



INFORME SOBRE EL ANTEPROYECTO DE LEY PROTECCIÓN DE DATOS PERSONALES

I

ANTECEDENTES

1. La Directora de Régimen Jurídico, Servicios y Procesos Electorales del Departamento de Seguridad del Gobierno Vasco, solicita a la Agencia Vasca de Protección de Datos informe relativo al Anteproyecto de Ley de Protección de Datos Personales.
2. Acompaña al borrador del Anteproyecto, consulta pública previa a su elaboración, comentarios a la consulta pública previa, Orden del Vicelehendakari Primero y Consejero de Seguridad, por la que se acuerda el inicio del procedimiento para la elaboración del Anteproyecto de Ley de Protección de Datos Personales, memoria explicativa, memoria económica, Orden de 31 de enero de 2022 por la que se acuerda la aprobación previa del Anteproyecto de Ley, Versión 1 del Anteproyecto, informe jurídico del Departamento de Seguridad del Gobierno Vasco, versión 2 del Anteproyecto y Resolución de la Directora de Régimen Jurídico, Servicios y Procesos Electorales por la que se somete el Anteproyecto a información pública.
3. En la memoria explicativa se analiza detenidamente la necesidad y oportunidad del anteproyecto, su contenido y análisis pormenorizado de su articulado. El informe jurídico del Departamento de Seguridad analiza con detalle el fundamento objetivo del proyecto y la adecuación de su contenido al marco jurídico existente. La versión 2 del Anteproyecto recoge las aportaciones realizadas por el informe jurídico, por lo que, centraremos nuestro informe en esta última versión.

II

INTRODUCCIÓN

La Constitución de 1978 fue precursora del reconocimiento y la defensa del derecho fundamental a la protección de datos personales, que nace de la necesidad de dar cobertura a la información personal que el derecho a la intimidad del artículo 18.1CE no podía abarcar. No se trata de preservar la información que la persona no quiere que sea conocida por los demás, sino de que las personas puedan controlar y disponer de sus datos, saber quién los tiene y para qué los usa. La Constitución española fue pionera, después de la Constitución portuguesa, en introducir la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar, en el artículo 18.4CE, al ser consciente de los riesgos que la informática podía tener para la privacidad de las personas

Al cumplimiento de ese objetivo de hacer frente a los riesgos que para los derechos de las personas puede suponer el tratamiento de datos por medios informáticos, responde la Ley



Orgánica 5/1992, de 22 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), que preveía que las Comunidades Autónomas pudiesen dotarse de Autoridades de control, pero exclusivamente respecto de los ficheros de las Administraciones de las propias Comunidades, y que posteriormente la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal(LOPD), amplió a los ficheros de la Entidades Locales de su ámbito territorial.

El TC fue perfilando el concepto, los principios y derechos que conforman el contenido esencial del derecho a la protección de datos personales, por primera vez, en STC 254/1993, de 20 de julio, y fundamentalmente en la STC 292/2000, de 30 de noviembre, señalando que el artículo 18.4CE consagra un derecho fundamental autónomo y distinto al derecho a la intimidad, como garantía constitucional, como respuesta a las amenazas provenientes del uso ilegítimo del tratamiento automatizado de los datos (la informática).

Por su parte, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal constituye el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos personales. No obstante, habrá que esperar hasta 1995 para se apruebe en el ámbito de la UE la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que viene a colmar el vacío existente en la legislación comunitaria respecto de la protección de los datos personales. Sin embargo, no será hasta año 2000 cuando la UE reconozca ese derecho como fundamental en el artículo 8 de su Carta de Derechos.

La Directiva 95/46/CE se transpuso al ordenamiento jurídico interno mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que deroga la ley anterior, la LORTAD.

Tras la aprobación de la LOPD, solo unos pocos Parlamentos Autonómicos legislaron en esta materia, como es el caso del Parlamento Vasco, que ya en el 2004, aprueba la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, en el ejercicio de la competencia exclusiva que a la CAE le atribuye el artículo 10.2 del Estatuto de Autonomía para la organización, régimen y funcionamiento de sus instituciones de autogobierno.

Pero es el 27 de abril de 2016, cuando se aprueban dos nuevas normas que configuran el actual marco europeo de protección de datos personales. El Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, y la Directiva (UE) 2016/680, de 27 de abril de 2016.

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, (RGPD), persigue garantizar un nivel uniforme de protección de las personas en el tratamiento de sus datos, y eliminar los obstáculos a la circulación de datos dentro de la Unión, facilitando así la actividad económica. Por ello, el Reglamento deja poco margen a los Estados miembros para normar sobre esta materia, salvo en las remisiones que contiene a la legislación nacional de esos Estados.



La aprobación del Reglamento Europeo, directamente aplicable en los Estados miembros de la UE desde el 25 de mayo de 2018, introduce numerosas novedades respecto a la normativa de los Estados miembros.

El RGPD extiende su ámbito de aplicación al tratamiento de los datos de las ciudadanas y ciudadanos europeos fuera del ámbito de la Unión; incluye nuevas categorías especiales de datos, como los datos genéticos y los biométricos, y exige que el consentimiento, como base legitimadora para el tratamiento de los datos, se preste mediante una declaración inequívoca o una acción afirmativa clara. Además, el RGPD amplía los derechos de los interesados, y regula nuevos principios aplicables a la protección de datos como el principio de transparencia y el principio de responsabilidad proactiva. Otras de las novedades del RGPD es que introduce modificaciones en el ámbito de las transferencias internacionales, y la ventanilla única, crea el Comité Europeo de Protección de Datos; suprime la obligación de notificar e inscribir los ficheros, regula el régimen sancionador, endureciendo las sanciones por incumplimiento del Reglamento y, amplía notablemente las funciones y poderes de las Autoridades de protección de datos.

Este nuevo modelo europeo de protección de datos personales ha exigido realizar las adaptaciones precisas de los derechos de los Estados miembros. y por lo que se refiere al ordenamiento jurídico interno, la actualización de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, que trasponía la derogada Directiva 95/46/CE, que ha sido sustituida por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El papel de la nueva Ley Orgánica 3/2018 (LOPDGDD), tal y como explicita su exposición de motivos, no ha sido otro que desarrollar o complementar las disposiciones del RGPD dentro de los márgenes que el propio RGPD establece, eliminando del ordenamiento las normas incompatibles con el mismo. Debe tenerse en cuenta que es el propio RGPD el que regula el contenido esencial del derecho, y establece un régimen completo y uniforme para toda la Unión. Siendo ello así, no se entiende que una parte del articulado de esa ley tenga rango de orgánica, y el resto, en su mayoría, el carácter de condiciones básicas, al dictarse al amparo del artículo 149.1.1CE.

Por su parte, la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, ha sido transpuesta al ordenamiento jurídico interno recientemente, mediante 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.

Según su exposición de motivos, esta ley orgánica asume la finalidad de lograr un elevado nivel de protección de los derechos de la ciudadanía en general, y de sus datos personales, en particular, que resulte homologable al del resto de los Estados de la UE, incorporando y concretando las reglas que establece la directiva, estableciendo un marco jurídico que proporcione la seguridad jurídica necesaria para facilitar la cooperación policial y judicial penal y, una mayor eficacia en el desempeño de sus funciones por las Fuerzas y Cuerpos de Seguridad y del sistema judicial penal en su conjunto, incluido el penitenciario.



A tenor de lo dispuesto en esta Ley Orgánica, la AEPD y las Autoridades Autonómicas, en sus respectivos ámbitos competenciales, serán las autoridades de protección de esos datos, regulando la ley sus potestades y funciones y la asistencia entre autoridades de los Estados miembros. Además, en cuanto a los procedimientos de reclamación ante esas Autoridades, esta Ley dispone que esos procedimientos se rijan por la Ley Orgánica 3/2018 o por la que regule la autoridad de protección de datos competente.

Este nuevo marco normativo obliga a la Comunidad Autónoma de Euskadi a abordar las reformas normativas necesarias, y el anteproyecto de ley sometido a informe responde a esta necesidad, sustituyendo a la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

III

CONSIDERACIONES GENERALES

1.- Competencia

El presente informe se emite en virtud de las funciones que el artículo 17 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, atribuye a la Agencia Vasca de Protección de Datos.

2.- Objeto de la norma

El Anteproyecto de Ley tiene por objeto, según proclama su artículo 1.1, adaptar la normativa autonómica vasca en materia de protección de datos al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, a la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y a 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.

Asimismo, el Anteproyecto tiene por objeto regular el régimen jurídico de la Autoridad Vasca de Protección de Datos.

Toda vez que las necesidades de adaptación normativa exigidas por el Reglamento General y las dos Leyes Orgánicas citadas ya han sido expuestas en la introducción, nos detendremos ahora en la necesidad de regular el régimen jurídico de la Autoridad Vasca de Protección de Datos.

En este sentido, debe destacarse que el RGPD dota a las autoridades de protección de datos de nuevas potestades y funciones, y establece normas relativas a su régimen jurídico, pero dejando un amplio margen a los Estados miembros, a los que encomienda el establecimiento por ley de sus Autoridades de protección de datos, las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control, las normas y procedimientos para su nombramiento, la duración de su mandato, el carácter renovable o no del cargo, y las condiciones por las que se rigen sus obligaciones, y las del personal de cada autoridad, las prohibiciones relativas a acciones, ocupaciones y



prestaciones incompatibles con el cargo durante su mandato y después del mismo, y las normas que rigen su cese, y también deberá ser la ley la que regule el ejercicio de sus potestades, los procedimientos en los que interviene, su régimen de personal y presupuestario.

Del mismo modo, la LO 7/2021, de 26 de mayo, atribuye a las autoridades de protección de datos, estatal o autonómica, amplias potestades y funciones en el marco de esa ley, y establece que los procedimientos de reclamación ante esas Autoridades serán los que la ley de la autoridad respectiva disponga

La Ley proyectada va a ser precisamente la que regule el régimen jurídico de la Autoridad de protección de datos de esta Comunidad Autónoma en los términos exigidos por estas normas, modificando su denominación actual como Agencia Vasca de Protección de datos por la de Autoridad Vasca de Protección de Datos, que creemos refuerza su verdadera naturaleza de Autoridad de Control en protección de datos.

III

ANÁLISIS DEL ANTEPROYECTO

TÍTULO

El Título de la Ley debe permitir conocer de manera breve el objeto de la misma. Por ello, creemos conveniente revisar el título del anteproyecto, para incluir en el mismo, al igual que lo hace la Ley 2/2004, de 25 de febrero, a la Autoridad Vasca de Protección de Datos, pues a ella se refiere tanto el objeto como gran parte del contenido del Anteproyecto. En consecuencia, y atendiendo a la relevancia del papel de la Autoridad como garante del derecho fundamental, proponemos que la futura ley se titule “**Ley de Protección de Datos Personales y de la Autoridad Vasca de Protección de Datos.**”

CAPÍTULO I

El Capítulo I dedicado a las Disposiciones Generales consta de dos artículos clave para la comprensión del texto: el artículo primero regulador del objeto, y el segundo en el que se describe el ámbito de aplicación.

En lo que se refiere el objeto del texto, como ya se ha expuesto, la nueva normativa aprobada en materia de protección de datos obliga a adaptar el texto autonómico, que en buena parte ya ha perdido su vigencia. Además, la aprobación del Reglamento Europeo de Protección de Datos ha supuesto un espaldarazo para las autoridades de control, que ven ahora mucho más reforzada su posición debido a las funciones y poderes que les atribuye el Reglamento General en sus artículos 57 y 58 y la Ley Orgánica 7/2021 de 26 de mayo en sus artículos 49 y 50. Por todo ello, se hace ineludible la regulación del régimen jurídico de la Autoridad Vasca de Protección de Datos.

En cuanto al ámbito de aplicación, debe destacarse que se produce un incremento exponencial del mismo por dos motivos: por una parte, el **ámbito subjetivo** se amplía al incluirse en el mismo la Administración Institucional y sector público de las Administraciones territoriales de la Comunidad Autónoma de Euskadi. Por otra parte, **el ámbito objetivo** actualmente existente queda rebasado al quedar bajo control de la Autoridad Vasca de



Protección de Datos los tratamientos a que se refiere 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. Esta doble modificación del ámbito, con la incorporación de un número importante de entidades de naturaleza jurídico-privada y con la asunción del control de tratamientos de datos policiales hasta ahora excluidos, tendrá una relevancia trascendental en el desenvolvimiento de la Institución, que deberá contar con los medios personales y materiales adecuados y suficientes para el correcto desempeño de su cometido.

CAPÍTULO II

El Capítulo II dedicado a la Autoridad Vasca de Protección de Datos es el más extenso del texto (artículos 3 a 23) y regula la organización y régimen jurídico, los órganos de la Autoridad Vasca de Protección de Datos, la potestad de investigación, la potestad normativa, otras funciones de la Autoridad y la cooperación con otras Autoridades de protección de datos.

La Sección primera de este Capítulo (artículos 3 a 7) regula la naturaleza y régimen jurídico de la Autoridad, su régimen económico y presupuestario, el régimen de personal, funciones y potestades y por último la transparencia.

A través de esos siete preceptos, el pre-legislador ha tratado de resaltar y garantizar una característica esencial de la Institución: su **independencia**. Ha de recordarse en ese sentido que, la Carta de Derechos Fundamentales de la Unión Europea, tras proclamar el derecho fundamental a la protección de datos en su artículo 8.1, declara en el apartado 3 de dicho precepto que el respeto de las normas de protección de datos “quedará sujeto al control de una autoridad independiente”.

En idénticos términos se expresa el Tratado de Funcionamiento de la Unión Europea en su artículo 16.2

El Reglamento General de Protección de Datos es consciente del papel de las Autoridades de Control como instituciones independientes llamadas a reforzar el sistema de garantías de los derechos de las personas, y por ello amplía notablemente sus funciones y poderes (artículos 57 y 58 RGPD).

La independencia de la Institución queda reflejada a través de varios aspectos, como la **naturaleza jurídica** atribuida, Autoridad Administrativa Independiente, que se relaciona con el Gobierno Vasco a través de la Lehendakaritza. Se configura pues la Autoridad Vasca sin un vínculo de subordinación con el Gobierno Vasco, sino en condiciones de igualdad y al más alto nivel de relación.

La regulación del **régimen económico y presupuestario** refleja asimismo la naturaleza independiente de la Autoridad, al elaborar y aprobar el anteproyecto de su presupuesto y al contar entre sus ingresos con aquellos derivados del ejercicio de su potestad sancionadora. En este punto, el texto de manera expresa dispone que el resultado positivo de sus ingresos al término del ejercicio se destinará por la Autoridad Vasca de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

En cuanto al **régimen de personal**, la condición de funcionario exigida al personal a su servicio redunda también en favor de la independencia, que igualmente se manifiesta en el



hecho de que sea la propia Autoridad la que determine el régimen de acceso a sus puestos de trabajo, los requisitos de las pruebas de selección y los procedimientos de provisión y promoción profesional.

En este punto, y teniendo en cuenta las limitaciones de personal de la Autoridad, proponemos incorporar al Anteproyecto de ley una previsión similar a la contemplada en la Ley 2/2004, para que **la representación y defensa letrada de la Autoridad Vasca de Protección de Datos se realice por el Servicio Jurídico Central del Gobierno Vasco.**

Respecto a las **funciones y potestades**, el artículo 6 se remite expresamente a las establecidas en los artículos 57 y 58 del RGPD, y en los artículos 49 y 50 de la LO7/2021, y también a cuantas competencias le sean legalmente atribuidas, posibilitando así que la AVPD pueda desempeñar las funciones y potestades que le atribuyan otras leyes.

En cuanto a la **transparencia**, la Autoridad Vasca como cualquier Administración Pública está sujeta a las obligaciones de publicidad activa que establece la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno. Sin embargo, el texto incluye en su artículo 7 compromisos adicionales a los recogidos en la ley estatal, al obligarse a publicar las resoluciones que pongan término a determinados procedimientos, así como directrices generales, informes preceptivos, dictámenes y códigos de conducta aprobados.

Añade el apartado 3 del artículo 7 que esa difusión se realizará tras disociar los datos personales y respetando los límites establecidos en la legislación de transparencia y acceso a la información pública. En relación con esta previsión, es necesario señalar que esa disociación no operará en los supuestos contemplados en el artículo 28 del anteproyecto (publicidad de las sanciones en el BOPV).

La Sección segunda regula en sus artículos 8 y 9 los dos órganos de la Autoridad Vasca de Protección de Datos, esto es, la Presidencia (art. 8) y el Consejo Consultivo (art.9)

En cuanto a la **Presidencia**, de nuevo el texto vuelve a incidir en el carácter independiente en el ejercicio de sus funciones, sin que pueda estar sujeta a instrucción alguna en el desempeño de las mismas. La independencia se ve reforzada también por el plazo de duración de su mandato, cinco años, al no coincidir con la duración de la legislatura.

En cuanto al nuevo procedimiento de designación de la persona candidata a la presidencia, entendemos muy acertada la intervención no solo del Poder Ejecutivo sino también del Poder Legislativo, a través de la Comisión de Instituciones, Seguridad y Gobernanza Pública, que deberá aprobar por mayoría absoluta la propuesta del Gobierno Vasco, lo que demanda una mayor necesidad de consenso, que redundará en beneficio de la independencia de la Institución. También se exigirá la mayoría absoluta de esa Comisión para la ratificación del cese de la persona que ocupe la Presidencia cuando la causa de su separación sea el incumplimiento grave de sus obligaciones, la incapacidad sobrevenida para el ejercicio de su función o la incompatibilidad. Con esta previsión se pretende evitar la arbitrariedad en el cese de la persona que ocupe la Presidencia de la Autoridad.

El aumento de rango de la Presidencia, asimilado al de las personas que ostenten una Viceconsejería, parece lógico, dado el impulso e incremento de funciones atribuido a las Autoridades de control tanto en el Reglamento General como en la Ley Orgánica 3/2018 de 5 de diciembre y la Ley Orgánica 7/2021 de 26 de mayo.



En cuanto al **Consejo Consultivo**, se mantiene como órgano de asesoramiento de la Autoridad, si bien aumenta su número de miembros. Este aumento puede considerarse razonable, si tenemos en cuenta que los Territorios Históricos solo disponían de un representante conjunto en el Consejo y que, además, al ampliarse el ámbito de aplicación de la ley al sector público vasco, las entidades de derecho privado deben estar reflejadas en su composición. Además, el Anteproyecto establece que en la composición de ese Consejo Consultivo se procurará que estén representados ambos sexos al menos al 40%, garantizando así una representación equilibrada de mujeres y hombres con capacitación, competencia y preparación adecuada.

Las Secciones 3ª, 4ª y 5ª de este Capítulo regulan las potestades de investigación, potestades normativas y otras funciones de la Autoridad Vasca de Protección de Datos.

En este punto, resulta obligado destacar que el RGPD tiene una especial incidencia en el marco autonómico. Al igual que la derogada Directiva 95/46/CE, contempla expresamente la posibilidad de que haya más de una Autoridad de Protección de Datos en cada Estado miembro (Art. 51.1), a fin de reflejar su estructura constitucional, organizativa y administrativa (Considerando 117), disponiendo que todas las autoridades de control tienen que tener en el Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las autoridades encargadas de la persecución de delitos (Considerando 129). Además, el RGPD exige que sean los Estados miembros quienes regule por ley las Autoridades de Protección de datos (artículo 54).

En cuanto a la LOPDGDD, tras regular en el Capítulo I de su Título VII, la Agencia Española de Protección de Datos, dedica el Capítulo II de ese Título a las Autoridades Autonómicas de Protección de Datos. Este Capítulo II se dicta al amparo del art. 149.1.1 CE, pero ese título competencial no puede convertirse en una suerte de legislación básica, dado que la realidad de cada Comunidad Autónoma no es homogénea, ni tiene que serla. Las CCAA pueden decidir dotarse o no de Autoridades de Protección de Datos. De hecho, en la actualidad solo tres Comunidades Autónomas disponen de esa Autoridad (Cataluña, Andalucía y Euskadi), ya que la Agencia de la Comunidad de Madrid fue suprimida en el año 2012, y ello sin perjuicio de que en un futuro se creen nuevas autoridades de control, particularmente, en las CCAA donde sus estatutos incorporan el derecho a la protección de datos como Aragón, Baleares y Castilla-León, aunque sólo el estatuto de esta última prevea la posibilidad de creación de una autoridad propia.

En relación con las funciones y potestades de las Autoridades Autonómicas, la Agencia Vasca, al informar el anteproyecto de la LOPDGDD, ya destacó la necesidad de que la ley fuese respetuosa con las funciones que conforme al modelo territorial del Estado pueden asumir las autoridades autonómicas, que se amplían a la luz del Reglamento Europeo, y que sin embargo el texto inicial no contemplaba, como su intervención en la promoción de códigos de conducta, mecanismos de certificación, y aprobación de normas corporativas vinculantes. También insistió la Agencia en la necesidad de que la ley estableciese mecanismos que garantizaran la participación efectiva de las autoridades autonómicas en el mecanismo de coherencia, y la capacidad de propuesta al representante común en el Comité Europeo de Protección de Datos, lo que finalmente tuvo reflejo en el texto de la LOPDGDD, que es consciente de que el Reglamento Europeo sitúa a todas las autoridades



de control en un mismo plano de igualdad, con independencia de que exista una autoridad principal.

Volviendo de nuevo al Anteproyecto, la Sección 3ª de este Capítulo II, está dedicado a las **potestades de investigación** (artículos 9 a 14). La potestad de investigación es algo inherente a la Autoridad, dada su condición de garante del derecho fundamental. Esta potestad es reconocida por el Reglamento, por la Ley Orgánica 3/2018 de 5 de diciembre y también por la Ley Orgánica 7/2021 de 26 de mayo.

Debe reseñarse a este respecto que se trata de una **potestad no condicionada** a la existencia de reclamación alguna, sino que la Autoridad puede ordenar la realización de diligencias de investigación motu proprio o incluso puede acordar la realización de planes de auditoría a fin de conocer el grado de cumplimiento del derecho fundamental en ámbitos sectoriales concretos.

En cuanto al personal competente para la actividad investigadora, es lógica la exigencia de condición funcionarial, así como su estatus de agente de la autoridad. Merece destacarse la novedad impuesta por el Reglamento a través del procedimiento transfronterizo, de la **actuación conjunta de inspectores** de distintos Estados miembros de la Unión.

Es verdaderamente destacable el **alcance de la actividad de investigación**, regulado en el artículo 12 que, con carácter enunciativo y no taxativo, concreta las actuaciones inspectoras en las diferentes posibilidades de acceso a locales, examen de soportes, de sistemas de información, requerimientos de envío de programas o documentos, de ejecución de aplicaciones, revisión de medidas técnicas u organizativas adoptadas, etc. Se trata de una regulación amplísima de las facultades inspectoras, a las que, eso sí, les sería de aplicación el límite de la inviolabilidad del domicilio, precisándose en este caso consentimiento o autorización judicial.

El ejercicio de las facultades de investigación implica necesariamente un **deber de colaboración de los responsables de tratamiento**. Por ello, el texto positiviza el deber de colaboración con la Autoridad Vasca de Protección de Datos (proporcionando la información necesaria para la investigación en su ámbito competencial) extendiéndolo no solo a Administraciones Públicas, sino también a personas físicas o jurídicas aun cuando sus tratamientos no estén sometidos a la ley vasca. Especialmente necesaria resulta la mención expresa que se realiza a la Hacienda Foral como Administración sometida al deber de colaboración, a fin de declarar su sometimiento a este deber, sin que pueda invocarse colisión con la normativa tributaria.

Finaliza esta Sección 3ª con la regulación de los **planes de auditoría**, instrumento de gran importancia, al que también se alude en la Sección 6ª cuando regula la posibilidad de su realización conjunta con otras Autoridades de Protección de Datos. Los planes de auditoría constituyen un elemento esencial para testar el grado de cumplimiento de la normativa en un sector, entre un concreto ámbito de responsables o encargados de tratamiento o respecto a tratamientos concretos. Como resultado de esto planes, las Autoridades pueden adoptar directrices de obligado cumplimiento, actuación que redundará en una mayor garantía del derecho fundamental.

La Sección cuarta del texto se dedica a la **potestad normativa**, regulada en un único precepto, el artículo 15. Esta potestad reglamentaria de la Autoridad Vasca de Protección de Datos se concreta en la posibilidad de elaboración de circulares, donde se fijarán los



criterios de actuación de la Autoridad Vasca en la aplicación del Reglamento y demás normativa de protección de datos. A pesar de que por su denominación pueda entenderse lo contrario, se trata de normas con eficacia ad extra, en cuya elaboración se debe garantizar la audiencia a los interesados, y que son de obligado cumplimiento una vez publicadas en el BOPV.

La Sección quinta del Capítulo II se dedica a **otras funciones de la Autoridad Vasca de Protección de datos** (artículos 16 a 20), comprendiendo la acción exterior, las competencias en materia de transferencias internacionales de datos, en materia de Códigos de conducta, certificación y formación.

El texto reafirma el papel de las Autoridades Autonómicas en el **ámbito exterior**, más concretamente de la Autoridad Vasca, que ya cuenta con un bagaje contrastado a través de su participación en las Conferencias Europeas e Internacionales de Protección de Datos durante muchos años, si bien el texto explicita además la posibilidad de la Autoridad de celebrar acuerdos internacionales administrativos y acuerdos no normativos.

El texto, tras reconocer a la Autoridad Vasca competencias para la aprobación de instrumentos legitimadores de **transferencias internacionales de datos**, como cláusulas contractuales tipo o normas corporativas vinculantes, plasma las competencias de la autoridad sobre dos elementos nuevos introducidos por el Reglamento General: los Códigos de Conducta y las certificaciones. Se trata de figuras que proceden del ámbito privado, pero que pueden servir para el cumplimiento del principio de responsabilidad proactiva: esto es, el principio en virtud del cual, el responsable no solo debe cumplir las disposiciones del Reglamento, sino que debe estar en condiciones de poder acreditar dicho cumplimiento.

El cambio introducido por el Reglamento Europeo en cuanto al modo de cumplimiento de sus principios obliga a poner a disposición de los responsables de tratamiento instrumentos que coadyuven a la acreditación del cumplimiento; por ello, tanto los **códigos de conducta** como las **certificaciones** pueden jugar un papel esencial en el principio de responsabilidad proactiva, por lo que su aprobación debe someterse a las Autoridades de control, tal y como dispone el texto en sus artículos 18 y 19.

En lo referente a la **formación en materia de protección de datos**, el artículo 20 del texto recoge el compromiso de la Autoridad Vasca de Protección de Datos para promover la difusión del derecho fundamental, con el propósito de garantizar un adecuado conocimiento por los ciudadanos en lo que se refiere a sus derechos y por los responsables en lo relativo a sus obligaciones.

Esta previsión es oportuna y necesaria, habida cuenta del desconocimiento existente sobre la materia tanto de ciudadanos como de responsables de tratamiento. Además, se trata de una función que el Reglamento atribuye de manera expresa a las Autoridades de Control (artículo 57.1 apartados b y d). También debemos reseñar que la ampliación del ámbito subjetivo de aplicación contenida en el texto, al incluir a responsables de tratamiento de naturaleza jurídico-privada, obliga a intensificar esta labor divulgativa, labor que en la memoria del texto es considerada objetivo prioritario.



Cooperación con otras Autoridades de protección de datos

Para finalizar el Capítulo II del Anteproyecto dedicado a la Autoridad Vasca de Protección de Datos, debemos detenernos en su Sección 6ª, referida a la cooperación con otras autoridades de protección de datos (artículos 21 a 23).

Las relaciones entre las distintas Autoridades de Protección de Datos no pueden basarse únicamente en el principio de competencia, sino que debe complementarse con base a principios de cooperación institucional, coordinación de criterios, e información mutua, como de hecho estamos actuando la Agencia Española y las Agencias Autonómicas, por ello la AVPD, en su informe al anteproyecto de LOPDGDD, criticó que la ley otorgue a la Agencia Española de Protección de Datos la potestad de intervención ante una hipotética dejación de funciones de las autoridades autonómicas de control (artículo 59 de la ley orgánica).

El principio de cooperación, colaboración y coordinación entre las Administraciones Públicas se consagra en el artículo 3.1k) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Este principio tiene reflejo en el proyecto de ley de forma expresa al regular la cooperación institucional entre la Autoridad Vasca de Protección de Datos y las restantes autoridades de protección de datos del Estado.

Esta cooperación se concreta en el intercambio de información, la prestación de asistencia y auxilio, la realización de actuaciones comunes de auditoría e investigación y la participación en los grupos de trabajo que al efecto se constituyan.

La invocación del principio de cooperación interadministrativa es realmente necesaria en un ámbito en el que, en muchas ocasiones, la adecuada garantía del derecho fundamental de las personas exige una actuación coordinada entre las distintas autoridades de control.

Fuera del ámbito local, la regulación del procedimiento transfronterizo contenida en el Reglamento es la expresión más acabada de la necesidad de colaboración entre Autoridades de control diferentes, como más adelante expondremos.

Proclamado el principio de cooperación institucional, el texto regula con detalle, como una concreción del citado principio, la **intervención conjunta en los planes de auditoría**. A estos planes se refiere el artículo 14 del texto; consisten en evaluar el grado de cumplimiento del derecho fundamental en un determinado sector de actividad. En estos supuestos, la actuación administrativa finaliza con la adopción de directrices dirigidas a los sujetos inspeccionados o a un responsable concreto.

La singularidad de los planes conjuntos estriba en la intervención de la AVPD con las diferentes Autoridades de Protección de Datos del Estado, incluso para la realización de actuaciones de investigación, atribuyendo además el papel coordinador a la AVPD cuando se trate de responsables o encargados sometidos a su ámbito de aplicación, lo que parece razonable por respeto al ámbito competencial de cada Autoridad.

Por último, el texto regula en el artículo 23 la cooperación en el marco de los procedimientos transfronterizos, para lo cual, parte de la regulación contenida en la LOPDGDD (art. 61.1) para determinar los supuestos en los que **la Autoridad Vasca de Protección de Datos puede ostentar la condición de autoridad principal o autoridad interesada**, esto es, en



aquellos supuestos en los que el tratamiento difiere en contenido, alcance y fines de los desarrollados por ese responsable en el resto del Estado.

El apartado 2 del precepto recuerda además las posibilidades de intervención de la AVPD en las reuniones del Comité Europeo de Protección de Datos.

CAPÍTULO III

El Anteproyecto dedica el Capítulo III (artículos 24 a 29) al régimen sancionador.

Una de las razones que motivaron la aprobación del RGPD fue la necesidad de regular un régimen sancionador uniforme en los Estados de la UE, dado que hasta esa fecha había Estados que ni siquiera sancionaban la vulneración de este derecho fundamental, y el resto lo hacían de manera muy distinta.

Entre las principales novedades del RGPD debe destacarse que se endurecen las sanciones por incumplimiento del Reglamento. El régimen sancionador se agrava y se vuelve mucho más exigente en toda la UE, y las multas pueden alcanzar hasta los 20 millones de euros, o tratándose de una empresa hasta el 4% del volumen de negocio total anual global del ejercicio anterior. Además, estas multas pueden ser impuestas con carácter sustitutivo o complementario de las medidas correctoras que establece el artículo 58 del RGPD.

No obstante, el Reglamento Europeo exige, que las sanciones sean individuales, efectivas, proporcionadas y disuasorias, en función de las circunstancias concurrentes en cada caso, y aplicando los criterios que señala en su art. 83. Además, en el caso de que se sancione a personas físicas habrá que considerar el nivel general de ingresos prevaeciente en el Estado miembro, y la situación económica de la persona sancionada

El RGPD regula las infracciones, los límites máximos de las sanciones y los criterios para determinar en cada caso la sanción a imponer. Sin embargo, no regula ni la graduación de las sanciones, ni la prescripción de las infracciones y sanciones. Tampoco cual será el procedimiento sancionador aplicable. Deberán ser los Estados miembros los que establezcan también las normas en materia de otras sanciones que podrán ser impuestas por la infracción del reglamento.

Las infracciones al RGPD tampoco se tipifican como leves, graves y muy graves, si bien, pueden ser sancionadas con unos límites distintos: hasta 20 millones de euros o el 4 % del volumen de negocio total anual global, cuando se infrinjan principios y derechos reconocidos por el Reglamento, y se sancionan en menor medida, hasta 10 millones de euros o el 2% del volumen de negocio total anual, las infracciones derivadas del incumplimiento de obligaciones formales y de medidas de seguridad.

El RGPD tampoco resuelve si las Administraciones y Entidades Públicas van a poder ser sancionadas económicamente, lo que debe determinarse por cada Estado, y reconoce también a los interesados el derecho a la indemnización por los daños y perjuicios sufridos como consecuencia de un tratamiento ilícito de los datos personales.

Por su parte, la LOPDGDD dedica todo su Título IX al régimen sancionador, que se dicta al amparo del artículo 149.1.1CE, y junto al RGPD desarrollan el sistema de sanciones en



materia de protección de datos personales, concretando las conductas y diferenciando las infracciones en muy graves, graves y leves a efectos de prescripción.

La LOPDGDD sigue optando por no sancionar económicamente a las Administraciones e Instituciones Públicas, lo que ha sido duramente criticado por el sector privado. Esta medida parece obedecer a distintas razones: de un lado, a la falta de recursos públicos y, por otro, a que las Administraciones no tratan de obtener un beneficio económico derivado del tratamiento de datos (petróleo del siglo XXI). Si infringen la normativa de PD no es por un interés económico, sino más bien por la deficiente gestión de los datos que manejan o en muchas ocasiones, por la evidente falta de medios materiales y personales, o la falta de formación de sus empleados.

Por su parte, la LO 7/2021, de 26 de mayo, en su Capítulo VIII (artículos 56 al 65) regula el régimen sancionador específico aplicable ante incumplimientos de las obligaciones previstas en esta Ley Orgánica. En su articulado se definen los sujetos sobre los que recaerá la responsabilidad por las infracciones cometidas, se determinan las reglas del concurso de normas para resolver los casos en los que un hecho pueda ser calificado con arreglo a dos o más de ellas, se tipifican las infracciones, que, en función de su gravedad, podrán ser leves, graves o muy graves y, por último, se establecen las sanciones que se pueden imponer, y se fijan los plazos de prescripción tanto de las infracciones como de las sanciones y de caducidad.

Las sanciones que podrán imponerse por infringir esta Ley Orgánica, irán desde 6.000 euros por la infracción más leve a 1.000.000 de euros para la conducta más grave. Además, tampoco serán sancionadas económicamente las Administraciones e Instituciones Públicas.

El Anteproyecto de ley, en su Capítulo III, introduce algunas novedades exigidas por el Reglamento General de Protección de Datos.

Así, **se amplía el catálogo de sujetos responsables**, que no se reducen a los sujetos enunciados en el ámbito de aplicación de la norma (artículo 2) cuando actúen como responsables o encargados del tratamiento, sino que incluye además a las entidades de supervisión de los códigos de conducta aprobados por la AVPD y a las entidades de certificación acreditadas por la AVPD. Se trata de una previsión totalmente necesaria, a la vista de las nuevas funciones que el Reglamento atribuye a las autoridades de control sobre las entidades anteriormente citadas.

En lo referente a las **infracciones**, para su determinación es obligada la remisión al Reglamento General de Protección de Datos, a la LO 3/2018 y a la LO 7/2021, tal y como recoge el texto en su artículo 25.1.

Asimismo, el Anteproyecto regula la interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la presunta persona infractora.

En lo relativo a las **sanciones**, el texto, al igual que la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, contempla un régimen sancionador diferenciado según la naturaleza jurídica pública o privada del responsable, encargado, entidad de supervisión o de la entidad de certificación.



En este sentido, el texto dedica el artículo 26 a las **sanciones** o medidas correctivas a imponer a los entes de naturaleza jurídica privada (multas) y el artículo 27 al régimen propio de las Administraciones, Entidades e Instituciones Públicas Vascas (apercibimiento). En este último caso, no existen por tanto sanciones económicas, pero sí una sanción reputacional, agravada en el caso de infracciones imputables a autoridades, altos cargos y directivos si se acreditase la existencia de informes técnicos o recomendaciones no debidamente atendidos. En este último caso, además del apercibimiento se prevé una amonestación pública (publicación en el BOPV) para el cargo, autoridad o directivo responsable.

Otra novedad muy importante introducida por el texto en el **régimen sancionador de los altos cargos autoridades o directivos** consiste en que, en caso de estar sometidos al Código Ético y de Conducta de los cargos públicos y personal eventual de la Administración General e Institucional de la Comunidad Autónoma de Euskadi, se dará igualmente traslado de la resolución a la Comisión de Ética Pública. Esta novedosa previsión, merecedora de elogio, implica la introducción de un criterio de rendición de cuentas que puede conllevar incluso el cese o el apartamiento del cargo.

El anteproyecto incorpora dos **preceptos relativos a publicidad** que obedecen a motivos distintos; nos referimos al art. 7 y el art. 28. Si bien el artículo 7 está conectado con el escrutinio público propio del principio de transparencia, la publicidad a que se refiere el artículo 28 está más vinculada al cumplimiento del principio de tipicidad, básico en materia sancionadora.

Así, este precepto prevé la publicación en el BOPV de la identidad de infractor, infracción e importe de aquellas sanciones superiores a un millón de euros y de las amonestaciones consecuencia de infracciones cometidas por autoridades, altos cargos y directivos. Esta publicidad (incluida en el Capítulo III “Régimen Sancionador”), no deja de ser una sanción añadida, y por tanto exige una previsión legal, por lo que se entiende acertada su inclusión en el texto.

En cuanto a la **prescripción**, el texto recoge idénticos plazos de prescripción que la Ley estatal.

CAPÍTULO IV

El Anteproyecto dedica el Capítulo IV a regular los procedimientos en caso de infracción de las normas de protección de datos.

Son tres los procedimientos previstos en el texto:

- 1) Procedimientos vinculados con la falta de atención o inadecuada atención de solicitudes de ejercicio de los derechos reconocidos en los art. 15 a 22 del RGPD y 21 a 23 de la Ley Orgánica 7/2021
- 2) Procedimientos que tienen por objeto la determinación de la existencia de una posible infracción en materia de protección de datos
- 3) Procedimientos transfronterizos. En estos la AVPD puede asumir la condición de autoridad principal o de autoridad interesada.



Los dos primeros procedimientos se corresponden con el ya conocido procedimiento de tutela de derechos, y con el procedimiento sancionador o declarativo de infracción.

El tercero de los procedimientos, el **procedimiento transfronterizo**, supone una novedad importantísima introducida por el RGPD que condiciona de forma notable la regulación de los distintos trámites como posteriormente analizaremos.

Una de las finalidades del RGPD era la implantación en la Unión Europea de una regulación armonizada del derecho fundamental que evitase la fragmentación normativa originada por la Directiva y las asimetrías derivadas de las diferentes interpretaciones de los principios básicos que regulan en Europa la privacidad de las personas. Los mecanismos de coherencia y cooperación previstos en el Reglamento, con participación activa de autoridades de control de diferentes Estados, vienen a traducir al derecho positivo esa necesidad de aplicación uniforme.

La aplicación del Reglamento genera por tanto un nuevo tipo de procedimiento, el **procedimiento transfronterizo**, en el que tal y como acertadamente preceptúa el Anteproyecto (art. 32), la Autoridad Vasca debe determinar su condición de autoridad principal o interesada, y en este último caso, dar traslado inmediato de la reclamación a la autoridad del Estado miembro de la Unión que ostente la condición de autoridad principal.

La intervención de diferentes autoridades de control exigida en el procedimiento transfronterizo (e incluso la posible intervención del Comité Europeo de Protección de Datos) afecta necesariamente a la regulación de los procedimientos.

Una evidencia de la afirmación anterior la encontramos en la inclusión del **trámite de admisión previa**, previsto en el artículo 33 del texto, trámite imprescindible, como bien dice la memoria explicativa, puesto que es preciso en todo caso el examen de la competencia de la Autoridad Vasca antes de proseguir el iter procedimental, y, en caso de tratarse de un procedimiento transfronterizo deberá determinarse además cuál es la autoridad principal y cuáles las autoridades interesadas, cuestión no siempre sencilla de resolver.

Creemos por ello acertada la inclusión de la admisión previa, cuyo acuerdo debe adoptarse en el plazo de tres meses (mismo plazo que el previsto en la LOPDGDD para la AEPD); asimismo entendemos muy acertada la previsión de que, ante la falta de resolución en plazo sobre la admisión previa, se prosiga la tramitación por el cauce correspondiente a la pretensión formulada por el interesado, de tal modo que la inactividad de la Autoridad de Control no redunde en perjuicio del reclamante.

La regulación de este nuevo trámite conlleva además la de las **causas de inadmisión**, que, de forma adecuada a nuestro juicio, se regulan en el artículo 34 del texto. Algunas de ellas tienen que ver con el desconocimiento por la ciudadanía del derecho fundamental, (cuando la reclamación no versa sobre protección de datos), otras con el escaso o nulo esfuerzo probatorio de las reclamaciones y otras con el ejercicio abusivo o antisocial del derecho (reclamaciones abusivas).

Igualmente, creemos que merece un favorable acogida la previsión de la **advertencia** incluida en el precepto, lo que permitirá reservar el ius puniendi del Estado a aquellas reclamaciones que verdaderamente lo merezcan.

En cuanto a los **procedimientos en caso de reclamaciones derivadas del ejercicio de derechos**, además de la inclusión del trámite de admisión previa, regula un procedimiento



similar al ya existente, si bien se insiste especialmente en la audiencia de la persona afectada, lo que en todo caso merece un comentario favorable. El plazo de seis meses para resolver es sensiblemente inferior al de los procedimientos de ejercicio de la potestad sancionadora, lo que parece lógico y adecuado. Una vez transcurrido el plazo sin resolución, **el sentido del silencio es negativo**, lo que parece razonable, pues la inactividad en este caso no es achacable al responsable del tratamiento, sino a la autoridad de control.

En cuanto a los **procedimientos de ejercicio de la potestad sancionadora**, en estos además del trámite de admisión previa se prevén unas actuaciones previas de investigación por un plazo máximo de duración de doce meses, plazo amplio derivado de la complejidad que introduce el procedimiento transfronterizo. En cuanto a su tramitación, se remite a la normativa reguladora del ejercicio de la potestad sancionadora en Euskadi, si bien se aparta en cuanto al plazo de duración de la tramitación del procedimiento, al ampliarlo de seis a nueve meses, ampliación motivada igualmente por las exigencias del RGPD.

Por último, se considera acertada la inclusión de las medidas cautelares a que se refiere el artículo 39 encaminadas al cese de la conducta infractora y a la minimización de los daños.

DISPOSICIONES ADICIONALES, TRANSITORIAS Y FINALES

La parte final del anteproyecto, contiene dos disposiciones adicionales, dos transitorias, una derogatoria y dos disposiciones finales.

En lo referente a las disposiciones adicionales, la **adicional primera** declara que, fuera de los procedimientos específicos regulados en el Capítulo IV, la actividad de la Autoridad Vasca de Protección de Datos estará sometida a la normativa reguladora del procedimiento administrativo que resulte de aplicación, previsión lógica dada la naturaleza jurídico-administrativa de la Autoridad.

Por otro lado, la Disposición **adicional segunda** resulta obligada al determinar que las referencias a la Agencia Vasca de Protección de Datos deben entenderse realizadas a la Autoridad Vasca de Protección de Datos, nueva denominación de la Institución, alineada con la nomenclatura utilizada por el Reglamento y más acorde con la trascendencia de las funciones y poderes que la normativa comunitaria le atribuye.

En cuanto a las **Disposiciones transitorias**, merece atención **la transitoria primera** que declara vigente el actual Estatuto de la Institución en lo que no se oponga a la futura ley; no obstante, es evidente la necesidad de que una vez aprobado el texto legal, se acometa la elaboración de un nuevo Estatuto de la Autoridad Vasca de Protección de Datos. Además, y continuando con la transitoria primera, es acertada la previsión de que el nuevo rango concedido a la persona que dirija la Institución al tiempo de la entrada en vigor de la futura ley se aplique una vez expirado su mandato.

La Disposición transitoria segunda establece el régimen aplicable a los procedimientos ya iniciados a la entrada en vigor de esta ley, o respecto de los que ya se hubiesen iniciado actuaciones previas, que se regirán por la normativa anterior.

En este punto podría considerarse oportuna la inclusión de una referencia al principio de irretroactividad de las normas sancionadoras desfavorables.



En lo referente a la **Disposición derogatoria**, razones de seguridad jurídica aconsejan la derogación expresa de la Ley 2/2004, de 25 de febrero, y de cuantas disposiciones de igual o inferior rango contradigan, se opongan o resulten incompatibles con lo dispuesto en esta ley. La aplicación de esta Disposición derogatoria debe entenderse sin perjuicio del régimen transitorio contenido en las Disposiciones transitorias primera y segunda del texto.

La **Disposición final primera** contiene una habilitación al Gobierno Vasco para la aprobación del futuro Estatuto de la Autoridad y la **segunda** elimina la vacatio legis para la entrada en vigor de la futura ley, previsión razonable toda vez que el contenido esencial del derecho fundamental, contenido en el Reglamento General de Protección de Datos, se encuentra en vigor desde mayo de 2018.

CONCLUSIÓN

La Agencia Vasca de Protección de datos valora muy positivamente el texto del Anteproyecto de ley sometido a informe. La norma proyectada, además de ser necesaria para adecuarse al nuevo marco normativo en esta materia, se concibe como una oportunidad para desarrollar e impulsar la protección de datos personales en esta Comunidad Autónoma, ampliando su ámbito de aplicación, y reforzando el papel de la Autoridad Vasca de Protección de Datos como garante de ese derecho fundamental.

Únicamente se propone modificar el título de la norma e incorporar al texto legal una previsión sobre la representación y defensa en pleito de la Autoridad, junto con las puntualizaciones señaladas a las Disposiciones Transitoria Segunda y Derogatoria del texto.

Vitoria-Gasteiz, 25 de marzo de 2022