazo de prescripción de las sanciones, la normativa es una reproducción de lo establecido en el artículo 30.3 de la LRJSP.



## Disposiciones finales

### Primera

La disposición final primera establece el carácter de ley ordinaria de los Capítulos VI (autoridades de protección de datos), VII (reclamaciones) y VIII (régimen sancionador).

Salvo los comentarios ya efectuados en el apartado IV, entendemos que se procede de igual modo que en la LOPDGD, en la que se estableció el carácter ordinario de los Capítulos VII (autoridades de protección de datos), VIII (procedimientos en materia de vulneración de datos) y IX (régimen sancionador).

### Segunda

La disposición final segunda establece que el título competencial la ley orgánica se dicta al amparo de la competencia exclusiva del Estado en el artículo 149 1º, 6º y 29º de la Constitución Española, que atribuye al Estado la competencia exclusiva en la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales y en materia de seguridad pública y la competencia exclusiva del Estado en relación con la legislación procesal.

Así, la STC 104/1989, de 8 de junio, dice que *“dicho concepto material, la seguridad pública, entendido como actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano, según pusimos de relieve en las SSTC 33/1982, 117/1984, 123/1984 y 59/1985, engloba, como se deduce de estos pronunciamientos, un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido”*.



### Tercera

La disposición final tercera introduce el apartado tercero del art. 236 octies de la Ley Orgánica 6/1985, de 1 de julio del Poder Judicial, que quedaría redactado de la siguiente manera:

*“Contra la denegación de las solicitudes de ejercicio de los derechos de acceso, rectificación, limitación y supresión en relación con los datos tratados con fines jurisdiccionales se podrá interponer directamente recurso contencioso-administrativo ante el órgano jurisdiccional competente de acuerdo con lo previsto en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa”.*

Respecto de la misma se han de realizar las siguientes consideraciones:

Dicha previsión, tal como se encuentra redactada, podría resultar de aplicación al Ministerio Fiscal ya que este realiza tratamientos de naturaleza jurisdiccional. Sin embargo, a la vista del antes analizado art. 19 del Anteproyecto, también cabría interpretarse que lo que el prelegislador pretende es dar un tratamiento diferenciado a las resoluciones dictadas por los órganos judiciales en denegación de solicitudes de ejercicio de derechos, limitando a ellas el recurso contencioso administrativo directo por lo que, de ser esta la interpretación, el Ministerio Fiscal quedaría excluido de ese “trato privilegiado”.

Esta Disposición Final provocará, innecesariamente, conflictos de competencia entre distintos órganos judiciales ya que el cauce para el ejercicio de los derechos, según el art. 236 octies de la LOPJ, se realiza conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados (en este caso de naturaleza penal), en cambio, se pretende que las resoluciones que resuelvan sobre esas solicitudes sean objeto de recurso por vía contencioso-administrativa.



#### **Cuarta**

La previsión contenida en la mencionada Disposición Final abre un cauce paralelo para que los órganos judiciales puedan “eludir” el procedimiento de tutela mediante la reclamación ante la Autoridad de control, previsto en los arts. 52.1 de la Directiva y 45 del Anteproyecto.

Por todo ello, se considera más razonable y coherente, mantener la vía de recurso por denegación de las solicitudes en base a las normas procesales en que los datos son tratados (art. 236 octies LOPJ) así como que sean el CGPJ y la Unidad de Protección de Datos del Ministerio Fiscal (cuya creación se propugna) los que asuman, respectivamente, la competencia para resolver las reclamaciones por denegación relativas el ejercicio de los derechos de los interesados en los tratamientos de datos jurisdiccionales.

En virtud de todo ello, se propone la supresión de la Disposición Adicional tercera por la que se modifica la LOPJ

#### **Novena**

La disposición final novena regula la entrada en vigor, que es al día siguiente de su publicación en el BOE, con excepción del Capítulo IV, relativo a los encargados, responsables, seguridad de los datos personales y delegado de protección de datos, cuya normativa producirá efectos a los seis meses de la entrada en vigor

### **6. CONCLUSIONES.**

**PRIMERA.** El Anteproyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la



seguridad públicas, tiene por objeto, esencialmente la incorporación al Ordenamiento español de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativo a la protección de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.*

**SEGUNDA.** El objeto del Anteproyecto, según su artículo 1.1 (y art. 1.1 de la Directiva), lo constituye la regulación del tratamiento de datos personales por parte de las autoridades competentes para los fines en ella descritos, y siendo indiscutible la condición del Ministerio Fiscal como autoridad competente y responsable del tratamiento, la efectiva plasmación legal de este Anteproyecto pudiera llegar a comprometer su autonomía funcional y el ejercicio de su misión por medio de órganos propios. Sería recomendable que, ya que la misma afecta a un derecho fundamental, y al igual que hace la Directiva, la denominación de la ley debería incidir en que la protección recae sobre las personas físicas en lo que respecta al tratamiento de sus datos personales

**TERCERA.** En la exposición de motivos del anteproyecto y respecto a la definición de autoridades competentes, debería citarse al Ministerio Fiscal, como se hace expresamente en su artículo 2 párrafo 6º, así como explicar las consecuencias jurídicas de su inclusión, de conformidad con lo establecido en el artículo 45.2 de la Directiva. Asimismo, debe utilizarse por razones de estilo a lo largo de todo el texto la palabra “*transferencia*”, e incluirse en el mismo un lenguaje inclusivo

**CUARTA.** Es necesario delimitar con claridad por el legislador el concepto y alcance de la “seguridad pública” citada en el artículo 1º en aras a la seguridad jurídica.



**QUINTA.** La regulación establecida en el artículo 2 párrafo 2º del Anteproyecto en relación con el uso de cámaras de videovigilancia no distingue cuándo el uso de las cámaras tenga como finalidad la prevención, detección e investigación de delitos, en cuyo caso debe de estar incluido en esta ley orgánica, o cuando el uso tenga una finalidad puramente administrativa sancionadora, fundamentalmente en materia de tráfico u otros aspectos puramente de vigilancia o de policía más propios de la seguridad ciudadana.

**SEXTA.** Se debe modificar el artículo 2.3 en relación al concepto de autoridad competente, y se propone que la frase *“para la consecución de los fines del artículo 1”* se sustituya por *“para el tratamiento de datos personales en base a alguno de los fines previstos en el artículo 1”*.

**SÉPTIMA.** Se debe de incluir como autoridad competente para realizar los tratamientos de datos personales referidos en el artículo 1, a la Tesorería General de la Seguridad Social de conformidad con lo establecido en el art.66 de la LGTGSS, ya que el artículo 5.1 incluye entre las Administraciones públicas que debe de proporcionar datos a las autoridades judiciales, Ministerio Fiscal y Policía Judicial a la de la seguridad social conjuntamente con la tributaria.

**OCTAVA.** El Anteproyecto, para cumplir adecuadamente con el mandato contenido en la Directiva, ante la ausencia en el ordenamiento nacional de disposiciones acordes con la actual normativa europea, debería realizar una adecuada, completa e integrada regulación de esta materia en el ámbito jurisdiccional ya que compromete no solo el ejercicio de las funciones del Ministerio Fiscal sino también a un derecho fundamental (18.4 CE), en este caso, el de la protección de datos personales de los ciudadanos, del que también es garante el Ministerio Público, ya que el régimen general que se plasma en el Anteproyecto es insuficiente



**NOVENA.** El artículo 3 del Anteproyecto se remite a las definiciones del artículo 4 del RGPD, mencionando su aplicación a los efectos de esta ley orgánica. Se entiende que dicha referencia es errónea, ya que las definiciones citadas en el artículo 4 del Anteproyecto, concuerdan con las reguladas en el artículo 3 de la Directiva 2016/680 del Parlamento y del Consejo, de 27 de abril de 2016. Es por ello por lo que debe modificarse el precepto, en el sentido de hacer constar textualmente en el párrafo final: *“tal y como se establecen en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.”*

**DÉCIMA.** El artículo 4.2 b) condiciona el tratamiento por el responsable o por otro, a los fines establecidos en el art. 1, en la medida en que el tratamiento sea necesario y proporcionado “de acuerdo con el Derecho de la Unión Europea o la legislación española”, no se entiende por qué el apartado a) del art. 4.2 no recoge esa salvedad al igual que lo hace el art. 4.2 a) de la Directiva. De no unir ese párrafo parecería como si el responsable del tratamiento no deba estar autorizado legalmente para tratar los datos, sobre todo cuando se trate un responsable distinto.

**DECIMOPRIMERA.** Se propone la modificación de la redacción del párrafo 5 del artículo 5º en el siguiente sentido: *“Con el objetivo de garantizar la actividad investigadora que se lleve a cabo por las autoridades competentes, a los fines previstos en el art. 1.1 de esta ley, las administraciones públicas y las personas físicas y jurídicas a los que el ordenamiento imponga el correspondiente deber de colaboración, en ningún caso, informarán al interesado de la efectiva transmisión de sus datos personales a las autoridades competentes ni, en su caso, de la solicitud de información efectuada por estas. En el supuesto de que los datos personales sean solicitados por la autoridad competente, la solicitud que esta efectúe atenderá a los principios recogidos en el art. 4.1 b) y c) de esta ley.”*



**DECIMOSEGUNDA.** Debe establecerse una definición del concepto de bloqueo de datos, o remitirse a la legislación aplicable a la misma para definir el ámbito material del bloqueo. Finalmente, debe constar en la normativa en relación con los datos personales recogidos en los ficheros jurisdiccionales penales de conformidad con los párrafos 5 y 6 del artículo 2, que en los tratamientos llevados a cabo por las autoridades jurisdiccionales y el Ministerio Fiscal haga referencia a los específicos plazos de conservación que respecto a los ficheros jurisdiccionales penales establecen las leyes procesales, a la vista de que son aquellas normas las que rigen el tratamiento de los datos en los órganos jurisdiccionales penales y Ministerio Fiscal.

**DECIMOTERCERA.** Las definiciones de las categorías de interesados previstas en los párrafos a, b y c del artículo 7 del Anteproyecto adolecen de falta de concreción en su definición, debiendo redefinirse en términos más rigurosos y coincidente con los de la Directiva.

**DECIMOCUARTA.** El art. 16.3.b), al hablar de la limitación -en lugar de la supresión- de los datos personales por el responsable del tratamiento, exige la concurrencia de dos circunstancias. Pues bien, las del apartado b), cuando los datos hayan de conservarse a efectos probatorios, añade la siguiente frase "o, en particular, por razones de seguridad". Esto supone una ampliación de lo dispuesto en el art. 16.3 b) de la directiva sin que se justifique las razones por las que el responsable limite el tratamiento de datos personales por razones de seguridad y no exclusivamente a efectos probatorios.

**DECIMOQUINTA.** Procede la modificación del artículo 17 añadiendo la previsión del apartado 4 del artículo 16 de la Directiva. Por último, se pone de manifiesto que existe un error en la numeración de los apartados de este precepto, por omisión de un párrafo 3º.

**DECIMOSEXTA.** Se propone la redacción del artículo 18 en el siguiente



sentido: “.1. En los casos contemplados en los artículos 15.3 y 16.1, el responsable del tratamiento informará al interesado de la posibilidad de que sus derechos sean ejercitados a través de la autoridad de protección de datos o en su caso, y en su respectivo ámbito, ante el Consejo General del Poder Judicial y la Unidad de Protección de Datos del Ministerio Fiscal. 2. Cuando, en virtud de lo establecido en el apartado anterior, sea la autoridad de protección de datos o, en su respectivo ámbito, los organismos mencionados en el apartado anterior, los que ejerciten los derechos, éstos deberán 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”.

**DECIMOSÉPTIMA.** Se propone la redacción del artículo 19, párrafo 1, en el siguiente sentido: “El ejercicio de los derechos contemplados en los artículos anteriores, en relación con el tratamiento de datos personales realizado con fines jurisdiccionales, se tramitará de conformidad con lo dispuesto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y, en su caso, conforme a las normas que resulten de aplicación al proceso, diligencias o expedientes en que esos datos figuren”.

**DECIMOCTAVA.** Se debe enmendar el artículo 20 en la referencia que hace a los supuestos previstos ya que, por error, se remite al artículo 18, cuando en realidad lo hace al artículo 19.

**DECIMONOVENA.** En el artículo 28, y al referirse a la evaluación de impacto relativa a la protección de datos, resulta más correcto hablar de “riesgos”, que de “peligros”, conforme a lo que establece el artículo 27 de la directiva. Igualmente, en el artículo 31, en cuanto a la obligación del responsable del tratamiento de notificar a la autoridad de protección de datos una violación de la seguridad de los datos personales, debe sustituirse la expresión “peligros”, por “riesgos”. Finalmente, en la letra p del artículo 52, por las razones expuestas



anteriormente, debe sustituirse “*peligro*” por “*riesgo*”.

**VIGÉSIMA.** Deben definirse o fijarse con claridad en el artículo 36 del Anteproyecto los términos a los que se refiere la Directiva, tales como “*amenaza*”, “*gravedad*” y “*nivel adecuado*”, al generar inseguridad, ya que por citar un concepto no especificado, se desconoce cómo valorar la adecuación en el supuesto de que el Estado miembro tenga un nivel superior de garantías al que la Unión considere como “*nivel adecuado*”, por lo que podría considerarse la adecuación como “*un nivel mínimo de protección*” que deberían cumplir todos los terceros países a los que se transfieren datos personales.

**VIGESIMOPRIMERA.** La Directiva establece una limitación a la autoridad de control respecto a los órganos jurisdiccionales en el ejercicio de su función judicial, ya que impone a los Estados miembros la exclusión de control de aquellos tratamientos de datos personales efectuados por órganos jurisdiccionales en el ejercicio de su función judicial, del mismo modo que lo hacen el artículo 55.3 del RGPD, o los artículos 2.4 y 44.3 de la LOPDGDD, que separan el ámbito de control de ambos, y el artículo 10.1 de la LOPDGDD que establece que solo se tratarán por la AEPD los datos penales que no gocen de la condición de los establecidos en la Directiva.

**VIGESIMOSEGUNDA.** El Ministerio Fiscal es “*autoridad judicial independiente*” de conformidad con lo establecido en el artículo 45.2 de la Directiva, y en los considerandos 20, 49 y 80 el legislador se ha inclinado, al introducir el artículo 2 apartado 6º del Anteproyecto, por disponer que las operaciones de tratamiento en ella citadas queden excluidas del control de la autoridad de control prevista en el artículo 41 del Anteproyecto. No obstante, el cumplimiento de las normas de la presente Directiva por los órganos jurisdiccionales y otras autoridades judiciales independientes debe estar siempre sujeto a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta (considerando 80).



**VIGESIMOTERCERA.** Se propone que se añada en el art. 41 del Anteproyecto un cuarto apartado: *“4º. Las competencias y facultades que la presente ley atribuye a la Agencia de Protección de Datos serán ejercidas, respectivamente, por el Consejo General del Poder Judicial y por la Unidad de Protección de Datos<sup>20</sup> del Ministerio Fiscal, en relación al tratamiento de datos personales con fines jurisdiccionales, al ejercicio de los derechos de los interesados en los tratamientos realizados con esa finalidad y al régimen sancionador en ese ámbito. La Agencia Española de Protección de Datos y los mencionados organismos colaborarán en aras del adecuado ejercicio de las respectivas competencias que les atribuye la normativa de protección de datos personales, la Ley Orgánica del Poder Judicial y el Estatuto Orgánico del Ministerio Fiscal”.*

**VIGESIMOCUARTA.** Se deben establecer en el artículo 46 del Anteproyecto unas normas más claras para delimitar la responsabilidad de responsable y encargado a los efectos de la indemnización, como las que aparecen previstas en el artículo 82 del RGPD.

**VIGESIMOQUINTA.** Como consecuencia de la redacción del apartado 4º del artículo 41 del anteproyecto, se añaden dos nuevas disposiciones finales *La primera con el siguiente contenido: “Modificación de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal.*

*Se modifica el art. 12 para incluir en nuevo apartado n):*

*n) La Unidad de Protección de Datos.*

*Se modifica el art. 20 y se incluye un nuevo apartado 4 con la siguiente redacción:*

*4. En la Fiscalía General del Estado, de igual modo, existirá la Unidad de Protección de Datos que, respecto del tratamiento de datos con fines jurisdiccionales realizado por el Ministerio Fiscal, del ejercicio de los derechos de los interesados en el tratamiento realizado con esa finalidad y del régimen sancionador en ese ámbito, ejercerá con autonomía las competencias y*



*facultades que por la normativa de protección de datos se atribuya a la Agencia Española de Protección de Datos.”*

*La segunda con el siguiente contenido: “Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

*Se incluye un nuevo apartado 5 en el artículo 1 con la siguiente redacción: 5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial y de las normas procesales que le sean aplicables.*

*Se modifica el apartado 3 del artículo 44 que pasará a tener la siguiente redacción: 3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y la Unidad de Protección de Datos del Ministerio Fiscal colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial y la Ley 50/1981, de 30 de diciembre reguladora del Estatuto Orgánico del Ministerio Fiscal les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.”*

**VIGESIMOSEXTA** Se propone la supresión de la Disposición Adicional tercera por la que se modifica la LOPJ, al considerar que más razonable y coherente, mantener la vía de recurso por denegación de las solicitudes en base a las normas procesales en que los datos son tratados (art. 236 octies LOPJ) así como que sean el CGPJ y la Unidad de Protección de Datos del Ministerio Fiscal (cuya creación se propugna) los que asuman, respectivamente, la competencia para resolver las reclamaciones por denegación relativas el



ejercicio de los derechos de los interesados en los tratamientos de datos jurisdiccionales

El Consejo Fiscal considera que la Fiscalía General del Estado a la vista del informe de memoria de análisis de impacto relativo al Proyecto de Real Decreto que concluye que no genera aumento de coste alguno en su aplicación, y es beneficioso para la profesionalización de la Administración de Justicia, debe informarse favorablemente en este aspecto.

Con la formulación de estas observaciones, el Consejo Fiscal da cumplimiento al preceptivo trámite de audiencia previsto en el Estatuto Orgánico del Ministerio Fiscal.

Madrid a 7 de mayo de 2020.



Dolores Delgado García