N/REF: 0014/2026

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

I

El anteproyecto de Ley Orgánica remitido tiene por objeto definir la arquitectura legal y los medios necesarios para reforzar la integridad pública y combatir la corrupción pública y privada en todas sus fases y dimensiones, dando cumplimiento efectivo al contenido del Plan Estatal de Lucha contra la Corrupción.

Este objetivo global puede desglosarse en cinco ejes fundamentales: Prevención de riesgos y fortalecimiento de controles; mejoras de racionalización en la gestión y aumento de transparencia en la contratación y subvenciones públicas; investigación, sanción y justicia eficaz; recuperación de activos y promoción de una cultura de integridad; y fortalecimiento institucional en la lucha contra el fraude y la corrupción, creando una agencia independiente que garantice la ejecución fiable y perdurable de las medidas normativas y reforzando las instituciones preexistentes.

El Anteproyecto se estructura en una parte expositiva y una parte dispositiva. Esta última consta de 56 artículos, agrupados 3 Libros, 2 disposiciones adicionales, 6 disposiciones transitorias, 1 disposición derogatoria y 10 disposiciones finales, con la siguiente estructura y contenido:

Título preliminar: artículos 1 a 3

Libro I, Del sistema de prevención de la corrupción

Título I, Medidas generales contra la prevención del fraude y la corrupción, artículo 4 a10

Titulo II, Medidas específicas de prevención del fraude y la corrupción, artículo 11 a 19

Título III, Innovación tecnológica para prevenir, identificar y actuar contra el fraude y la corrupción, 20 a 25

Libro II, Del fortalecimiento institucional frente a la corrupción

Título I, Agencia Independiente de Integridad Pública, 26 a 42

Título II, Gobernanza de la integridad pública en el sector público estatal, 43 a 45

Título III, Refuerzo de las capacidades del Poder Judicial y el Ministerio Fiscal y de la protección del informante, 46 a 50

Libro III, de la Restitución a la Hacienda Pública, artículos 51 a 56.

Se trata de una Ley Orgánica dictada en cumplimiento de lo previsto en el artículo 81 de la Constitución Española 1978, y al amparo de lo dispuesto en los apartados 6,13,14 y 18 del artículo 149.1 de la Constitución Española, que atribuyen al Estado, respectivamente, la competencia en materia de legislación mercantil, penal y penitenciaria; legislación procesal, sin perjuicio de las necesarias especialidades que en este orden se deriven de las particularidades del derecho sustantivo de las Comunidades Autónomas, bases y coordinación de la planificación general de la actividad económica, Hacienda general y Deuda del Estado y las bases del régimen jurídico de las Administraciones públicas y del régimen estatutario de sus funcionarios que, en todo caso, garantizarán a los administrados un tratamiento común ante ellas; el procedimiento administrativo común, sin perjuicio de las especialidades derivadas de la organización propia de las Comunidades Autónomas; legislación sobre expropiación forzosa; legislación básica sobre contratos y concesiones administrativas y el sistema de responsabilidad de todas las Administraciones públicas.

En su MAIN se indica la previsión de un impacto económico positivo en la economía española puesto que las medidas adoptadas de lucha contra la corrupción generan una mayor confianza en el mercado español y, por ende, mejora las expectativas inversoras en la economía española. Impacto presupuestario positivo para los Presupuestos de la Administración General del Estado tanto para el desempeño de las funciones en materia de localización y recuperación de bienes, como de su gestión. El impacto de la ley en relación con la competencia en el mercado español es positivo puesto que, al luchar contra la corrupción, en especial en materia contractual, se fomenta una competencia más justa y transparente en el mercado español, penalizando a quienes recurren a la corrupción y premiando a quienes cumplen las reglas, lo que beneficia la eficiencia, la innovación y la confianza en el entorno empresarial. Desde el punto de vista de los presupuestos implica un gasto. En materia de cargas administrativas, supondrá una reducción de cargas administrativas: La digitalización y simplificación de procedimientos reducirán cargas administrativas y costes operativos a medio plazo. Impacto de género nulo, impacto en la infancia y en la adolescencia neutro, impacto en la familia neutro, impacto en materia de carácter social y medioambiental, igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad neutro.

Finalmente, en relación con las medidas previstas en la presente norma, la OCDE exige a España una estrategia nacional anticorrupción, mecanismos de seguimiento y evaluación, y la publicación de informes anuales sobre el grado de cumplimiento y el impacto de las medidas. Con esta Ley se dota al Plan Estatal de Lucha Contra la Corrupción de fuerza normativa, asegurando su cumplimiento y garantizando su permanencia en el tiempo.

II

El marco normativo aplicable a los tratamientos de datos de carácter personal que puedan realizarse al amparo de la norma proyectada está constituido, con carácter general, 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 (Reglamento General de Protección de Datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

Asimismo, en cuanto a los tratamientos de datos personales que se realicen por las autoridades competentes con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, quedarán sujetos a las disposiciones de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El anteproyecto remitido incide en el derecho fundamental a la protección de datos personales de diversas maneras, el título primero de su libro II crea la Agencia Independiente de Integridad Pública, como un órgano destinado a dotar de coherencia al sistema de integridad pública, conforme a lo establecido en esta ley y a coordinar y supervisar las políticas de integridad. Con ello se da respuesta a la primera medida prevista en el Plan Estatal de Lucha Contra la Corrupción, que estableció que la nueva Agencia debía asumir "*las competencias clave en materia de prevención, supervisión y planificación en el ámbito de la lucha contra la corrupción y la integridad pública aunando las competencias de varios organismos estatales y estableciendo una coordinación a partir de un mismo eje central*". Tal y como señala la Exposición de Motivos de este APLO: "*La nueva Agencia debe tener facultades para iniciar investigaciones, supervisar el cumplimiento de normativas clave (contratación pública, lobbies, conflictos de interés, rendición de cuentas) y articular mecanismos de protección para informantes de corrupción y otras infracciones normativas. Ante estas competencias, se recoge expresamente que el tratamiento y la comunicación de datos se realizarán conforme a los principios de licitud, minimización, limitación de finalidad, exactitud, integridad y confidencialidad, establecidos en el Reglamento (UE) 2016/679 (RGPD) y en la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales".*

Centrándonos en el análisis de los preceptos de este proyecto normativo con mayor incidencia en la materia que constituye el objeto esencial de este informe, dentro del libro I en materia de prevención contra la corrupción, el artículo 21 regula el uso y compartición de datos en la prevención y lucha contra la corrupción del siguiente modo:

"*1.Los datos generados y custodiados por diferentes órganos del sector público podrán ser compartidos directamente, mediante intermediación o a través de espacios de datos, con la Agencia Independiente de Integridad Pública y con los demás sujetos responsables en materia de prevención y lucha contra el fraude y la corrupción, de acuerdo con lo previsto en leyes especiales, en ejercicio de las competencias atribuidas por el ordenamiento a cada una de las entidades.*

2. De acuerdo con lo previsto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, mediante las correspondientes normas técnicas de interoperabilidad y seguridad se establecerán los procedimientos y guías de operación precisos para la compartición de datos en espacios de datos, se definirán los estándares de gestión, seguridad y calidad del dato, la metodología de gestión de riesgos y su aplicación, las previsiones relativas a la interoperabilidad y el modo de evaluar su desempeño efectivo. En todo caso, el tratamiento y la comunicación de datos deberán realizarse conforme a los principios de licitud, minimización, limitación de finalidad, exactitud, integridad y confidencialidad, establecidos en el Reglamento (UE) 2016/679 (RGPD) y en la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales".

El artículo 25 regula la Base Nacional de Subvenciones con el siguiente tenor:

"Se llevarán a cabo las modificaciones necesarias para asegurar el carácter completo de la información incorporada en la Base de Datos Nacional de Subvenciones. Se facilitará su interconexión con cualquier otro registro oficial, así como su acceso para prevenir y detectar el conflicto de interés, el fraude y la corrupción, mediante el empleo del análisis masivo de datos e inteligencia artificial".

Por otra parte, al abordar la regulación de la Agencia Independiente de Integridad Pública el artículo 39 en materia de colaboraciones con ella dispone que:
"*La Agencia podrá auxiliarse, para el correcto cumplimiento de sus funciones, de la información que obre en cualquier fichero, archivo o registro público, estando obligados todos los organismos y entidades del sector público estatal a facilitarle cuanta información les sea solicitada, así como la información de carácter tributario, mercantil y de seguridad social, de conformidad con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en su caso, en la Ley 58/2003, de 17 de diciembre, General Tributaria, o en el texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre.. Asimismo, la Agencia podrá solicitar la información, los ficheros, archivos o registros de carácter público así como la información y los datos de las Administraciones tributarias y las entidades gestoras y servicios comunes de la Seguridad Social, que resulten necesarios para el ejercicio de sus funciones y que deberán ser proporcionados de conformidad con lo establecido*

en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en la Ley 58/2003, de 17 de diciembre, General Tributaria. Los datos de carácter tributario estarán acotados a lo previsto en el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria. De igual modo, los datos obtenidos por las entidades gestoras y los servicios comunes que integran la Administración de la Seguridad Social estarán acotados a lo establecido en el artículo 77 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre".

En esta misma línea, el artículo 45 sobre Refuerzo de la colaboración con la Agencia Independiente de Integridad Pública en su último apartado añade que:
"*El tratamiento de los datos personales se ajustará a lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) , 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales .*

No se informará al afectado de la cesión de sus datos personales, en la medida en que su comunicación podría imposibilitar u obstaculizar el objetivo del tratamiento, de conformidad con lo establecido en la letra b, del artículo 14.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE".

Finalmente, el título tercero del libro II tiene por objeto la modificación de normativa relativa al Poder Judicial, el Ministerio Fiscal, y la protección del informante, con el objetivo de reforzar sus capacidades en la lucha contra el fraude y la corrupción, incluyendo reformas sobre la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, en el sentido de reconocer a la Oficina de Recuperación y Gestión de Activos (ORGA) como autoridad competente para el tratamiento de datos personales en procesos penales, exclusivamente para acordar medidas inmediatas de preservación de bienes (artículo 49). Indicándose que esta reforma cumple con los artículos 6.2 y 6.3 de la Directiva 2024/1260, de 24 de abril, reforzando el acceso a registros oficiales y garantizando la protección de derechos fundamentales en la localización de activos susceptibles de embargo.

De este modo, atendiendo a la regulación contenida en el anteproyecto, la base jurídica del tratamiento de los datos personales, sin perjuicio de algunos supuestos en

los que se hace referencia al consentimiento de los propietarios de los datos como ocurre en la modificación del artículo 39 de la Ley de Defensa de la Competencia operada por la disposición final segunda, vendrá determinada con carácter general por lo dispuesto en las letras c) y e) del artículo 6 del RGPD:

> *c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
>
> *e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

Para estos supuestos, el RGPD contiene previsiones adicionales en los apartados 2 y 3 del propio artículo 6:

> *2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.*
>
> *3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:*
> *a) el Derecho de la Unión, o*
> *b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.*
>
> *La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.*

Complementando dichos preceptos, el artículo 8 de la LOPDGDD especifica lo siguiente:

> *Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*
>
> *1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.*
>
> *2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.*

Dichas previsiones deben ponerse en relación con la jurisprudencia del Tribunal Constitucional y del TJUE referida a la limitación del derecho fundamental a la protección de datos personales, tal y como viene señalando de manera reiterada esta Agencia.

De acuerdo con la misma, el derecho a la protección de datos personales es un derecho fundamental, cuyo contenido 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» (STC76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre). Pero, además, estas sentencias señalaron igualmente la necesidad de que la injerencia esté prevista en una ley o norma de la Unión Europea, con respeto, en todo caso, al principio de proporcionalidad.

En concreto, el Tribunal Constitucional, en la STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

> *- En segundo lugar, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas,*

STC 49/1999, de 5 de abril, FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10)."

Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (STC 49/1999, FJ 4). En otras palabras, "no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites" (STC 292/2000, FJ 15).

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

"En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de

proporcionalidad en sentido estricto; STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, F. 6).”

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

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

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

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

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

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

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

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

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

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

Como ya mencionamos más arriba en este informe, la STC 76/2019, tan reiterada, dispone:

> *Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, «no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites» (STC 292/2000, FJ 15).*

Más recientemente, la Sentencia del TJUE (Gran Sala) de 21 de junio de 2022, al pronunciarse respecto de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, recuerdo su propia doctrina en los siguientes términos:

112 Hay que tener en cuenta que los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta no son derechos absolutos, sino que deben considerarse en relación con su función en la sociedad (Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, EU:C:2017:592, apartado 136 -y jurisprudencia citada, y sentencia de 6 de octubre de 2020, Privacy International, C623/17-, EU:C:2020:790, apartado 63 y jurisprudencia citada).

113 Según la primera frase del apartado 1 del artículo 52 de la Carta, toda limitación del ejercicio de los derechos y libertades reconocidos por la Carta debe estar prevista por la ley y respetar la esencia de dichos derechos y libertades. En virtud de la segunda frase del apartado 1 del artículo 52 de la Carta, y sin perjuicio del principio de proporcionalidad, sólo pueden establecerse limitaciones a estos derechos y libertades si son necesarias y responden realmente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de proteger los derechos y libertades de los demás. A este respecto, el apartado 2 del artículo 8 de la Carta establece que los datos personales deben tratarse, entre otras cosas, "con fines determinados y sobre la base del consentimiento del interesado o en virtud de otro fundamento legítimo previsto por la ley".

114 Debe añadirse que la exigencia de que toda limitación del ejercicio de los derechos fundamentales esté prevista por la ley implica que el acto que permite la injerencia en dichos derechos debe definir por sí mismo el alcance de la limitación del ejercicio del derecho de que se trate, teniendo en cuenta, por una parte, que esta exigencia no se opone a que la limitación de que se trate se formule en términos suficientemente abiertos para poder adaptarse a los distintos supuestos y seguir el ritmo de la evolución de las circunstancias (véase, en este sentido, la sentencia de 26 de abril de 2022, Polonia/Parlamento y Consejo, C401/19-, EU:C:2022:297, apartados 64 y 74 y la jurisprudencia citada) y, por otra parte, que el Tribunal de Justicia puede, en su caso, precisar, por vía interpretativa, el alcance efectivo de la limitación a la luz del propio tenor de la normativa de la UE en cuestión, así como de su régimen general y de los objetivos que persigue, interpretados a la luz de los derechos fundamentales garantizados por la Carta.

115 Por lo que respecta a la observancia del principio de proporcionalidad, la protección del derecho fundamental al respeto de la vida privada en el ámbito de la UE exige, según reiterada jurisprudencia del Tribunal de Justicia, que las excepciones y limitaciones a la protección de datos personales sólo se apliquen en la medida estrictamente necesaria. Además, un objetivo de interés general no puede perseguirse sin tener en cuenta que debe conciliarse con los derechos fundamentales afectados por la medida, ponderando adecuadamente el objetivo de interés general con los derechos en cuestión [Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado

140, y sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C140/20-, EU:C:2022:258, apartado 52 y jurisprudencia citada].

116 Más concretamente, la cuestión de si los Estados miembros pueden justificar una limitación de los derechos garantizados en los artículos 7 y 8 de la Carta debe apreciarse midiendo la gravedad de la injerencia que tal limitación supone y verificando que la importancia del objetivo de interés general perseguido por dicha limitación es proporcional a dicha gravedad (véanse, en este sentido, las sentencias de 2 de octubre de 2018, Ministerio Fiscal, C207/16-, EU:C:2018:788, apartado 55 y la jurisprudencia citada, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C140/20, EU-:C:2022:258, apartado 53 y la jurisprudencia citada).

117 Para cumplir el requisito de proporcionalidad, la legislación en cuestión que implique la injerencia debe establecer normas claras y precisas que regulen el alcance y la aplicación de las medidas previstas e impongan unas garantías mínimas, de modo que las personas cuyos datos hayan sido transferidos dispongan de garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso. En particular, debe indicar en qué circunstancias y bajo qué condiciones puede adoptarse una medida que prevea el tratamiento de dichos datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de estas garantías es aún mayor cuando los datos personales son objeto de tratamiento automatizado. Estas consideraciones se aplican especialmente cuando los datos del PNR pueden revelar datos sensibles de los pasajeros (Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, -EU:C:2017:592, apartado 141, y sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C511/18-, C512/18 -y C520/18-, EU:C:2020:791, apartado 132 y la jurisprudencia citada).

118 Así, la legislación que prevé la conservación de datos personales debe seguir satisfaciendo criterios objetivos que establezcan una conexión entre los datos que deben conservarse y el objetivo perseguido (véanse, en este sentido, el Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 191 y la jurisprudencia citada, y las sentencias de 3 de octubre de 2019, A y otros, C70/18, EU:C-:2019:823, apartado 63, y de 6 de octubre de 2020, La Quadrature du Net y otros, C511/18-, C512/18 -y C520/18-, EU:C:2020:791, apartado 133).

III

Sentada la anterior doctrina, como hemos anticipado más arriba, con carácter general el proyecto normativo que ahora se informa incide de manera especialmente intensa en el tratamiento de datos personales en los artículos 21, 25, 39, 45 y 49.

El primero de ellos es el artículo 21, sobre uso y compartición de datos en la prevención y lucha contra la corrupción, por el que se establece que: "*Los datos generados y custodiados por diferentes órganos del sector público podrán ser compartidos directamente, mediante intermediación o a través de espacios de datos, con la Agencia Independiente de Integridad Pública y con los demás sujetos responsables en materia de prevención y lucha contra el fraude y la corrupción, de acuerdo con lo previsto en leyes especiales, en ejercicio de las competencias atribuidas por el ordenamiento a cada una de las entidades",* ligándolo en el apartado inmediatamente posterior al respeto de los principios de licitud, minimización, limitación de la finalidad, exactitud, integridad y confidencialidad previstos en el RDPD y LOPDGDD.

En relación con este precepto se advierte de la existencia de múltiples riesgos en materia de protección de datos, en primer lugar aunque se haga referencia al respeto del principio de limitación de la finalidad lo cierto es que la finalidad que se introduce es potencialmente indeterminada (prevención y lucha contra el fraude y la corrupción), lo que introduce el riesgo de posible reutilización de los datos para otras finalidades administrativas, así como el riesgo de generación de un sistema de reutilización masiva de datos administrativos.

En segundo lugar, se plantea el riesgo de vulneración del principio de minimización, porque el artículo que ahora se examina no limita las categorías de datos que se pueden compartir, con el riesgo de que se generen flujos de datos excesivos o indiscriminados entre Administraciones Públicas, o de que se facilite más información de la estrictamente necesaria para combatir el fraude.

En tercer lugar, se plantea el riesgo de falta de determinación de los sujetos intervinientes en estos tratamientos, el texto del precepto cita a la Agencia Independiente de Integridad Pública, y también a otros sujetos responsables en materia de prevención y lucha contra el fraude y la corrupción, pero sin identificar de qué entidades se trataría, es decir, sin concretar qué otras entidades podrían convertirse en receptoras de estos datos; lo que genera riesgos no solo de excesiva transferencia de datos, sino también de falta de determinación acerca de los posibles responsables del tratamiento de estos datos.

En cuarto lugar, el artículo hace referencia a un espacio de datos, lo que plantea potenciales problemas de control y gestión de los mismos, así como de control de accesos y de eventual falta de seguridad.

En quinto y sexto lugar, se plantean los riesgos que analizaremos más adelante, de falta de referencia de garantías específicas en el caso de que el tratamiento pudiera alcanzar datos sensibles, y falta de elaboración de un análisis de riesgos y de una evaluación de impacto en materia de protección de datos.

El artículo 25 regula la Base Nacional de Subvenciones con el siguiente tenor:

Se llevarán a cabo las modificaciones necesarias para asegurar el carácter completo de la información incorporada en la Base de Datos Nacional de Subvenciones. Se facilitará su interconexión con cualquier otro registro oficial, así como su acceso para

prevenir y detectar el conflicto de interés, el fraude y la corrupción, mediante el empleo del análisis masivo de datos e inteligencia artificial.

Desde el punto de vista de la protección de datos esta regulación es susceptible de generar una interconexión generalizada de los registros públicos con el riesgo inherente a tal indeterminación y generalización, con posible interconexión masiva de bases de datos administrativas sin una limitación clara, riesgo de creación de ciudadanos de cristal con perfiles completos a partir de múltiples fuentes de información administrativa, y consiguiente vulneración de principios esenciales del tratamiento de datos como minimización y limitación de la finalidad.

Asimismo, el tratamiento masivo de datos (big data) que propone esta regulación implicaría un tratamiento a gran escala de datos personales, con riesgo de reutilización de datos para finalidades distintas a la original, y potencial perfilado de personas físicas, lo que pone de manifiesto, como más adelante se indicará, la falta de regulación de garantías técnicas y organizativas adecuadas, unida a la indispensable realización de un análisis de riesgos y evaluación de impacto.

El artículo 39 regula la Colaboración con la Agencia con el siguiente tenor literal:

1. *Todas las entidades y organismos públicos, así como las entidades privadas y particulares, tendrán la obligación de cooperar con la Agencia en el ejercicio de sus funciones.*

2. *El personal funcionario de carrera que participe en las investigaciones tendrá la consideración de agentes de la autoridad y podrá recabar de las autoridades y de quienes en general ejerzan funciones públicas el debido apoyo y colaboración.*

3. *La Agencia Independiente de Integridad Pública tendrá derecho de acceso, en el ejercicio de sus funciones, a la información pertinente, incluida la contenida en bases de datos, de que dispongan las instituciones, entidades u organismos dependientes del sector público o que ejerzan funciones públicas.*

4. *Las autoridades y el personal de la Agencia deberán guardar la debida confidencialidad y secreto respecto de los asuntos que conozcan por razón de su trabajo, así como cualquier otra persona que haya accedido o recibido a través de la Agencia cualquier tipo de información relacionada con los mismos. Se garantizará la protección y reserva de los datos obtenidos en el ejercicio de sus funciones, limitando su difusión a los supuestos expresamente previstos, y la publicación de información solo podrá realizarse de forma anonimizada o agregada, cuando no afecte a la confidencialidad de las investigaciones ni a los derechos de las personas físicas o jurídicas concernidas.*

5. *Los datos, documentos o antecedentes obtenidos en el desarrollo de sus funciones solo podrán utilizarse para los fines asignados a la Agencia y, en su caso, para poner en conocimiento de los órganos competentes los hechos que*

puedan servir de fundamento para la exigencia de reintegro o ser constitutivos de infracción administrativa, responsabilidad contable o penal

6. *La Agencia podrá auxiliarse, para el correcto cumplimiento de sus funciones, de la información que obre en cualquier fichero, archivo o registro público, estando obligados todos los organismos y entidades del sector público estatal a facilitarle cuanta información les sea solicitada, así como la información de carácter tributario, mercantil y de seguridad social, de conformidad con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en su caso, en la Ley 58/2003, de 17 de diciembre, General Tributaria, o en el texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre.. Asimismo, la Agencia podrá solicitar la información, los ficheros, archivos o registros de carácter público así como la información y los datos de las Administraciones tributarias y las entidades gestoras y servicios comunes de la Seguridad Social, que resulten necesarios para el ejercicio de sus funciones y que deberán ser proporcionados de conformidad con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en la Ley 58/2003, de 17 de diciembre, General Tributaria. Los datos de carácter tributario estarán acotados a lo previsto en el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria. De igual modo, los datos obtenidos por las entidades gestoras y los servicios comunes que integran la Administración de la Seguridad Social estarán acotados a lo establecido en el artículo 77 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre.*

De nuevo, cabe advertir de los riesgos inherentes a una habilitación de acceso a datos personales tan amplia y genérica. Como venimos señalando, se aprecia falta de delimitación de las entidades públicas y privadas con las que se podrá colaborar, este precepto tampoco determina qué datos podrán solicitarse, ni en qué supuestos, ni con qué limites o garantías. Del mismo modo, tampoco se especifican qué categorías de datos podrán tratarse, ni cuales serán los criterios para determinar la pertinencia de llevar a cabo su tratamiento.

En relación con la posibilidad de acceder a datos de seguridad social o a información tributaria, aunque se remita el precepto estudiado a los límites derivados del artículo 77 LGSS o 95 LGT existen otros posibles riesgos asociados a una habilitación tan amplia, tales como los derivados de la alta sensibilidad de los datos, la concentración de excesiva información personal, y en definitiva, de la falta de exigencia de una motivación singular ligada a cada caso en concreto para plantearse permitir o no el posible acceso a estos datos personales.

A mayor abundamiento, estos preceptos tienen en común que tampoco regulan cómo se garantizará el ejercicio por parte de los ciudadanos de sus derechos de acceso, rectificación, limitación del tratamiento o de oposición por poner algunos ejemplos.

Por todo ello, sin perjuicio de que esta Agencia valore positivamente determinados aspectos de la regulación propuesta tales como la referencia al necesario respeto de

las obligaciones de confidencialidad y secreto, limitación de la finalidad en el uso de los datos, publicación anonimizada o referencia expresa a las limitaciones contenidas en la legislación especial, debe reiterarse que estas garantías no son suficientes para compensar y contrarrestar los riesgos derivados de una habilitación tan amplia al acceso a datos personales.

En este mismo orden de cosas, el artículo 45 regula el Refuerzo de la colaboración con la Agencia Independiente de Integridad Pública, del siguiente modo:

1. *Toda persona natural o jurídica, pública o privada, estará obligada a proporcionar, previo requerimiento, toda clase de datos, documentos o antecedentes con trascendencia para las actuaciones de protección de los intereses financieros de la Unión Europea.*

2. *Podrán suscribirse convenios con cualesquiera órganos o entidades públicas o privadas con la finalidad de articular los cauces y mecanismos de colaboración que resulten necesarios para el ejercicio de sus funciones en el ámbito de la prevención y lucha contra el fraude a los intereses financieros de la Unión Europea.*

3. *En las actuaciones que la Agencia realice en cumplimiento de sus obligaciones de asistencia a la Oficina Europea de Lucha contra el Fraude (OLAF), estas se entenderán realizadas por esa Oficina, sujetándose al régimen de confidencialidad y suministro de información a lo previsto en la normativa europea.*

4. *Previa suscripción del correspondiente convenio con la OLAF, la Agencia podrá asumir la realización de actuaciones de comprobación e investigación. En su desarrollo, sus funcionarios gozarán de las mismas facultades y prerrogativas que el personal de la OLAF y tendrán, asimismo, la consideración de autoridad.*

5. *El tratamiento de los datos personales se ajustará a lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) , 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales .*

   No se informará al afectado de la cesión de sus datos personales, en la medida en que su comunicación podría imposibilitar u obstaculizar el objetivo del tratamiento, de conformidad con lo establecido en la letra b, del artículo 14.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril

de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

A propósito de este precepto, tal y como se viene alertando, se observa la regulación de una obligación general de suministro de información excesivamente amplia e indeterminada que, en efecto, podría conllevar dar permiso de acceso a datos personales a terceros sin la suficiente delimitación y sin las suficientes garantías, con la consecuente vulneración de los principios esenciales en materia de protección de datos.

IV

En línea con lo expuesto, de la regulación contenida en este anteproyecto se desprenden habilitaciones de tratamientos de datos tan amplias que arrojan la hipótesis de que incluso pudieran ser objeto de tratamiento datos referidos a categorías especiales de datos personales. En esta hipótesis debe recordarse la prohibición general de tratamiento de dichos datos salvo que concurra alguna de las causas de levantamiento de la prohibición previstas en el artículo 9.2. del RGPD.

En estos casos en los que queda implicado el tratamiento de las categorías especiales de datos personales, cabe destacar la imperiosa necesidad de **recoger en la ley habilitante las correspondientes garantías es destacada por el Tribunal Constitucional en la ya citada sentencia 76/2019, en sus FJ 6 y 8:**

c) La necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles, pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad.

La exigencia de especial protección de esta categoría de datos está prevista en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (instrumento de ratificación publicado en el «Boletín Oficial del Estado» núm. 274, de 15 de noviembre de 1985), cuyo artículo 6 establece lo siguiente: «Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. […].» Esa exigencia ha sido igualmente afirmada por la Agencia Española de Protección de Datos. De acuerdo con el preámbulo de su Circular 1/2019, esas garantías adecuadas y específicas para proteger los intereses y derechos fundamentales de los afectados «adquieren una especial relevancia tanto por la importancia de los datos personales objeto de tratamiento como por tratarse

de tratamientos a gran escala de categorías especiales que entrañarán un alto riesgo para los derechos y libertades de las personas físicas difícilmente mitigable si no se toman medidas adecuadas». Asimismo, como ya se indicó en el fundamento jurídico 4 de esta sentencia, el Reglamento (UE) 2016/679 reitera la exigencia de que el legislador que regule el tratamiento de datos personales relativos a las opiniones políticas establezca dichas garantías adecuadas [artículo 9.2.g) y considerando 56].

Las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías que resulten constitucionalmente exigibles en cada caso dependerán de tres factores esencialmente: el tipo de tratamiento de datos que se pretende llevar a cabo; la naturaleza de los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo de tratamiento y a la categoría de datos de que se trate. Así, no plantean los mismos problemas una recogida de datos con fines estadísticos que una recogida de datos con un fin concreto. Tampoco supone el mismo grado de injerencia la recopilación y el procesamiento de datos anónimos que la recopilación y el procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la salud, la vida sexual o la orientación sexual de una persona física, que el tratamiento de otro tipo de datos.

El nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales. (FJ.6)

[…]

(iv) Por último, debemos recordar que el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí.

> *El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que el Derecho del Estado miembro establezca «medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado» [artículo 9.2.g) RGPD] y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas, no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.* (FJ.8)

Con el fin de dar adecuado cumplimiento a la normativa y jurisprudencia citada, esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos tienen como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa, o cuando el mismo implique el tratamiento de categorías especiales de datos personales, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma (ley, real decreto etc.) quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto “Otros impactos”, el análisis del “impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma”.

> *g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma*

Dicha EIPD no se ha llevado a cabo por el órgano proponente de la disposición general, sin que tampoco la MAIN contenga previsión alguna respecto del tratamiento de los datos de carácter personal, si bien en el texto de la norma sí que se han incluido previsiones específicas, tal y como se ha indicado en la referencia a varios de sus preceptos. Su realización permitiría que los responsables o encargados del tratamiento no tuvieran la obligación de realizar dicha evaluación de impacto de datos personales (EIPD) prescrita en el art. 35 RGPD (y que el Real Decreto del ENS ha considerado asimismo obligatoria) precisamente por haberse llevado ya a cabo en el seno del proceso de gestación de la norma de carácter general.

Esta Agencia recuerda, asimismo, que el citado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta "los riesgos que se derivan del tratamiento de los datos personales" (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

En definitiva, esta AEPD recomienda que, con la participación del delegado de protección de datos (DPD), se lleven a cabo y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el Anteproyecto de ley establece (ver art. 35 RGPD).

Corresponde, cabe recordar, al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, y que ello habrá de hacerlo "desde el diseño" del tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento, y ello aconsejaría que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el análisis de riesgos, se incorporen a la propia norma.

Por todo ello, sin perjuicio de que el texto remitido haya tenido en cuenta la protección del derecho a la protección de los datos personales incluyendo distintas remisiones a la normativa vigente en esta materia, **una adecuada regulación conforme a la normativa de protección de datos personales requeriría la realización, con intervención de los DPD de los ministerios proponentes, de**

dichos análisis, con el fin de incorporar las garantías adecuadas, previa identificación de los correspondientes tratamientos de datos que se pretenden realizar, así como la tipología de los datos personales que pueden ser tratados, incluidos en su caso los correspondientes a las categorías especiales de datos del artículo 9 del RGPD o datos referidos a condenas e infracciones penales del artículo 10 del RGPD (a los que también se refiere el artículo 10 de la LOPDGDD), cuyo tratamiento requeriría que la norma legal habilitante estuviera dotada de las correspondientes garantías que emanan de la jurisprudencia del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea anteriormente indicadas.

V

Los tratamientos de datos personales sujetos al RGPD, además de la necesaria licitud a la que ya se ha hecho referencia, deben cumplir con todos los principios de protección de datos personales contenidos en el artículo 5 del RGPD:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

El texto remitido ha incluido previsiones específicas que inciden en el tratamiento de los datos personales, por poner algunos ejemplos al regular en el artículo 21 el uso y compartición de datos en la prevención y lucha contra la corrupción, artículo 25 en materia de Base de Datos Nacional de Subvenciones, o al regular en el artículo 39 y 45 la colaboración con la Agencia Independiente de Integridad Pública.

Atendiendo a lo señalado, esta Agencia valora positivamente la inclusión en dichas previsiones de la delimitación de los fines para los que podrán usarse los datos obtenidos prevista por ejemplo en el artículo 39.5. Sin embargo, como se ha indicado en el considerando primero de este informe, dada la amplitud de las habilitaciones contempladas en este proyecto normativo, tales como la prevista en el artículo 45.5 sobre refuerzo del deber de colaboración con la Agencia, disponiendo que: "*No se informará al afectado de la cesión de sus datos personales, en la medida en que su comunicación podría imposibilitar u obstaculizar el objetivo del tratamiento, de conformidad con lo establecido en la letra b, del artículo 14.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE",* se reitera la advertencia de que esta regulación debería revisarse o completarse con el fin de cumplir adecuadamente con la garantía del derecho fundamental a la protección de datos personales, **lo que requeriría la realización del análisis de riesgos y de la evaluación de impacto a los que ya nos hemos referido.**

Asimismo, la habilitación contenida en el ut supra transcrito artículo 45 parece convertir en regla general lo que el artículo 14 RGPD contempla como un supuesto excepcional, con el compromiso que esto pudiera representar para el principio de transparencia. La excepción del artículo 14 requeriría para ser aplicable que se cumplieran los principios de necesidad, proporcionalidad y limitación de la finalidad perseguida, sin embargo, al no establecerse límites claros en el precepto ahora discutido sino habilitarse su uso generalizado siempre que *su comunicación pudiera imposibilitar u obstaculizar el objetivo del tratamiento,* sin especificar en qué supuestos en concreto podría aplicarse, ni durante cuanto tiempo podría mantenerse la falta de información, existe, como decimos, un riesgo de vulneración de los principios esenciales en materia de protección de datos.

VI

Para concluir, respecto de las modificaciones que introduce la norma proyectada en la Ley Orgánica 7/2021, de 26 de mayo, sin perjuicio de las observaciones contenidas en este informe, se hace notar que en la medida en la que pudieran referirse a tratamientos de datos personales con fines jurisdiccionales, los mismos excederían de las competencias de esta Agencia correspondiendo la competencia para informar el texto remitido, en cuanto autoridad de control, al Consejo General del Poder Judicial y, en su caso, a la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado.

Dicho lo cual, el artículo 56 sobre Modificación del Real Decreto 948/2015, de 23 de octubre, por el que se regula la Oficina de Recuperación y Gestión de Activos, introduce la modificación de los apartados 1 y 3, y la inclusión de los apartados 3 y 5, en el artículo 12 de dicha norma reglamentaria, proponiendo la siguiente redacción para el apartado 3: *La Oficina de Recuperación y Gestión de Activos podrá intercambiar información con los organismos de terceros Estados que tengan entre sus competencias la localización, el seguimiento, identificación, recuperación y gestión de activos, cuando resulte conveniente, en el ejercicio de sus funciones, dentro del marco jurídico internacional y con sujeción la normativa aplicable vigente en materia de protección de datos.*

Como acabamos de señalar esta actividad de recuperación de activos suele estar vinculada a las investigaciones penales lo que aconseja su revisión por las autoridades competentes para el tratamiento de datos con fines jurisdiccionales previstas en la LO 7/2021, de 26 de mayo.

Uno de los principales riesgos que pudiera llevar aparejada esta regulación es la previsión de la posibilidad de intercambiar información con organismos de terceros estados, lo que de acuerdo con la normativa contenida en los artículos 44 y siguientes del RGPD requeriría, entre otras garantías, la existencia de una decisión de adecuación, garantías adecuadas y/o instrumentos jurídicos específicos de cooperación. Asimismo, se aprecia indeterminación en los destinatarios de los datos al no identificarse qué autoridades concretas podrán recibir los datos, lo que introduce un problema de inseguridad jurídica y de falta de control sobre los tratamientos. Finalmente, la previsión de ser posible el intercambio "*cuando resulte conveniente en el ejercicio de sus funciones*" constituye un criterio excesivamente amplio con posible vulneración de los principios de minimización y limitación de la finalidad.