

0004/2025

I

El APL tiene por objeto la transposición de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

Los objetivos que se persiguen con su aprobación son:

- Crear una Autoridad Nacional Competente única en materia de ciberseguridad.
- Definir un criterio uniforme para determinar las entidades que están incluidas en el ámbito de aplicación clasificadas en entidades esenciales y entidades importantes.
- Establecer un catálogo de medidas necesarias para la gestión de riesgos de ciberseguridad.
- Reforzar el procedimiento de notificación de incidentes que perturben o puedan perturbar la prestación de los servicios de entidades esenciales e importantes.
- Crear la figura del responsable de seguridad de la información.
- Reforzar las normas relativas al intercambio de información sobre ciberseguridad.
- Establecer un marco institucional y de coordinación entre las autoridades competentes.

Y su estructura se concreta en una exposición de motivos, cincuenta artículos distribuidos en siete capítulos, ocho disposiciones adicionales, tres disposiciones transitorias y cinco disposiciones finales.

## II

Como punto de partida debemos acudir a las definiciones del RGPD que contiene en su artículo 4, y en concreto aquellas referidas a dato de carácter personal y a tratamiento de datos personales.

Así el apartado 1 se refiera a: *«datos personales» como toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

Mientras en el apartado 2 se refiere a *«tratamiento» 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;*

Pues bien, se observa que durante buena parte del articulado del APL sometido a informe se van a producir tratamientos de datos de carácter personal, como más adelante se analiza pormenorizadamente, por lo que en lo que a la materia de protección de datos personales se refiere, la norma a la que debe ajustarse el APL sometido a consulta es, en primer lugar, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (RGPD en lo sucesivo) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo).

En segundo lugar, y dadas las distintas finalidades que se recogen en la norma, también resultará de aplicación, en determinados tratamientos, 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.

### III

Para que un tratamiento de datos personales se considera conforme a la normativa de protección de datos (RGPD, LOPDGDD, sin perjuicio del análisis de la LO 7/2021 de 26 de mayo, que se hará con posterioridad) han de cumplirse como punto de partida los principios de protección de datos, que con carácter general se encuentran en el artículo 5 del RGPD a cuyo tenor:

*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»).*

En cuanto al principio de licitud, debe acudirse a lo indicado en el artículo 6 del RGPD y en concreto a lo dispuesto en el apartado 1 letras c) y e) a cuyo tenor:  
*1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

*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;*

El Considerando 45 del RGPD señala que “Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.”

Por su parte la LOPDGDD establece en su artículo 8 bajo la denominación Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos” dispone lo siguiente:

*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.”*

Llegados a este punto es preciso identificar al responsable del tratamiento para determinar la aplicación de la base jurídica prevista en la letra c) o la prevista en la letra e) del artículo 6.1 RGPD o ambas, es decir, procede analizar desde la perspectiva del responsable, si actúa al amparo de una obligación legal o si el tratamiento de datos es consecuencia del ejercicio de potestades públicas derivados de una competencia atribuida mediante ley.

El artículo 4.7 del RGPD considera «responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;*

En el APL se establecen distintos sujetos que pueden ser considerados responsables del tratamiento, en función de las competencias, funciones y en concreto de los tratamientos que recoge la norma sometida a informe.

Así, un primer conjunto de actores que pueden denominarse como “autoridades” y que serían, el Centro Nacional de Ciberseguridad (artículo 6) las autoridades competentes, autoridades de control (artículo 7), autoridades de gestión de crisis de ciberseguridad y aquellos equipos de respuesta a incidentes de seguridad informática también denominados CSIRT (artículo 9) y por otro lado, un segundo grupo de actores que se pueden identificar como “obligados” y que van desde proveedores de distintos servicios (de DNS, de nombres de dominio de primer nivel, de redes sociales, de servicios seguridad gestionados) pasando por entidades que prestan servicios de registros (de nombre de dominio) entidades u operadores con incidencia en Defensa Nacional, así como las denominadas entidades esenciales e importantes (que son un elemento esencial en esta regulación).

Pues bien, la base jurídica del tratamiento que realicen las distintas “autoridades” que identifica la norma, como la prevista en el artículo 6.1 e) del RGPD y el artículo 8.2 de la LOPDGD, es decir, *el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable*, y la norma con rango legal que se exige será precisamente la ley que finalmente se apruebe a partir del presente APL.

Son ejemplos de estos tratamientos que contienen datos personales, lo que se citan a continuación:

La elaboración por parte del Centro Nacional de Ciberseguridad de la lista de entidades esenciales e importantes (artículo 4.3), el intercambio de información por parte de los CSIRT nacionales de referencia, que incluye protocolo TLP y datos personales (artículo 9.6), la divulgación coordinada de las vulnerabilidades por parte de los CSIRT (artículo 11), entre otros.

Todo ello sin perjuicio de que, en algunos casos, incluso las denominadas autoridades, estén sometidas al cumplimiento de una obligación de carácter legal que también se deriva del propio APL, como por ejemplo la elaboración y mantenimiento del Registro de proveedores de servicios e infraestructuras digitales que corresponde al Centro Nacional de Seguridad (artículo 26) y que se nutre de la información que le proporcionen los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, o la comunicación de la información de dicho registro a la ENISA.

Por otra parte, en cuanto a aquellos tratamientos que se darían por parte de los “obligados por la norma” y que se encontrarían legitimados en el artículo 6.1 c) del RGPD y el artículo 8.1 de la LOPDGDD, es decir *aquellos fundados en una obligación legal exigible al responsable*, serán en esencia todos los que se deriven de la gestión de los incidentes de seguridad de acuerdo con el artículo 17, aquellos tratamientos que se deriven de las obligaciones de notificación tal como prevé el artículo 18, y que se realizarán, preferentemente a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes como dispone el artículo 19.

Asimismo, tendrían cabida en este tipo de tratamientos todas aquellas obligaciones de información y colaboración que se realicen al amparo del artículo 23, así como la información que deben proporcionar al Centro de Seguridad Nacional, para la elaboración del registro al que hace referencia el artículo 26.

A lo que hay que añadir la creación de la base de datos del registro de nombres de dominio prevista en el artículo 27, que se instituye en una obligación de las entidades que prestan servicio de registros de dominio.

#### IV

Especial atención merece el artículo 25 del APL que, bajo la rúbrica “Autorización para la cesión de datos personales”, recuerda la vigencia de los principios de minimización y limitación de la finalidad en el tratamiento de datos personales al indicar que:

*Si para realizar notificación de incidentes o su gestión, análisis o resolución es necesario comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas*

Para a continuación concretar las cesiones de datos personales que únicamente autoriza el propio APL y que se concreta en los siguientes:

*a) De las entidades esenciales e importantes a los CSIRT nacionales de referencia o a las autoridades de control.*

*b) Entre los CSIRT nacionales de referencia y las autoridades de control.*

*c) Entre los CSIRT nacionales de referencia y los CSIRT designados en otros Estados miembros de la Unión Europea.*

*d) Entre los CSIRT nacionales de referencia y otros CSIRT nacionales o internacionales.*

*e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea*

Se valora positivamente esta indicación por cuanto, al incluir una listado de supuestos en las que la cesión se puede llevar a cabo, supone una garantía legal de acuerdo con la reserva de ley que se extrae del artículo 8 de la LOPDGDD cuando aborda el tratamiento basado en el artículo 6.1 c) y e) del RGPD y en consonancia con la doctrina del Tribunal Constitucional en este aspecto (STC 292/2000 y STC 76/2019).

V

Por su parte, los artículos 26 y 27 se sitúan en el Capítulo IV denominado “Registros de entidades de naturaleza transfronteriza” y suponen la creación de distintas bases de datos que contienen datos de carácter personal.

La primera se refiera al Registro de proveedores de servicios e infraestructuras digitales cuyo responsable es el Centro Nacional de Ciberseguridad y que supone la obligación de diversos actores, de proporcionar información



susceptible de contener datos de carácter personal para configurar el citado registro. Así como la obligación del propio Centro Nacional de Ciberseguridad de proporcionar la información contenida en el registro a la ENISA (Agencia de la UE para la Ciberseguridad).

Dicha regulación se considera conforme a la base jurídica que legitima dicho tratamiento y en consecuencia no se hace indicación alguna al respecto.

La segunda se refiere a la Base de datos sobre el registro de nombres de dominio, cuyos responsables serán los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio, con la finalidad de contener la información necesaria para poder identificar y contactar con los titulares de los nombres de dominio y las entidades que administran los nombres de dominio en los dominios de primer nivel.

Continúa el precepto indicando qué la información de la base de datos del registro incluye los siguientes elementos:

- a) El nombre del dominio.*
- b) La fecha de registro.*
- c) El nombre del solicitante, su dirección de correo electrónico de contacto y su número de teléfono.*
- d) La dirección de correo electrónico de contacto y el número de teléfono del punto de contacto que administra el nombre de dominio en caso de que no sean los del solicitante.*

Y a continuación establece que *se harán públicos, sin demora indebida, después del registro de un nombre de dominio, aquellos datos del registro que no sean de carácter personal.*

Se valora positivamente la intención del prelegislador que se extrae del artículo citado, pero al no especificarse ni la finalidad de dicha publicidad, ni el contexto o soporte de la misma, es decir, si es a través de una página web o de cualquier otra plataforma, adolece de inconcreción y ambigüedad que no justifica el tratamiento de datos que supondría que esa información se haga pública.



Asimismo, conviene recordar llegados a este punto la amplitud del concepto de dato de carácter personal y la interpretación (extensiva) que del mismo hace la jurisprudencia nacional e internacional, por cuanto atendiendo al contenido de la información que recoge el artículo parcialmente transcrito, puede considerarse dato de carácter personal, en determinadas circunstancias, la totalidad de la información que en el se contiene (salvo la fecha de registro y no en cualquier contexto).

Es decir supone un sinsentido indicar que la información se hará pública salvo que contenga datos personales, por cuanto si no la totalidad, la mayoría de la información que recoge el precepto puede tener dicha consideración.

Por tanto, en relación a lo indicado se sugiere la eliminación del primer párrafo del apartado 4 del artículo 27.

Continúa el citado apartado 4 indicando que:

*concederán acceso a datos específicos sobre el registro de nombres de dominio a los solicitantes de acceso legítimos, de conformidad la normativa en materia de protección de datos de carácter personal, previa solicitud lícita y debidamente justificada. La solicitud de acceso deberá resolverse sin demora indebida y, en cualquier caso, en un plazo de setenta y dos horas desde su recepción. Las políticas y los procedimientos de divulgación de dichos datos serán públicos.*

De la lectura del precepto se infiere que se está regulando una suerte del derecho de acceso que podría contravenir la normativa de protección de datos personales.

En efecto, sobre la premisa de que la base de datos contiene datos de carácter personal, se estaría limitando sin justificación alguna el ejercicio del derecho de acceso previsto en el artículo 15 del RGPD y 13 de la LOPDGDD, así como el artículo 12 del RGPD, que establece disposiciones comunes al respecto.

Si bien el apartado 5 del artículo 12 de la LOPDGDD establece que: *5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.*, lo cierto es que el APL remite a “la normativa en materia de protección de datos”, por lo que no podemos considerar que estemos ante un régimen especial y que se aplique por tanto este apartado.

Dicho esto, ni el RGPD ni la LOPDGDD se requiere que la solicitud “*sea lícita y debidamente justificada*”, por lo que supone una restricción, al menos formal del régimen de derechos tal como se regula en el marco jurídico básico, que no requiere justificación ni formalidad alguna, más allá de estar debidamente identificados y en caso de multitud de datos, una concreción respecto a los que se pretende acceder. (artículo 13.1 segundo párrafo LOPDGDD)

En consecuencia, se informa desfavorablemente la redacción de dicho segundo párrafo del apartado 4.

Cuestión distinta es que el precepto se refiera a solicitudes de acceso a la base de datos, de personas distintas a los titulares de los nombres de dominios, y por tanto terceros ajenos a los datos personales.

En ese hipotético caso, no estaríamos ante el ejercicio del derecho de acceso y la referencia a “*de conformidad con la normativa de protección de datos de carácter personal*” podría tener razón de ser en el sentido de que dicho tratamiento, dicho acceso, tenga una base jurídica que lo legitime, además de cumplir con los restantes principios (en especial limitación de la finalidad, minimización y confidencialidad), que a priori, y dada la ambigua redacción del precepto no se puede establecer con total certeza.

Por lo tanto, aun admitiendo hipotéticamente que estemos ante el acceso de terceros definido en el párrafo anterior, también se informa desfavorablemente la redacción del apartado 4, por las razones expuestas, pues se desconoce porqué se haría el acceso (principio de licitud), para qué o con qué finalidad se hace el acceso (principio de limitación de la finalidad) , sobre qué datos (principio de minimización) y quiénes serían los destinatarios y que salvaguardas se deberían tomar (principio de confidencialidad).

## VI

La Disposición adicional quinta del APL, se refiere a la “*Base de datos de incidencias de seguridad que revistan carácter de delito*” y que dada la finalidad de los tratamientos que en ella se dan según su apartado 2: *La finalidad que persigue el tratamiento es la utilización de los datos obtenidos en la gestión, seguimiento y resolución de incidentes de ciberseguridad que afecten a entidades esenciales o importantes, cuando puedan entenderse presuntamente delictivos*, se sitúa bajo la aplicación de la LO 7/2021 de 26 de mayo.

La disposición regula qué tipo de datos se tratan en su apartado 2 y los destinatarios de dicha información en su apartado 4, así como la identificación del órgano responsable del tratamiento de dicha base de datos, la Dirección General de Coordinación y Estudios, de la Secretaría de Estado de Seguridad, en su apartado 1.

Asimismo se identifica la base jurídica de este tipo de tratamientos en los artículos 11 y 13 de la LO 7/2021, de 26 de mayo, en el apartado 5 a cuyo tenor:

*La base jurídica principal del tratamiento de acuerdo con el objetivo y finalidad de la presente ley es el cumplimiento de acuerdo con lo dispuesto en el artículo 11 y 13 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, sin perjuicio de la aplicación a su tratamiento de la legislación reguladora del ejercicio de la potestad jurisdiccional o las que en su caso resultaren de aplicación.*

Procede por tanto acudir a dichos preceptos para analizar su adecuación.

Dispone el artículo 11 bajo la rúbrica “*Licitud del tratamiento*” lo siguiente:

- 1. El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones.*
- 2. Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.*

Por lo tanto, la regulación de la Disposición adicional quinta analizada resultaría conforme al principio de licitud, con la salvedad que se hace a continuación respecto de los datos a tratar y la aplicación el artículo 13.

En efecto, debe hacerse una mención al apartado 2 de la citada Disposición que recoge los datos que se tratan, a cuyo tenor:

*Se podrán tratar, al menos, los datos relativos a la identidad de las personas, datos identificativos de terminales y dispositivos de conectividad y los datos personales de identidad y contacto de los responsables, gestores y usuarios del fichero del tratamiento.*

La inclusión del término, “al menos” dota a la redacción de inconcreción y ambigüedad por cuanto al utilizar dicha expresión, se está admitiendo la posibilidad de incluir más datos de los que ahí constan, lo que contraviene los requisitos del artículo 11.2 que la propia disposición adicional quinta señala como base jurídica para el tratamiento de los datos en esta base de datos.

Es decir, para considerar válida esa base jurídica habría que cumplir precisamente el artículo 11, que requiere que se identifiquen los datos a tratar, algo que no puede considerarse que sucede al utilizar dicha expresión.

Por tanto, se sugiere que se elimine el término indicado “al menos” para adecuarse plenamente al artículo 11.2 LO 7/2021, que requiere que se identifiquen “los datos que van a ser objeto del mismo”, pues de otro modo se desconoce qué información contendría dicha base de datos.

Por su parte, el artículo 13 de la ley se refiere a “Tratamiento de categorías especiales de datos personales.”, cuya redacción es la siguiente:

*1. El tratamiento de 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, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:*

*a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.*

*b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.*

*c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.*

*2. Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.*

*3. Los datos de los menores de edad y de las personas con capacidad modificada judicialmente o que estén incursas en procesos de dicha naturaleza, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.*

Atendiendo a los datos personales que se han determinado que van a ser objeto de tratamiento en esta base de datos (y sin perjuicio de la propuesta de eliminación del término “al menos” en la redacción analizada ut supra), no parece que se vayan a someter a tratamiento categorías especiales de datos.

El artículo 13 prevé que como presupuesto para este tipo de tratamientos que la norma establezca el mismo, y de la lectura del APL no se puede concluir esa afirmación.

No puede entenderse cumplido el requisito del artículo 13.1 a) LO 7/2021, simplemente porque la ley cite que se cumple dicho artículo 13 o, como ocurre en el presente caso, porque indique que ese precepto es la base jurídica principal, como hace la redacción del apartado 5 de la disposición adicional quinta analizada.

En efecto, para que se cumpliera dicho requisito ha de ser la propia APL la que prevea el tratamiento de las categorías especiales de datos, algo que no se extrae ni directa ni indirectamente del apartado 2 de la citada disposición al que se hace la oportuna remisión.

En consecuencia, se informa desfavorablemente la redacción del apartado 5, sugiriendo o bien la eliminación de la referencia del artículo 13 LO 7/2021, o bien introduciendo expresamente las categorías especiales de datos en el apartado 2.

Por su parte el apartado 7 tiene la siguiente redacción:

*7. La recolección de datos se hará conforme a la legislación vigente con especial atención al cumplimiento del deber de información previa a los interesados sobre las condiciones, derechos y obligaciones del tratamiento, así como a los posibles destinatarios en los términos previstos en la ley.*

Cabe indicar que en cuanto a la información que debe ofrecerse resulta de aplicación lo dispuesto en el artículo 21 de la LO 7/2021 a cuyo tenor:

*1. El responsable del tratamiento de los datos pondrá a disposición del interesado, al menos, la siguiente información:*

- a) La identificación del responsable del tratamiento y sus datos de contacto.*
- b) Los datos de contacto del delegado de protección de datos, en su caso.*
- c) Los fines del tratamiento a los que se destinen los datos personales.*
- d) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.*
- e) El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento.*

*2. Además de la información a la que se refiere el apartado 1, atendiendo a las circunstancias del caso concreto, el responsable del tratamiento proporcionará al interesado la siguiente información adicional para permitir el ejercicio de sus derechos:*

- a) La base jurídica del tratamiento.*
- b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.*

*c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.*

*d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.*

Puede observarse que la redacción del apartado 7 resulta insuficiente en relación con el contenido del artículo 21 ahora transcrito, asimismo de la expresión “la recolección de datos se realizara conforme a la legislación vigente” no se sabe a qué legislación vigente se refiere, si es a la normativa de protección de datos o a cualquier otra, a lo que hay que añadir que ya se ha indicado en el apartado correspondiente que la base jurídica se encuentra en la LO 7/2021, por lo que sí es a esa norma a la que se refiere la “legislación vigente” resultaría reiterativo y con la ambigüedad que ahora se pone de manifiesto. Por lo que, a fin de evitar una transcripción del mismo en el texto de la ley se propone la siguiente modificación:

**El responsable del tratamiento proporcionará al titular de los datos personales que se incorporan a la base de datos la información a la que se refiere el artículo 21 de la LO 7/2021 de 26 de mayo.**

En cuanto a los plazos de conservación, el apartado 8 indica que:

*8. De acuerdo con la finalidad del tratamiento, se conservarán los datos recogidos durante el tiempo necesario para el cumplimiento del fin para el cual fueron recogidos en virtud del artículo 8 de la Ley Orgánica 7/2021, de 26 de mayo, y en su caso por el tiempo necesario para atender a las responsabilidades derivadas de su tratamiento ante los órganos administrativos o jurisdiccionales competentes. Una vez transcurrido dicho periodo de conservación, los datos serán suprimidos de manera que se imposibilite la correlación o identificación de estos con los interesados.*

El artículo 8 de la LO 7/2021, dispone lo siguiente:

*Artículo 8. Plazos de conservación y revisión.*



- 1. El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1.*
- 2. El responsable del tratamiento deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado.*
- 3. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines del artículo 1.*

Al igual que para el anterior apartado, se propone una modificación que simplifique la redacción y que se adecue más al precepto. Asimismo, el último párrafo adolece de cierta contradicción al señalar que “*los datos serán suprimidos de manera que se imposibilite la correlación o identificación de estos con los interesados*”. Si los datos se suprimen dejan de existir o de constar en la base de datos, porque precisamente son eliminados, por lo que cualquier referencia adicional a partir de ese momento está fuera de lugar.

Además, parece que el prelegislador tiene la intención de instaurar una suerte de anonimización tras el cumplimiento de los plazos, lo que se valora positivamente.

No obstante y dada la redacción del APL en este aspecto, es preciso recordar los conceptos de anonimización y seudonimización por cuanto va a resultar esencial para determinar la aplicación de la normativa de protección de datos.

En efecto, la información seudonimizada se considera dato de carácter personal por cuanto existe la posibilidad de reversión, es decir, de reidentificación.

El artículo 4. 5 del RGPD considera la seudonimización como *el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;*

Así el Considerando 26 del RGPD establece que:

*Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos*

En definitiva los datos seudonimizados son datos de carácter personal y por tanto se les aplica el RGPD.

Por el contrario, en cuanto a datos anónimos, debe recordarse que ya en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la hoy derogada Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se encontraba una definición de dato disociado que podemos asimilar a dato anónimo, en el artículo 5:

*e) Dato disociado: aquél que no permite la identificación de un afectado o interesado*

En la actualidad, en el RGPD encontramos únicamente la noción al dato anónimo (información anónima), también en el Considerando 26 del RGPD que excluye la aplicación del mismo al indicar que:

*(...) los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con*

*una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima (...)*

Es decir la anonimización es una garantía para la protección de datos personales, pues dicha información no se considera como tal.

Incluso existen ejemplos en nuestro ordenamiento jurídico que traspasan dicha garantía imponiendo obligaciones adicionales sobre la información anonimizada, así en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público se establece en su artículo 8. f) lo siguiente:

*f) Cuando la información, aun siendo facilitada de forma disociada, contuviera elementos suficientes que pudieran permitir la identificación de los interesados en el proceso de reutilización, la prohibición de revertir el procedimiento de disociación mediante la adición de nuevos datos obtenidos de otras fuentes.*

En conclusión, el prelegislador dispone de distintas opciones a la hora de escoger qué tipo de información puede ser tratada (conservada) transcurridos los plazos correspondientes, que van desde datos seudonimizados hasta datos anonimizados, incluso puede añadir obligaciones adicionales al respecto.

En cualquier caso, esta Agencia considera al amparo de criterios de prudencia y pertinencia, la eliminación de la información una vez transcurridos los plazos que se establezcan y en su defecto la conservación pero de manera anónima.

Por tanto, se propone la siguiente modificación:

**Los datos personales se conservarán de conformidad con lo dispuesto en el artículo 8 de la LO 7/2021, de 26 de mayo. Transcurrido el plazo de conservación los datos serán suprimidos, salvo que se conserven de manera anonimizada.**

Por último, se observa que la disposición analizada recoge referencias al ejercicio de los derechos en el apartado 9 que es coherente con las limitaciones que permiten los artículos 15 y 18 de la Directiva (UE) 2016/680, en general y con el régimen de derechos que recoge la propia LO 7/2021, de 26 de mayo en el Capítulo III, en particular, lo que se informa favorablemente.

