

**MEMORIA DE ANÁLISIS DE IMPACTO NORMATIVO DEL ANTEPROYECTO DE LEY  
ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

**FICHA DEL RESUMEN EJECUTIVO**

<b>Ministerio/Órgano proponente</b>	Ministerio de Justicia	<b>Fecha</b>	10/11/2017
<b>Título de la norma</b>	<b>ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.</b>		
<b>Tipo de Memoria</b>	Normal <input checked="" type="checkbox"/> Abreviada <input type="checkbox"/>		
<b>OPORTUNIDAD DE LA PROPUESTA</b>			
<b>Situación que se regula</b>	Se regula el ejercicio del derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución.		
<b>Objetivos que se persiguen</b>	Se persigue adaptar y completar las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, Reglamento general de protección de datos (RGPD), aprobando a tal fin una nueva Ley Orgánica de Protección de Datos de carácter personal.		
<b>Principales alternativas consideradas</b>	a) Alternativa “cero”: Descartada por la inseguridad jurídica que generaría la convivencia formal del RGPD con la vigente LOPD, la cual habría de entenderse desplazada en la mayoría de sus previsiones como consecuencia del principio de primacía del Derecho de la Unión Europea.		

	b) Introducción de las necesarias adaptaciones del Reglamento Europeo.
<b>CONTENIDO Y ANÁLISIS JURÍDICO</b>	
<b>Tipo de norma</b>	Ley orgánica.
<b>Estructura de la norma</b>	<p>La ley consta de 78 artículos estructurados en nueve títulos, diecisiete disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y cinco finales. La parte articulada se divide así:</p> <p>Título I. Disposiciones generales. Artículos 1 a 3.</p> <p>Título II. Principios de protección de datos. Artículos 4 a 10.</p> <p>Título III. Derechos de las personas.</p> <p>Capítulo I. Transparencia e información. Artículo 11.</p> <p>Capítulo II. Ejercicio de los derechos. Artículos 12 a 18.</p> <p>Título IV. Disposiciones aplicables a tratamientos concretos. Artículos 19 a 27.</p> <p>Título V. Responsable y encargado del tratamiento.</p> <p>Capítulo I. Disposiciones generales. Medidas de responsabilidad activa. Artículos 28 a 32.</p> <p>Capítulo II. Encargado del tratamiento. Artículo 33.</p> <p>Capítulo III. Delegado de protección de datos. Artículos 34 a 37.</p> <p>Capítulo IV. Códigos de conducta y certificación. Artículos 38 y 39.</p> <p>Título VI. Transferencias internacionales de datos. Artículos 40 a 43.</p> <p>Título VII. Autoridades de protección de datos.</p> <p>Capítulo I. La Agencia Española de Protección de Datos.</p> <p>Sección 1ª. Disposiciones generales. Artículos 44 a 50.</p> <p>Sección 2ª. Potestades de investigación y planes de</p>

	<p>auditoría preventiva. Artículos 51 a 54.</p> <p>Sección 3ª. Otras potestades de la Agencia Española de Protección de Datos. Artículos 55 y 56.</p> <p>Capítulo II. Autoridades autonómicas de protección de datos.</p> <p>Sección 1ª. Disposiciones generales. Artículos 57 a 59.</p> <p>Sección 2ª. Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679. Artículos 60 a 62.</p> <p>Título VIII. Procedimiento en caso de reclamaciones tramitadas por la Agencia Española de Protección de Datos. Artículos 63 a 69.</p> <p>Título IX. Régimen sancionador. Artículos 70 a 78.</p>
<p><b>Informes recabados</b></p>	<p>Con carácter previo a la elaboración del borrador, la Secretaría General Técnica del Ministerio de Justicia solicitó a las Secretarías Generales Técnicas de los diferentes Departamentos Ministeriales que realizasen propuestas sobre su normativa sectorial. Han contestado o formulado observaciones los Ministerios que se indican a continuación:</p> <ul style="list-style-type: none"> <li>– MAEC (sin observaciones).</li> <li>– MAPM: Sec. G. Agricultura y Alimentación.</li> <li>– MECD: Sub. G. Propiedad Intelectual.</li> <li>– MEIC: I.S. Carlos III. C.N. Epidemiología.</li> <li>– MEIC: INE, Banco de España, C.N. Mercado de Valores.</li> <li>– MESS: SGT, SE Seguridad Social, Sec. G. Inmigración y Emigración.</li> <li>– MHFP.</li> <li>– MPRA: AEBOE, CNI.</li> <li>– MSSI: Sec. G. Sanidad y Consumo.</li> </ul> <p>Efectuada la consulta pública previa del art. 26.2 de la Ley del Gobierno, se recibieron observaciones de:</p> <ul style="list-style-type: none"> <li>– ADIGITAL.</li> <li>– AEB.</li> <li>– AMCHAM EU.</li> <li>– AMCHAM SPAIN.</li> <li>– AMETIC.</li> </ul>

- ANGECO.
- APEP.
- ASEDIE.
- ASIPRODAT.
- ASNEF-EQUIFAX.
- ASOCIACIÓN ESPAÑOLA DE STARTUPS.
- AUDEA.
- CAIXABANK.
- CECA.
- CEOE.
- C.O. GESTORES ADMINISTRATIVOS MADRID.
- C.P. INGENIEROS INFORMATICA ANDALUCÍA.
- C.G.C.O. FARMACÉUTICOS.
- DERECHOS ARCO.
- Despacho GERVÁS.
- Despacho HIGUERA.
- Despacho MARTÍNEZ.
- Despacho NAVARRO.
- Despacho PÉREZ.
- EXPERIAN-EQUIFAX.
- FUNDACIÓN ESYS.
- FUNDACIÓN FIDE.
- GOOGLE.
- HUAWEI.
- IAB.
- ISACA MADRID.
- ISMS FORUM SPAIN-DATA PRIVACY INSTITUTE.
- MICROSOFT.
- ORANGE.
- SIGACUS GESTIÓN.
- TELEFÓNICA.
- UNESPA.
- UNIVERSITAT BARCELONA.
- D. ELÍAS (Particular).
- GEMMA SMP (Particular).
- V. GIL (Particular).
- A. GUTIÉRREZ (Particular).
- J. IGLESIAS (Particular).
- E. ORDÁS (Particular).
- I. SÁNCHEZ (Particular).

El borrador fue sido aprobado por la Sección de Derecho Público de la Comisión General de Codificación en su

reunión del día 19 de mayo de 2017.

A continuación la Secretaría General Técnica del Ministerio de Justicia ha recabado los siguientes informes dentro del Departamento:

- Secretaría de Estado.
- Dirección General de los Registros y del Notariado.
- Abogacía del Estado.

Una vez elevado el anteproyecto a primera vuelta de Consejo de Ministros, a través de la Comisión General de Secretarios de Estado y Subsecretarios, se celebró el trámite de información pública (junio-julio 2017) a través del portal web del Ministerio de Justicia. Se recibieron alegaciones de:

- Angeco (Asociación Nacional de entidades de gestión de cobro)
- Pablo Fernández Burgueño socio de Abanlex abogados
- American Express Card España
- Antonio Gutiérrez Cardenete
- Antonio Sánchez Díaz
- Artico Consultores SL
- ACIE (Asociación de comercializadores independientes de energía)
- ADECOSE (Asociación española de correidurías de seguros)
- AMAT (Asociación de mutuas de accidentes de trabajo)
- Asociación de usuarios "AZOTE LEGAL"
- BAKER-MCKENZIE (Raúl Rubio Velázquez, clientes sector sanitario)
- Cámara de Comercio de León
- CCII (Consejo de Colegios de Ingeniería Informática)
- CECA
- Autocontrol (Asociación para la autoregulación de la comunicación comercial)
- Christian Hidalgo Nieto
- Colegio Médicos de Barcelona
- ICPM (Ilustre Colegio de Procuradores de Madrid)
- DAS SEGUROS (Asesoría Jurídica)
- Despacho Abogados Davara-Davara
- Digital ES (Asociación Española para la Digitalización)
- DISA Corporación petrolífera SA
- ASISA
- Écija

- Enatic (Asociación de expertos nacionales de la Abogacía)
- Samuel Parra, Privacidad en Internet SL
- Save The Children ( Eulalia Port)
- Farmaindustria
- COMPLIANZA SL (Isidorro Cantero)
- Grupo REPSOL SA
- IAB SPAIN
- IBERIA (Asesoría Jurídica)
- Fundación Protección de Datos (Jorge Badiola)
- Vidau Abogados (Luis Gervás de la Pisa)
- Mafpre
- MME, multinacionales marca España
- Pablo Fernández Burgueño
- Pantallas amigas
- Pedro Menchén Herreros (Estudio Abogados)
- Universidad Internacional de La Rioja (aportaciones estudiantes master universitario)
- Asociación de STARTUPS
- TARSYS (Consultoría)
- TELEFÓNICA ESPAÑA
- UNACC (Unión Nacional Cooperativas de Crédito)
- UNESPA
- Víctor Salgado
- EXPERIAN y ASNEF EQUIFAX
- EXPERIAN y ASNEF EQUIFAX Observaciones complementarias
- ADIGITAL (Asociación Española de la economía digital)
- AMCHAMSPAIN
- AEB (Asociación Española de la Banca)
- APEP (Asociación Profesional de Privacidad)
- ASEDIE (Asociación Multisectorial de la Información)
- AXESOR
- CEOE
- CGAE (Consejo General de la Abogacía Española)
- COIT (Colegio Oficial de Ingenieros de Telecomunicaciones)
- José Luis Falcón
- EDRI
- AMETIC
- AMI (Asociación medios de comunicación)
- ANEIMO (Asociación Española de Empresas de investigación de mercados y de la opinión)
- PRIBATUA (Asociación Vasca de Privacidad y

Seguridad de la información)

- ASNEF
- Coalición de Creadores e Industrias de Contenido
- Rosario García, Catedrática de Derecho Constitucional (Introducción)
- Rosario García (Continuación)
- Helvetia Seguros (Angel Luis Soto)
- Consejo General de Colegios Oficiales de Farmacéuticos)
- Solicitud del trámite de audiencia a sindicatos y grupos empresariales.
- Contestación de CC OO.

La propuesta ha sido informada por:

Informe de la Agencia Española de Protección de Datos (11/07/2017)

Informe del Ministerio de Defensa (11/07/2017)

Informe del Ministerio de Asuntos Exteriores y Cooperación (13/07/2017)

Informe del Consejo Fiscal (14/07/2017)

-Informe complementario de Fiscalía General del Estado, Unidad de Criminalidad Informática.

Informe del Ministerio de la Presidencia y para las Administraciones Territoriales (19/07/2017)

a) Informe DGRCCYEL

b) Informe CNI

c) Informe Agencia Estatal B.O.E.

Informe del Ministerio de Sanidad, Servicios Sociales e Igualdad (19/07/2017)

Informe del Ministerio de Educación, Cultura y Deporte (21/07/2017)

a) Informe del Gabinete de la Secretaría de Estado de Educación, Formación Profesional y Universidades.

b) Observaciones de la Biblioteca Nacional de España al Anteproyecto de Ley Orgánica de Protección de Datos de carácter personal.

Informe del Ministerio de Empleo y Seguridad Social (21/07/2017)

	<p>Oficio Secretaría General Técnica del Ministerio de Energía, Turismo y Agenda Digital (21/07/2017)</p> <p>a) Informe de la Subdirección General de Inspección General de los servicios y relaciones con los ciudadanos</p> <p>b) Informe de la Secretaría de Estado de telecomunicaciones y para la sociedad de la información</p> <p>c) Informe de la Secretaría de Estado para la sociedad de la información y Agencia Digital</p> <p>d) Informe de la Secretaría General Técnica del Ministerio de Energía, Turismo y Agenda Digital</p> <p>e) Informe de la Secretaría de Estado de Energía</p> <p>Informe del Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente (24/07/2017)</p> <p>Informe de la Autoridad Catalana de Protección de Datos (26/07/2017)</p> <p>Informes del Ministerio de Fomento (26/07/2017)</p> <p>a) Informe de la Secretaría General Técnica.</p> <p>b) Informe de la Dirección General de Marina Mercante.</p> <p>Informe de la Secretaría General Técnica del Ministerio del Interior (27/07/2017)</p> <p>Informe de la Secretaría General Técnica del Ministerio de Economía y Competitividad (27/07/2017)</p> <p>Aprobación previa del Ministro de Hacienda y Función Pública (31/07/2017).</p> <p>Informe del Consejo General Poder Judicial (01/08/2017).</p> <p>Informe de la Agencia Vasca de Protección de Datos (02/08/2017)</p> <p>Informe de la Secretaría General Técnica del Ministerio de Justicia.</p> <p>El anteproyecto se ha dictaminado por el Pleno del Consejo de Estado en fecha de 26 octubre de 2017.</p>
<p><b>Trámite de audiencia</b></p>	<p>En el proceso de estudio previo y preparación de este anteproyecto se han mantenido múltiples contactos con expertos del sector empresarial y de la abogacía, así como con colectivos o asociaciones relacionadas con el ámbito que se regula. El texto que se incluye en el anteproyecto ha sido elaborado en el seno de la Comisión General de la Codificación, en su condición de órgano consultivo superior del Ministro de Justicia, a través de la Ponencia creada</p>



	<p>mediante Orden y constituida por vocales permanentes de la Sección de Derecho Público, la Directora de la Agencia Española de Protección de Datos en su condición de vocal nato y representantes de la Agencia Española de Protección de Datos, y ha estado asistida por la Subdirección General de Política Legislativa de la Secretaría General Técnica.</p> <p>La Ponencia ha tenido en cuenta las cartas y documentos remitidos al Presidente de la Ponencia y de la Sección, a la Secretaría General de la Comisión General de Codificación, y a la Agencia Española de Protección de Datos (fundación ESYS, Colegio de Registradores de la Propiedad y Mercantiles de España, Ametic, AmCham UE, Coalición de creadores e industrias de contenidos).</p> <p>La Ponencia ha recibido en dos ocasiones a la Directora de la Agencia Vasca de Protección de Datos y a la Directora de la Autoridad Catalana de Protección de Datos y a sus respectivos equipos.</p> <p>Asimismo, la Ponencia ha tenido en cuenta las observaciones remitidas por las Secretarías Generales Técnicas y las recibidas con ocasión del trámite de consulta pública, según se ha expuesto más arriba.</p> <p>También se ha celebrado un trámite de información pública, con una participación representativa de múltiples sectores académicos, empresariales, sindicales y profesionales. Los escritos de observaciones recibidos han sido analizados, lo que ha dado lugar a cambios relevantes en el anteproyecto.</p>
<b>ANÁLISIS DE IMPACTOS</b>	
<b>ADECUACIÓN AL ORDEN DE COMPETENCIAS</b>	<p>La Ley se dicta al amparo de la competencia exclusiva del Estado en el artículo 149.1.1ª de la Constitución. El Título VII, la disposición adicional cuarta y la disposición transitoria tercera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.</p> <p>La modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, contenidas en la presente ley se amparan en la competencia</p>

	<p>exclusiva del Estado del artículo 149.1.6ª de legislación procesal, sin perjuicio de las necesarias especialidades que en este orden se deriven de las particularidades del derecho sustantivo de las Comunidades Autónomas, y cuyos títulos competenciales se encuentran ya en la norma objeto de modificación.</p>	
<p><b>IMPACTO ECONÓMICO Y PRESUPUESTARIO</b></p>	<p>Impacto presupuestario</p>	<p>La existencia de un régimen armonizado en toda la UE tendrá un efecto económico positivo como es la ubicación de empresas y operadores económicos en el territorio de la UE.</p> <p>El cumplimiento de la obligación de establecer el régimen de las Autoridades de control independientes va a requerir un esfuerzo presupuestario.</p>
	<p>Desde el punto de vista de las cargas administrativas</p>	<p><input type="checkbox"/> Supone una reducción de cargas administrativas.</p> <p><input type="checkbox"/> Incorpora nuevas cargas administrativas.</p> <p><input type="checkbox"/> no afecta a las cargas administrativas</p>
	<p>Desde el punto de vista de los presupuestos, la norma</p> <p><input checked="" type="checkbox"/> Afecta a los presupuestos de la Administración del Estado</p> <p><input checked="" type="checkbox"/> Afecta a los presupuestos de otras Administraciones Territoriales</p>	<p><input checked="" type="checkbox"/> implica un gasto</p> <p><input type="checkbox"/> implica un ingreso</p>

<b>IMPACTO DE GÉNERO</b>	La norma tiene un impacto de género	Negativo <input type="checkbox"/> Nulo <input checked="" type="checkbox"/> Positivo <input type="checkbox"/>

## **MEMORIA DE ANÁLISIS DE IMPACTO NORMATIVO DEL ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

Efectuada con arreglo a la Guía Metodológica, aprobada por Acuerdo del Consejo de Ministros de 11 de diciembre de 2009, tal y como prevé la Disposición adicional primera del Real Decreto 1083/2009, de 3 de julio, por el que se regula la MAIN.

Dado que se derivan impactos apreciables en los ámbitos señalados, de acuerdo con lo dispuesto en el artículo 3 del citado Real Decreto, procede realizar una **Memoria extensa** y no abreviada.

### **1) OPORTUNIDAD DE LA PROPUESTA:**

#### **A) Motivación.**

**La oportunidad de la propuesta tiene su origen inmediato en la necesidad de** cumplir con las obligaciones derivadas de la pertenencia de España a la Unión Europea, adaptando previsiones de la normativa comunitaria.

#### **B) Objetivos.**

En los últimos años de la pasada década fueron cada vez mayores los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. En este desarrollo resulta obligado recordar la adopción, en el seno de la Conferencia Internacional de autoridades de privacidad y protección de datos celebrada en Madrid en octubre de 2009, de los *“Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal”* (la llamada **“Declaración de Madrid”**) en que se sistematizaban los principios, derechos y obligaciones en materia de protección de datos de carácter personal, adaptándolos a la evolución producida como consecuencia del desarrollo de la sociedad de la información.

Los estándares fueron el germen de una nueva evolución en la regulación del derecho fundamental a la protección de datos. Así se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental, que interpreta no sólo lo dispuesto en la Directiva 95/46/CE sino también en el artículo

8 de la Carta. Baste citar las sentencias de 8 de abril de 2014 (asuntos C-293/12 y C-594/12, Digital Rights Ireland), 13 de mayo de 2014 (Asunto C 131/12, Google Spain, Google Inc v. AEPD, Costeja), 6 de octubre de 2015 (Asunto C 362/14, Schrems) o 21 de diciembre de 2016 (asuntos C-203/15 y C-698/15, Tele2).

El último hito en esta evolución tuvo lugar con la adopción el 27 de abril de 2016 del Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por la que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva 680/2016 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 a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo..

La presente Ley Orgánica tiene por objeto la adaptación del sistema normativo español a las disposiciones del Reglamento general de protección de datos, excluyendo la trasposición de la citada Directiva, que deberá llevarse a cabo mediante una Ley especial.<sup>1</sup>

### **B.1) Problemas que se pretenden solucionar con la nueva norma.**

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental recogido en el artículo 18.4 de la Constitución española. De esta manera nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos de carácter personal cuando en su artículo 18.4 dispuso que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*. Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno a partir de la aprobación de la Ley del Land de Hesse en 1973.

La **Sentencia del Tribunal Constitucional 94/1988** señaló ya que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y

---

<sup>1</sup> La directiva regula un régimen jurídico autónomo de protección en el tratamiento de datos personales.

Este régimen jurídico autónomo se aplica si se cumplen determinados requisitos en el tratamiento de los datos personales. Pero no es el régimen general con especialidades, sino un régimen diferenciado, ya que:

- a) el régimen jurídico general, que vendría constituido por el Reglamento, no se aplica con carácter supletorio a todo aquello no regulado en la Directiva.
- b) los dos regímenes se asientan sobre principios diferentes, básicamente en lo que al consentimiento se refiere, y otorgan derechos parcialmente coincidentes pero con contenido distinto.

sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención.

Por su parte, la **Sentencia del Tribunal Constitucional 292/2000**, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

En segundo lugar, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea; y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Actualmente dichos artículos se encuentran desarrollados en el Reglamento general de protección de datos de la Unión Europea que se configura como un marco normativo único para toda la Unión Europea en materia de protección de datos personales, garantizando de este modo un nivel de protección equivalente en todos los Estados miembros.

Anteriormente, a nivel europeo, la armonización se produjo con la adopción de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 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. Su objeto era asegurar que la garantía del derecho a la protección de datos de carácter personal no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a la previstas en la propia Directiva.

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la Directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución

tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. El Reglamento será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99.

## **B. 2. Necesidad y oportunidad de su aprobación.**

El Reglamento general de protección de datos procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. En concreto, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del Reglamento.

Asimismo, es preciso tener en cuenta que existen normas sectoriales específicas junto a la normativa general y horizontal en materia de protección de datos, la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y junto a la Agencia Española de Protección de Datos coexisten agencias en los territorios de las Comunidades Autónomas.

La adaptación al Reglamento general de protección de datos, requiere, en suma, la elaboración de una nueva Ley Orgánica que sustituya a la actual.

## **B.3. Objetivos de la norma.**

Los objetivos de la reforma proyectada deben ser examinados con relación a los siguientes aspectos:

1. Regulación del ejercicio del derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución.
2. Adaptación al Reglamento general de protección de datos para evitar contradicciones con la normativa interna y proceder a ejecutar las previsiones del Reglamento en los puntos que el mismo Reglamento habilita.

3. Introducción de mejoras concretas en relación a aspectos del ordenamiento jurídico español en la normativa general en materia de protección de datos.
4. Introducción de mejoras concretas en relación a aspectos del ordenamiento jurídico español en las normas sectoriales en materia de protección de datos.

#### **B. 4. Alternativas, regulatorias y no regulatorias.**

En virtud del artículo 288 del Tratado de Funcionamiento de la Unión Europea, el reglamento "tendrá un alcance general" y "será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". Se integra, pues, en los ordenamientos jurídicos nacionales a partir de su publicación en el Diario Oficial de la Unión Europea, desplegando su eficacia a partir de la fecha que él mismo fije o, a falta de ella, a los veinte días de su publicación (artículo 297 del citado tratado internacional). Como se ha señalado más atrás, el Reglamento general de protección de datos será plenamente aplicable a partir del 25 de mayo de 2018.

Dado que se trata de una norma no necesitada de incorporación mediante otra de naturaleza interna, presenta una clara vocación unificadora de los Derechos nacionales, tendente a excluir cualquier particularidad o diversidad interna en la materia por él regulada, al limitar la intervención de los Estados, en principio, a la aplicación material de la norma única europea, sin perjuicio de la labor de depuración normativa y de los eventuales desarrollos de los que aquella pueda ser objeto, y teniendo en cuenta lo que establece el considerando 8 del Reglamento general de protección de datos.

Así, no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Ambas cuestiones han de ser analizadas someramente por separado:

a) El principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico.

En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho europeo quede definitivamente eliminada "mediante disposiciones internas de carácter



obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse" (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia).

b) Los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de "desarrollo" o complemento del Derecho europeo.

Por tanto, la "alternativa cero" (esto es, no promover iniciativa alguna) ha sido descartada por inadecuada. Sin la aprobación de la norma que se tramita, la aplicación del RGPD el día 25 de mayo de 2018 generaría un escenario de inseguridad jurídica, en la que la norma europea directamente aplicable conviviría con la apariencia de vigencia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, pese a que muchas de sus previsiones habrían de entenderse desplazadas, que no derogadas, como consecuencia del principio de primacía del Derecho de la Unión Europea. Sin la depuración del ordenamiento jurídico a la que se aspira, quedaría gravemente mermado el principio de seguridad jurídica. Además, el anteproyecto resulta necesario para complementar el RGPD en aquellos aspectos que lo requieren, además de para hacer uso de las opciones que la disposición europea otorga a los Estados miembros.

Descartada –por las razones anteriores- dicha "alternativa cero", se aboga por el impuso de la ley orgánica imprescindible para la adaptación del Derecho interno al RGPD, que, por una parte, exige la depuración de todas aquellas disposiciones, incluidas las de rango legal, contrarias a su dicción y, por otra, incluye numerosas previsiones en que hay una autorización o una remisión a la normativa estatal, la cual ha de operar de complemento necesario para la plena efectividad del referido reglamento europeo. A grandes rasgos, de cara a afrontar la aplicación del RGPD a partir del 25 de mayo de 2018:

- La LOPD y sus normas de desarrollo deben ser revisadas y adaptadas al Reglamento Europeo.
- La AEPD debe desarrollar cuestiones concretas que el Reglamento Europeo remite a las Autoridades Nacionales de Control.
- Las Empresas deben revisar sus tratamientos de datos personales y adaptarlos a las exigencias del Reglamento Europeo.

El único Estado miembro que hasta ahora ha tramitado su ley de adaptación al Reglamento (UE) 2016/679 es Alemania. En Alemania existen leyes generales de protección de datos a nivel federal y de los Länder, así como

disposiciones de protección de datos específicas de cada sector. Esta estructura se mantendrá cuando el Reglamento (UE) 2016/679 se aplique directamente en mayo de 2018. En Alemania, el Reglamento (UE) 2016/679 requiere adecuar tanto la legislación general como la legislación sectorial de protección de datos a nivel federal y de los Länder. Mediante la Ley “Datenschutzanpassungs- und Umsetzungsgesetz - DSAnpUG-EU” adoptada por el Bundestag el 27 de abril de 2017 y aprobada por el Bundesrat el 12 de mayo de 2017, el Gobierno Federal Alemán introduce importantes modificaciones para adecuar el régimen general de la protección de datos al Reglamento (UE) 2016/679, al tiempo que transpone la Directiva (EU) 2016/680. Actualmente los ministerios competentes están preparando ajustes adicionales en función de su legislación sectorial.

## **2) CONTENIDO, ANÁLISIS JURÍDICO Y DESCRIPCIÓN DE LA TRAMITACIÓN:**

### **A) Contenido y análisis jurídico.**

El anteproyecto consta de setenta y ocho artículos distribuidos en ocho títulos.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la Ley Orgánica como desarrollo del derecho fundamental reconocido en el artículo 18.4 de la Constitución, a la vez que procede a adaptar al ordenamiento español el Reglamento general de protección de datos y completar sus disposiciones. Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues tras excluir del ámbito de aplicación de la Ley su tratamiento, se permite en el artículo 3 que los herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido que, por lo demás, se podrán incorporar a un registro, según se dispone en la disposición adicional séptima. El artículo 2 también excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas; mención especial requieren los tratamientos sometidos a la Directiva 680/2016 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 a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. En esta materia, como consecuencia del propio acervo de la Unión Europea, no serán aplicables las disposiciones del Reglamento, sino las de la legislación nacional que trasponga la mencionada Directiva. No obstante, a fin de evitar que dichos tratamientos queden huérfanos de una regulación específica en tanto no se lleve a cabo dicha trasposición, la disposición transitoria cuarta de la Ley, como excepción a su disposición derogatoria, deja vigente, exclusivamente para esos tratamientos, lo dispuesto en la Ley Orgánica 15/1999.

En el Título II, “Principios de protección de datos”, se establece que a efectos del Reglamento (UE) 2016/679, no serán imputables al responsable del tratamiento, siempre que éste haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, los datos personales que sean inexactos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador, También se recoge expresamente el deber de confidencialidad, se regulan garantías específicas y se aplica el principio de minimización de datos para entender desproporcionado el tratamiento de los datos por quien carezca de competencia. Dentro de lo que se viene denominando la “legitimación para el tratamiento”, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como “consentimiento tácito”, se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para cada una de ellas, y se fija la edad a partir de la cual el menor puede prestar su consentimiento en trece años para asimilar el sistema español al de otros Estados de nuestro entorno.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679 , cuando así lo prevea una norma de Derecho de la Unión Europea o una 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, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras se derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y sólo 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 reglamento europeo, cuando derive de una competencia atribuida por la ley. . Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas

categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de “listas negras” de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2 b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2 d) de la misma norma europea.

El Título III se dedica a los “Derechos de las personas” y se estructura en tres capítulos.

El Capítulo I, titulado “Transparencia e información”, adapta al derecho español a través del artículo 11 el principio de transparencia en el tratamiento del Reglamento, que regula el derecho de los afectados a ser informados acerca del tratamiento, se recoge la denominada “información por capas” ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las “cookies”), y se especifican las circunstancias que permiten que la información se pueda facilitar a través de una dirección electrónica.

El Capítulo II regula el “Ejercicio de los derechos”. Se hace uso en este capítulo de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. En las disposiciones generales del artículo 12 se prevé el ejercicio de los derechos por medio de un representante voluntario, que el afectado pueda conocer los medios puestos a su disposición para el ejercicio de sus derechos, o la posibilidad de que se ejerciten ante un encargado del tratamiento, dejando a salvo la aplicación de regímenes especiales, como son las normas reguladoras de determinados registros públicos. A continuación, la ley contempla los derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, derecho a la portabilidad y derecho de oposición.

En el Título IV se recogen “Disposiciones aplicables a tratamientos concretos”, incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquéllos respecto de los que el legislador establece una presunción iuris tantum de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos, se recogen otros, tales como la videovigilancia, los ficheros de

exclusión publicitaria o los sistemas de denuncias internas en el sector privado, en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1 e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que la ley se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento y el Título V de la ley orgánica, a cuyo anteproyecto se dedica esta memoria.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades la ley mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las disposiciones generales y medidas de responsabilidad activa, el régimen del encargado del tratamiento, la figura del delegado de protección de datos y los códigos de conducta y certificación.

Las medidas generales de responsabilidad activa con las que se inicia el Capítulo I exigen la ponderación del riesgo como aplicación de lo que se denomina “enfoque basado en el riesgo”, estableciendo los criterios que deberían ser tomados en consideración en el artículo 28.2, se regulan los supuestos de corresponsabilidad en el tratamiento exigiendo que la relación entre los distintos intervinientes se plasme en un documento escrito; se regula la figura del representante del responsable o encargado del tratamiento no establecido en la Unión Europea pero sometido al régimen del Reglamento conforme al artículo 3 del Reglamento (UE) 2016/679; se impone al sector público y a parte del sector privado la llevanza de un registro de operaciones de tratamiento; en el ámbito del sector público y de los sujetos enumerados en el artículo 77 se impone que el registro sea público bajo la denominación de “inventario de actividades de tratamiento”, sustituyendo de esta forma la obligación de dictar disposiciones de creación, modificación o supresión de ficheros. La obligación de bloqueo se recoge para diferenciarla de los derechos, y garantiza, a través del artículo 32, la adecuada aplicación y supervisión del cumplimiento de las normas de protección de datos.

En el Capítulo II, la regulación del encargado del tratamiento en relación con el responsable que establece el artículo 33 garantiza que en todo caso sea posible identificar al autor de la infracción, se prevé la transmisión y conservación de los datos cuando se suceden los encargados y en el ámbito del sector público

se permite que la designación de encargado del tratamiento pueda derivar de una norma.

Ya en el Capítulo III, la figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrán removerle, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Capítulo IV promueve la existencia de mecanismos de autorregulación tanto en el ámbito del sector público como del privado y, dentro de este último, estos sistemas podrán tener tanto un carácter sectorial como referirse a grupos de empresas o a una sola empresa. Igualmente, será posible la promoción de códigos de conducta por organismos o entidades que asuman funciones de supervisión y resolución extrajudicial de controversias. En todo caso, los organismos o entidades de supervisión deberán someterse a la evaluación de la autoridad de protección de datos. Se atribuye a la Entidad Nacional de Acreditación (ENAC) la función de acreditar a las entidades de certificación en los supuestos en que la competencia corresponda a la Agencia Española de Protección de Datos.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos. Su regulación, siguiendo el mandato del Reglamento (UE) 2016/679, se ha de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la Ley Orgánica regula en el Capítulo I el régimen de la Agencia Española de Protección de Datos y, en el Capítulo II, refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación y coordinación entre las autoridades de control.

El Reglamento (UE) 2016/679 inviste a las autoridades de control de “total independencia”. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, que se relaciona con el Gobierno a través del Ministerio de Justicia. Según se deriva de reiterada jurisprudencia del Tribunal de Justicia de la Unión Europea, la independencia excede de la meramente funcional para informar toda la actividad de las autoridades de control. La primera Sección, dedicada a las disposiciones generales, remite el Estatuto de la Agencia Española de Protección de Datos a desarrollo mediante real decreto y a continuación regula el régimen presupuestario, las funciones y potestades de la Agencia, su Presidente, el Consejo Consultivo y la publicidad de sus resoluciones. La segunda Sección se centra en las potestades de investigación y planes de auditoría preventiva, regulando el ámbito y personal competente, el deber de colaboración, el alcance de la actividad de investigación y los planes de auditoría preventiva. Otras potestades de la Agencia son las previstas en la tercera Sección, en concreto, las potestades de regulación y circulares de la Agencia Española de Protección de Datos y la acción exterior.

El Capítulo II se refiere a las autoridades autonómicas de protección de datos. Sus competencias se delimitan a partir de las establecidas en el artículo 41 de la Ley Orgánica 15/1999 y la doctrina emanada del Tribunal Constitucional, pero teniendo en cuenta que algunos estatutos de autonomía han especificado el ámbito competencial de dichas autoridades. Se prevén mecanismos de cooperación mediante el mantenimiento de encuentros periódicos y el intercambio de información, se mantiene el mecanismo establecido en el artículo 42 de la Ley Orgánica 15/1999 para los supuestos en los que la Agencia Española de Protección de Datos constata un incumplimiento por responsables o encargados del tratamiento sometidos a una autoridad autonómica, y se regula el mecanismo de coordinación para los casos en los que pudieran verse afectadas por el procedimiento de cooperación establecido en el Reglamento (UE) 2016/679.

El Título VIII regula el “Procedimientos en caso de posible vulneración de la normativa de protección de datos”. El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de “ventanilla única”, en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal. La ley orgánica se limita a regular el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; el plazo de tramitación de los

procedimientos y, en su caso, su suspensión; las actuaciones previas de investigación; y las medidas provisionales, entre las que destaca el bloqueo de los datos. Las especialidades del procedimiento se remiten a desarrollo reglamentario. La disposición adicional cuarta prevé la aplicación de la ley orgánica a los procedimientos que la Agencia Española de Protección de Datos haya de tramitar en el marco de otras leyes.

El régimen sancionador del Título IX parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación

En este marco, la Ley Orgánica procede a describir en los artículos 70 a 78, de la forma más detallada posible, las conductas típicas, manteniendo la distinción entre infracciones muy graves, graves y leves, a la vista de la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones afecta también a sus plazos de prescripción. La Ley Orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el Reglamento, en función de si el procedimiento se tramita exclusivamente por la Agencia o si se acude al procedimiento coordinado del artículo 60 del Reglamento.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. El artículo 76 de la Ley Orgánica aprovecha la cláusula residual del artículo 83.2 del Reglamento, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos. Por otro lado, el artículo 77 hace uso de la previsión del Reglamento que permite no imponer sanciones económicas al sector público, por lo que se aplica la sanción de apercibimiento y se publica la resolución en la página web de la Agencia Española de Protección de Datos. La prescripción de las sanciones se mantiene de forma coherente con los criterios previstos en la Ley 39/2015.

Al margen de las disposiciones adicionales que ya han sido mencionadas, la primera se refiere a las medidas de seguridad en el ámbito del sector público. En la actualidad, las medidas establecidas en el Esquema Nacional de Seguridad para garantizar la protección de los datos de carácter personal lo son por remisión al Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999. Dado que dicha norma es derogada por la Ley Orgánica será preciso que el Esquema amplíe el ámbito de las medidas que considere oportuno adoptar en relación con la seguridad de los datos a partir del enfoque de riesgo exigido por el Reglamento general de protección de datos.



La segunda disposición adicional, sobre protección de datos y transparencia y acceso a la información pública, clarifica el equilibrio teniendo en cuenta el artículo 86 del Reglamento (UE) 2016/679.

En la disposición adicional tercera se establecen normas sobre el cómputo de los plazos, similares a las previstas en la Ley 39/2015, tratando de establecer un régimen uniforme para los sectores público y privado. Como peculiaridad, se establece el modo de cómputo del plazo por semanas, toda vez que el mismo ha de ser recogido por la Ley al venir previstos cómputos de dicha naturaleza en el Reglamento general de protección de datos. La inclusión de esta disposición se hace necesaria, dado que se pretende unificar el cómputo de los plazos con independencia de la naturaleza jurídico pública o jurídico privada de los responsables o encargados del tratamiento.

La disposición adicional cuarta se refiere al procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.

La disposición adicional quinta se refiere a la autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencias internacionales de datos. Prevé que, cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. La concesión de dicha autorización requerirá del previo planteamiento de una cuestión prejudicial de validez en los términos del artículo 267 del TFUE, y que el TJUE declare inválida la decisión de la Comisión Europea.

Esta medida tiene su fundamento en la sentencia del Tribunal de Justicia de la Unión de 6 de octubre de 2015 (Asunto C 362/14, Schrems); que justamente se trataba de una transferencia internacional amparada en una decisión de adecuación de la Comisión Europea.

Debe tenerse en cuenta el párrafo 65 de la citada sentencia que señala *que “corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta”*. Así, y a raíz del informe del Consejo del Poder Judicial se introduce la disposición final cuarta de modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, con el objeto de regular un proceso especial respecto a esta cuestión.

La disposición adicional sexta reconoce expresamente el régimen regulador de los registros de apoyo a la Administración de Justicia, recogido actualmente en el Real Decreto 95/2009, de 6 de febrero, como base legal para el tratamiento de datos relacionados con infracciones penales y condenas y medidas de seguridad.

La disposición adicional séptima contempla el acceso a contenidos de personas fallecidas, regulando las denominadas instrucciones relacionadas con los servicios de la sociedad de la información para el caso de fallecimiento. En el marco de la sociedad actual es creciente la información que los interesados facilitan a prestadores de servicios de la sociedad de la información. No solamente con el ánimo de hacerla pública en un ámbito sometido a mayores o menores restricciones, como ocurre, por ejemplo, con la información incorporada a redes sociales o plataformas de intercambio de archivos, sino por otros muchos y variados motivos, entre los que reviste gran importancia el almacenamiento de la información por tales prestadores, como sucede en caso de contratación de servicios de computación en nube. Los derechos relacionados con el uso y conservación de esta información pueden incluso ser una parte no despreciable del caudal relicto en caso de fallecimiento. Por este motivo, se hace necesario establecer una normativa mínima que garantice al titular de la información la posibilidad de disponer de ella, tanto en lo que afecte a sus propios datos de carácter personal como en lo que respeta al resto de las informaciones cuando se haya hecho uso de estos servicios. La Ley Orgánica establece en este punto un sistema que en parte puede asimilarse al de las instrucciones previas en el ámbito sanitario: el interesado podrá incorporar en un documento de instrucciones su manifestación de voluntad en lo que respecta al uso y destino de sus datos, documentos o ficheros, si opta por su conservación, destrucción o portabilidad, así como por el mantenimiento o cancelación de sus cuentas, pudiendo designar a una persona para que ejecute sus instrucciones. Las instrucciones se podrán incorporar a un registro, para cuya creación y regulación se habilita al Gobierno y que sólo será accesible por terceros en caso de fallecimiento. Además sólo el designado y, en su defecto, los herederos del difunto podrán acceder al contenido mismo de las instrucciones para poder dar cumplimiento a la voluntad del fallecido y ejercer por él los derechos que le otorga el ordenamiento jurídico.

La incorporación de deudas a sistemas de información crediticia figura en la disposición adicional octava, que introduce una cuantía que podrá ser actualizada reglamentariamente. Las siguientes disposiciones adicionales regulan ~~la contratación centralizada de la Agencia Española de Protección de Datos,~~ la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos, la potestad de verificación de las Administraciones Públicas, el no incremento de gasto, el tratamiento de datos de carácter personal en relación con la notificación de incidentes de seguridad, las comunicaciones de datos por los sujetos enumerados en el artículo 77.1, la privacidad en las comunicaciones electrónicas, las disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público, las

transferencias internacionales de datos tributarios, así como la vigencia de las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, para clarificar que siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas..

De conformidad con la disposición adicional decimoséptima, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional decimoséptima, las Administraciones tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el art. 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

En lo que atañe al régimen transitorio, la primera disposición transitoria declara expresamente vigente el estatuto de la Agencia española de Protección de Datos, aprobado por Real decreto 428/1994 en cuanto no se oponga a la Ley Orgánica.

La disposición transitoria segunda prevé la adaptación en el plazo de un año de los códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre.

La disposición transitoria tercera establece el régimen transitorio aplicable a los procedimientos, que se someterán a la legislación anterior no sólo cuando ya se hubiese dictado acuerdo de inicio en el momento de entrada en vigor de la Ley Orgánica, sino también en caso de que se iniciado respecto de los mismo actuaciones previas de investigación con anterioridad a esa fecha. Ello se debe al especial régimen procedimental derivado de la aplicación del procedimiento coordinado previsto en el artículo 60 del Reglamento general de protección de datos, que exigiría, con anterioridad incluso a la realización de esas actuaciones, un acuerdo para la determinación de la autoridad del establecimiento principal.

Asimismo, la disposición transitoria cuarta

señala que aun cuando se deroga la Ley Orgánica 15/1999 y sus disposiciones de desarrollo, dicha Ley será de aplicación a los tratamientos que se llevase a cabo en el marco de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales en tanto no entre en vigor la norma que trasponga al ordenamiento español la Directiva (UE) 2016/680, reguladora de esos tratamientos. Por su parte, la transitoria sexta recoge una previsión para los contratos de encargado de tratamiento suscritos con anterioridad al 25 de mayo de 2018.

La disposición transitoria quinta se refiere al mantenimiento de la vigencia de contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto la Ley Orgánica 15/1999 hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado de forma indefinida, hasta transcurridos cuatro años desde la citada fecha.

La disposición transitoria sexta hace innecesario recabar nuevamente el consentimiento dado con anterioridad a la aplicación de la norma europea si la forma en que se otorgó se ajusta a las condiciones del Reglamento (UE) 2016/679, de acuerdo con lo que se prevé en su considerando 171.

A continuación de la disposición derogatoria única figuran las disposiciones finales sobre la naturaleza de la ley y los preceptos con carácter de ley ordinaria y título competencial.

La disposición final tercera modifica la Ley de Enjuiciamiento Civil, habilitando la intervención de la Agencia Española de Protección de Datos, la Comisión Europea, y las autoridades autonómicas de protección de datos a intervenir como *amicus curiae en el proceso civil*, mediante la inclusión de un nuevo apartado 3 en el artículo 15 bis que ya preveía esta figura en materia de defensa de la competencia

La disposición final cuarta modifica la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, introduciendo un nuevo artículo 122 ter, que regula específicamente el procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos y añadiendo un nuevo apartado en sus artículos 10, 11 y 12, para atribuir la competencia para la citada autorización, respectivamente a los Tribunales Superiores de Justicia de las Comunidades Autónomas, a la Audiencia Nacional y al Tribunal Supremo, según sea solicitada por la autoridad de protección de datos de una Comunidad Autónoma, la AEPD o el Consejo General del Poder Judicial.

Analizado el Reglamento y la propia jurisprudencia del TJUE (en el citado asunto Schrems se trataba de un supuesto del ámbito contencioso-administrativo)

se ha llegado a la conclusión que la única modificación precisa es la relativa a permitir que las autoridades de control puedan participar en el proceso como *amicus curiae*.

Dicha participación tendrá lugar, de oficio o a instancia del propio órgano judicial, en procesos en los que la pretensión afecte sustancialmente a la configuración del derecho fundamental a la protección de datos.

En línea con lo anterior, y como ya se dijo anteriormente, a raíz del informe del Consejo del Poder Judicial se introduce la disposición final cuarta de modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, que introduce un nuevo artículo 122 ter, con un procedimiento de autorización judicial para declarar la vulneración del Derecho europeo por una decisión de la Comisión Europea en materia de transferencia internacional de datos, con el objeto de regular un especialidad procesal respecto a esta cuestión.

Finalmente, la disposición final quinta regula la entrada en vigor para coincidir con la aplicación del Reglamento (UE) 2016/679.

Cabe concluir este análisis destacando las explicaciones sobre el texto que proporciona el informe de la Agencia Española de Protección de Datos, el cual incluye un estudio en profundidad de la justificación de las distintas opciones reflejadas en el anteproyecto.

## **B) Tramitación.**

- I. Con carácter previo a la redacción del borrador se celebró una reunión el día 7 de octubre de 2016 en la que se solicitó a los a los Departamentos Ministeriales que realizaran un análisis de la normativa sectorial que se podría ver afectada por el Reglamento general de protección de datos, de cara a su posible modificación. La Secretaría General Técnica del Ministerio de Justicia solicitó a las demás Secretarías Generales Técnicas propuestas concretas mediante los correos electrónicos remitidos los días 23 de noviembre y 20 de diciembre de 2016. Han contestado o formulado observaciones los Ministerios que se indican a continuación:<sup>2</sup>
  - Ministerio de Asuntos Exteriores y de Cooperación (MAEC): sin observaciones. 22/12/2016.
  - Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente (MAPM): Secretaría General de Agricultura y Alimentación. 20/12/2016.

---

<sup>2</sup> Como anexo nº 1 se incorpora un cuadro con el resumen de las observaciones recibidas.

- Ministerio de Educación, Cultura y Deporte (MECD): Subdirección General de Propiedad Intelectual. 11/01/2017.
- Ministerio de Economía, Industria y Competitividad (MEIC): Instituto de Salud Carlos III. Centro Nacional de Epidemiología. 13/12/2016.
- Ministerio de Economía, Industria y Competitividad (MEIC): Instituto Nacional de Estadística, Banco de España, Comisión Nacional del Mercado de Valores. 27/01/2017.
- Ministerio de Empleo y Seguridad Social (MESS): Secretaría General Técnica, Secretaría de Estado de la Seguridad Social, Secretaría General de Inmigración y Emigración. 24/11/2016.
- Ministerio de Hacienda y Función Pública (MHFP). 10/01/2017.
- Ministerio de la Presidencia y para las Administraciones Territoriales (MPRA): Agencia Estatal Boletín Oficial del Estado. 30/01/2017.
- Ministerio de la Presidencia y para las Administraciones Territoriales (MPRA): Centro Nacional de Inteligencia. 28/02/2017.
- Ministerio de Sanidad, Servicios Sociales e Igualdad (MSSI): Secretaría General de Sanidad y Consumo. 20/12/2016.

II. Se ha efectuado la consulta pública previa del art. 26.2 de la Ley del Gobierno en el portal web del Ministerio de Justicia del 07/02/2017 al 28/02/2017. Se recibieron informes de: <sup>3</sup>

- ADIGITAL. 28/02/2017.
- AEB. 28/02/2017.
- AMCHAM EU. 13/02/2017.
- AMCHAM SPAIN. 27/02/2017.
- AMETIC. 28/02/2017.
- ANGECO. 27/02/2017.
- APEP. 28/02/2017.
- ASEDIE. 28/02/2017.
- ASIPRODAT. 28/02/2017.
- ASNEF-EQUIFAX. 28/02/2017.
- ASOCIACIÓN ESPAÑOLA DE STARTUPS. 27/02/2017.
- AUDEA. 27/02/2017.
- CAIXABANK. 28/02/2017.
- CECA. 28/02/2017.
- CEOE. 28/02/2017.
- C.O. GESTORES ADMINISTRATIVOS MADRID. 27/02/2017.
- C.P. INGENIEROS INFORMATICA ANDALUCÍA. 10/02/2017.
- C.G.C.O. FARMACÉUTICOS. 20/02/2017.
- DERECHOS ARCO. 28/02/2017.
- Despacho GERVÁS. 06/02/2017.
- Despacho HIGUERA. 28/02/2017.

---

<sup>3</sup> Como anexo nº 2 se incorpora un cuadro con el resumen de las principales observaciones recibidas (art. 26.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno).

- Despacho MARTÍNEZ. 28/02/2017.
- Despacho NAVARRO. 27/02/2017.
- Despacho PÉREZ. 15/02/2017.
- EXPERIAN-EQUIFAX. 28/02/2017.
- FUNDACIÓN ESYS. 27/02/2017.
- FUNDACIÓN FIDE. 28/02/2017.
- GOOGLE. 27/02/2017.
- HUAWEI. 28/02/2017.
- IAB. 28/02/2017.
- ISACA MADRID. 07/03/2017.
- ISMS FORUM SPAIN-DATA PRIVACY INSTITUTE. 27/02/2017.
- MICROSOFT. 28/02/2017.
- ORANGE. 28/02/2017.
- SIGACUS GESTIÓN. 27/02/2017. 28/02/2017.
- TELEFÓNICA. 01/03/2017.
- UNESPA. 02/03/2017.
- UNIVERSITAT BARCELONA. 28/02/2017.
- D. ELÍAS (Particular). 09/02/2017.
- GEMMA SMP (Particular). 28/02/2017.
- V. GIL (Particular). 28/02/2017.
- A. GUTIÉRREZ (Particular). 22/02/2017.
- J. IGLESIAS (Particular). 14/02/2017.
- E. ORDÁS (Particular). 28/02/2017.
- I. SÁNCHEZ (Particular). 28/02/2017.

III. El borrador del que partió la tramitación del anteproyecto fue elaborado en el seno de la Comisión General de la Codificación, en su condición de órgano consultivo superior del Ministro de Justicia, a través de la Ponencia creada mediante Orden y constituida por vocales permanentes de la Sección de Derecho Público, la Directora de la Agencia Española de Protección de Datos en su condición de vocal nato y representantes de la Agencia Española de Protección de Datos, y ha estado asistida por la Subdirección General de Política Legislativa de la Secretaría General Técnica.

Además de las observaciones y propuestas antes expuestas, la Ponencia ha tenido en cuenta los comentarios recibidos por medio de:

- Carta dirigida al Presidente de la Ponencia y de la Sección por el Presidente de la Fundación ESYS, incluyendo las propuestas de Endesa, Gas Natural-Fenosa, Securitas, Prosegur y Telefónica y el apoyo del Banco Santander.
- Carta dirigida al Presidente de la Ponencia y de la Sección por el Decano-Presidente del Colegio de Registradores de la Propiedad y Mercantiles de España, para ofrecer su colaboración.
- Carta dirigida al Presidente de la Ponencia y de la Sección por el Director General de Ametic.

- Cartas recibidas en la Secretaría General de la Comisión General de Codificación por parte de la Cámara de Comercio de Estados Unidos en Europa y documento titulado “Recomendaciones de la AmCham UE sobre la implementación del GDPR. Garantizar un marco de protección de datos equilibrado y prospectivo en Europa”.
- Documento enviado a la Agencia Española de Protección de Datos por “La coalición de creadores e industrias de contenidos” en relación con la “Necesaria modificación de la Ley Orgánica de Protección de Datos”.

La Ponencia ha recibido a la Directora de la Agencia Vasca de Protección de Datos y a la Directora de la Autoridad Catalana de Protección de Datos y a sus respectivos equipos según se indica a continuación:

- 6 de febrero de 2017. Ambas Directoras.
- 8 de marzo de 2017. Directora de la Agencia Vasca de Protección de Datos.
- 10 de marzo de 2017. Directora de la Autoridad Catalana de Protección de Datos.

El borrador fue aprobado por la Sección de Derecho Público de la Comisión General de Codificación en su reunión celebrada el día 19 de mayo de 2017.

**IV.** En el seno del Ministerio de Justicia se han recabado los siguientes informes:

- Informe de la Secretaría de Estado, de 28 de mayo de 2017.
- Informe de la Dirección General de los Registros y del Notariado, de 29 de mayo de 2017.
- Informe de la Abogacía General del Estado, remitido el día 2 de junio de 2017.

**V.** Por su parte, una vez elevado el anteproyecto a primera vuelta de Consejo de Ministros, a través de la Comisión General de Secretarios de Estado y Subsecretarios, se celebró el trámite de información pública (entre el 28 de junio y el 19 de julio de 2017) a través del portal web del Ministerio de Justicia, con la siguiente participación<sup>4</sup>:

- Angeco (Asociación Nacional de entidades de gestión de cobro)
- Pablo Fernández Burgueño socio de Abanlex abogados
- American Express Card España
- Antonio Gutiérrez Cardenete
- Antonio Sánchez Díaz
- Artico Consultores SL
- ACIE (Asociación de comercializadores independientes de energía)

---

<sup>4</sup> Como anexo nº 3 se incorpora un cuadro con el resumen de las principales observaciones recibidas (art. 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno).



- ADECOSE (Asociación española de correidurías de seguros)
- AMAT (Asociación de mutuas de accidentes de trabajo)
- Asociación de usuarios “AZOTE LEGAL”
- BAKER-MCKENZIE (Raúl Rubio Velázquez, clientes sector sanitario)
- Cámara de Comercio de León
- CCII (Consejo de Colegios de Ingeniería Informática)
- CECA
- Autocontrol (Asociación para la autoregulación de la comunicación comercial)
- Christian Hidalgo Nieto
- Colegio Médicos de Barcelona
- ICPM (Ilustre Colegio de Procuradores de Madrid)
- DAS SEGUROS (Asesoría Jurídica)
- Despacho Abogados Davara-Davara
- Digital ES (Asociación Española para la Digitalización)
- DISA Corporación petrolífera SA
- ASISA
- Écija
- Enatic (Asociación de expertos nacionales de la Abogacía)
- Samuel Parra, Privacidad en Internet SL
- Save The Children ( Eulalia Port)
- Farmaindustria
- COMPLIANZA SL (Isidorro Cantero)
- Grupo REPSOL SA
- IAB SPAIN
- IBERIA (Asesoría Jurídica)
- Fundación Protección de Datos (Jorge Badiola)
- Vidau Abogados (Luis Gervás de la Pisa)
- Mafpre
- MME, multinacionales marca España
- Pablo Fernández Burgueño
- Pantallas amigas
- Pedro Menchén Herreros (Estudio Abogados)
- Universidad Internacional de La Rioja (aportaciones estudiantes master universitario)
- Asociación de STARTUPS
- TARSYS (Consultoría)
- TELEFÓNICA ESPAÑA
- UNACC (Unión Nacional Cooperativas de Crédito)
- UNESPA
- Víctor Salgado
- EXPERIAN y ASNEF EQUIFAX
- EXPERIAN y ASNEF EQUIFAX Observaciones complementarias
- ADIGITAL (Asociación Española de la economía digital)
- AMCHAMSPAIN
- AEB (Asociación Española de la Banca)

- APEP (Asociación Profesional de Privacidad)
- ASEDIE (Asociación Multisectorial de la Información)
- AXESOR
- CEOE
- CGAE (Consejo General de la Abogacía Española)
- COIT (Colegio Oficial de Ingenieros de Telecomunicaciones)
- José Luis Falcón
- EDRI
- AMETIC
- AMI (Asociación medios de comunicación)
- ANEIMO (Asociación Española de Empresas de investigación de mercados y de la opinión)
- PRIBATUA (Asociación Vasca de Privacidad y Seguridad de la información)
- ASNEF
- Coalición de Creadores e Industrias de Contenido
- Rosario García, Catedrática de Derecho Constitucional (Introducción)
- Rosario García (Continuación)
- Helvetia Seguros (Angel Luis Soto)
- Consejo General de Colegios Oficiales de Farmacéuticos)
- Solicitud del trámite de audiencia a sindicatos y grupos empresariales.
- Contestación de CC OO.

**VI. El Anteproyecto ha sido informado por<sup>5</sup>:**

- Informe de la Agencia Española de Protección de Datos (11/07/2017).
- Informe del Ministerio de Defensa (11/07/2017)
- Informe del Ministerio de Asuntos Exteriores y Cooperación (13/07/2017)
- Informe del Consejo Fiscal (14/07/2017)
  - Informe complementario de Fiscalía General del Estado, Unidad de Criminalidad Informática.
- Informe del Ministerio de la Presidencia y para las Administraciones Territoriales (19/07/2017)
  - Informe DGRCCYEL
  - Informe CNI
  - Informe Agencia Estatal B.O.E.
- Informe del Ministerio de Sanidad, Servicios Sociales e Igualdad (19/07/2017)
- Informe del Ministerio de Educación, Cultura y Deporte (21/07/2017)
  - Informe del Gabinete de la Secretaría de Estado de Educación, Formación Profesional y Universidades.
  - Observaciones de la Biblioteca Nacional de España al Anteproyecto de Ley Orgánica de Protección de Datos de carácter personal.
- Informe del Ministerio de Empleo y Seguridad Social (21/07/2017)

---

<sup>5</sup> Como anexo nº 4 se incorpora un cuadro con el resumen de las principales observaciones recibidas en los informes preceptivos (art. 26.5 de la Ley 50/1997, de 27 de noviembre, del Gobierno, y otros).

- Oficio Secretaría General Técnica del Ministerio de Energía, Turismo y Agenda Digital (21/07/2017):
  - Informe de la Subdirección General de Inspección General de los servicios y relaciones con los ciudadanos
  - Informe de la Secretaría de Estado de telecomunicaciones y para la sociedad de la información
  - Informe de la Secretaría de Estado para la sociedad de la información y Agencia Digital
  - Informe de la Secretaría General Técnica del Ministerio de Energía, Turismo y Agenda Digital
  - Informe de la Secretaría de Estado de Energía
- Informe del Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente (24/07/2017)
- Informe de la Autoridad Catalana de Protección de Datos (26/07/2017)
- Informes del Ministerio de Fomento (26/07/2017)
  - Informe de la Secretaría General Técnica.
  - Informe de la Dirección General de Marina Mercante.
- Informe de la Secretaría General Técnica del Ministerio del Interior (27/07/2017)
- Informe de la Secretaría General Técnica del Ministerio de Economía y Competitividad (27/07/2017)
- Aprobación previa del Ministro de Hacienda y Función Pública (31/07/2017).
- Informe del Consejo General Poder Judicial (01/08/2017).
- Informe de la Agencia Vasca de Protección de Datos (02/08/2017).
- Informe de la Secretaría General Técnica del Ministerio de Justicia.

Finalmente, el Anteproyecto ha sido sometido a **dictamen del Consejo de Estado. El Pleno del Alto Cuerpo Consultivo ha evacuado el 26 de octubre de 2017 su dictamen.** En el correspondiente anexo se analiza el tratamiento dado a las observaciones formuladas en este trámite.

### **3) ANÁLISIS DE IMPACTOS:**

#### **A) Consideraciones generales.**

#### **B) Adecuación al orden de distribución de competencias. Título competencial.**

El presente anteproyecto de Ley se dicta al amparo de la competencia exclusiva del Estado prevista en el artículo 149.1.1ª de la Constitución respecto de

“La regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales”.

El Título VII, la disposición adicional cuarta y la disposición transitoria tercera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

La modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, contenidas en la presente ley se amparan en la competencia exclusiva del Estado del artículo 149.1.6ª de legislación procesal, sin perjuicio de las necesarias especialidades que en este orden se deriven de las particularidades del derecho sustantivo de las Comunidades Autónomas. No se considera procedente la mención de este título en la disposición final segunda del anteproyecto, puesto que se trata del que ya ampara las normas objeto de modificación.

El Tribunal Constitucional, en su Sentencia 290/2000, ha declarado que la materia objeto de regulación se encuadra a efectos competenciales en el título relativo a "la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales" (artículo 149.1.1º de la Constitución), que es competencia exclusiva del Estado. Este artículo hay que ponerlo en relación con el artículo 18.4 de la Constitución, el cual establece que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Como señala expresamente el Tribunal Constitucional (SSTC 5/1981, de 13 de febrero, y 6/1982, de 22 de febrero), en materia de derechos fundamentales la Constitución no se ha limitado a reservar su desarrollo normativo a leyes orgánicas (artículo 81), sino que ha dispuesto además que todos los españoles tengan los mismos derechos y obligaciones en cualquier parte del territorio nacional (artículo 139) y, para asegurar que así sea, ha reservado al Estado la competencia exclusiva para "la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales" (artículo 149.1.1ª).

El Tribunal Constitucional ha establecido, en la Sentencia 173/1998, que "la reserva de ley orgánica del artículo 81.1 CE no contiene, en puridad, ningún título competencial habilitante a favor del Estado. Así lo señaló entre otras la STC 137/1986 (FJ. 3º 8), con cita de otras precedentes, destacando que en este punto rige el «criterio general de que, en el Estado de autonomías territoriales, las normas entronizadoras de reservas a determinadas fuentes no son, sólo por ello, atributivas de competencia a un cierto ente (STC 37/1981, FJ. 2º)". Sin embargo, continua la citada Sentencia "siendo cierto que la reserva de Ley Orgánica no

supone atribución de ningún título competencial, no lo es menos que, en virtud del artículo 81.1 CE, sólo el Estado puede dictar esta forma de leyes en desarrollo de los derechos fundamentales y libertades públicas y que las Comunidades Autónomas al ejercer sus competencias deben respetar el contenido de las mismas so pena de incurrir en un vicio de inconstitucionalidad por vulneración del artículo 81.1 CE” (FJ. 7).

En cualquier caso, el Tribunal Constitucional considera que el artículo 149.1.1ª "constituye un título competencial autónomo, positivo o habilitante, constreñido al ámbito normativo, lo que permite al Estado una "regulación", aunque limitada a las condiciones básicas que garanticen la igualdad, que no el diseño completo y acabado de su régimen jurídico” (STC 61/1997, FJ. 7). Además, la STC 290/2000, afirma en su FJ. 14, que “junto a la normación como aspecto esencial del artículo 149.1.1 CE las regulaciones estatales dictadas al amparo de este precepto también pueden contener, cuando sea imprescindible para garantizar la eficacia del derecho fundamental o la igualdad de todos los españoles en su disfrute, una dimensión institucional (...) De lo anterior se desprende, pues, que la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (artículo 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas «ex» artículo 149.1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales”.

El contenido del título competencial contemplado en el artículo 149.1.1ª de la Constitución se ha definido a través de diversos pronunciamientos del Tribunal Constitucional; especialmente significativa en el caso que nos ocupa resulta la citada STC 290/2000, que determina que “... es significativo que el constituyente haya querido introducir mediante la cláusula del artículo 149.1.1 CE la garantía de los derechos fundamentales en el pórtico del reparto competencial y, a este fin, que haya apoderado al Estado para asegurar su respeto en todo el territorio nacional mediante el establecimiento de aquellas «condiciones básicas» que hagan posible que el disfrute de tales derechos sea igual para todos los españoles. Imponiendo así un límite a las potestades de las Comunidades Autónomas en aquellas materias donde éstas ostenten un título competencial. Y si bien el alcance del artículo 149.1.1 CE es «esencialmente normativo», como hemos dicho en la reciente STC 208/1999, de 15 de noviembre, F.J. 6, por referirse a «la regulación» de esas condiciones básicas, cabe observar, sin embargo, que ninguna calificación adicional se ha agregado por el constituyente respecto a la naturaleza de tales condiciones que pueda restringir su alcance. De lo que se desprende, en definitiva, que junto a la normación como aspecto esencial del artículo 149.1.1 CE las regulaciones estatales dictadas al amparo de este precepto también pueden contener, cuando sea imprescindible para garantizar la eficacia del derecho fundamental o la igualdad de todos los españoles en su disfrute, una dimensión institucional (...) A lo que cabe agregar que no es infrecuente que la Ley Orgánica

que lo ha llevado a cabo haya establecido un órgano al que encomienda la ejecución de sus preceptos(...).

De lo anterior se desprende, pues, que la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (artículo 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas ex artículo 149.1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales”.

#### **a) Garantías normativas.**

El alcance de las competencias normativas estatales amparadas en el artículo 149.1.1ª de la Constitución se ha definido a través de diversos pronunciamientos del Tribunal Constitucional desde una doble perspectiva: negativa y positiva.

Respecto de la delimitación negativa de dicho título, la STC 61/1997 afirma que el mismo “no se puede identificar con el contenido derivado de otros preceptos constitucionales, (...) que son presupuestos o límites, pero no títulos competenciales” (...).

El Tribunal Constitucional viene señalando reiteradamente "que "condiciones básicas" no es sinónimo de "legislación básica", "bases" o "normas básicas". El artículo 149.1.1º CE, en efecto, no ha atribuido al Estado la fijación de las condiciones básicas para garantizar la igualdad en el ejercicio de los derechos y libertades constitucionales, sino sólo el establecimiento -eso sí, entero- de aquellas condiciones básicas que tiendan a garantizar la igualdad” (...) El Estado tiene la competencia exclusiva para incidir sobre los derechos y deberes constitucionales desde una concreta perspectiva, la de la garantía de la igualdad en las posiciones jurídicas fundamentales, dimensión que no es, en rigor, susceptible de desarrollo como si de unas bases se tratara; será luego el legislador competente, estatal y autonómico, el que respetando tales condiciones básicas establezca su régimen jurídico, de acuerdo con el orden constitucional de competencias” (STC 61/1997, de 20 de marzo, FJ. 7). En este mismo sentido se señala que “este Tribunal ha afirmado reiteradamente que las «condiciones básicas» no son normas básicas susceptibles de desarrollo por las Comunidades Autónomas" (SSTC 61/1997, de 20 de marzo, F. 7 a), 37/2002, de 14 de febrero, F. 12 y 133/2006, FJ. 9).

En lo que se refiere a la delimitación positiva de esta competencia estatal, la misma STC 61/1997 mantiene que “(...), las condiciones básicas que garanticen la igualdad se predicen de los derechos y deberes constitucionales en sí mismos considerados, no de los sectores materiales en los que éstos se insertan y, en

consecuencia, el artículo 149.1.1º CE sólo presta cobertura a aquellas condiciones que guarden una estrecha relación, directa e inmediata, con los derechos que la Constitución reconoce. De lo contrario (...) quedaría desbordado el ámbito y sentido del artículo 149.1.1º CE, que no puede operar como una especie de título horizontal, capaz de introducirse en cualquier materia o sector del ordenamiento por el mero hecho de que pudieran ser reconducibles, siquiera sea remotamente, hacia un derecho o deber constitucional". Esta misma doctrina ha sido reiterada por STC 228/2003, de 18 de diciembre, F. 10, y las resoluciones allí citadas.

Por su parte, el FJ. 8 de la STC 61/1997 precisa que "una comprensión sistemática del entero orden competencial lleva a concluir, de acuerdo con nuestra jurisprudencia, que las "condiciones básicas" hacen referencia al contenido primario (STC 154/1988) del derecho, a las posiciones jurídicas fundamentales (facultades elementales, límites esenciales, deberes fundamentales, prestaciones básicas, ciertas premisas o presupuestos previos.)". Dentro de esas "condiciones básicas" cabe entender incluidos asimismo aquellos criterios que guardan una relación necesaria e inmediata con aquéllas, tales como el objeto o ámbito material sobre el que recaen las facultades que integran el derecho (...); los deberes, requisitos mínimos o condiciones básicas en que ha de ejercerse un derecho (...); los requisitos indispensables o el marco organizativo que posibilitan el ejercicio mismo del derecho, etcétera".

No obstante, la STC 54/2002, FJ. 3, recordando la anterior STC 173/1998, afirma que "(...) el artículo 149.1.1 CE, más que delimitar un ámbito material excluyente de toda intervención de las Comunidades Autónomas, lo que contiene es una habilitación para que el Estado condicione -mediante, precisamente, el establecimiento de unas "condiciones básicas" uniformes- el ejercicio de esas competencias autonómicas con el objeto de garantizar la igualdad de todos los españoles en el ejercicio de sus derechos y en el cumplimiento de sus deberes constitucionales".

## **b) Garantías institucionales.**

El reconocimiento constitucional de la eventual existencia de garantías institucionales de los derechos constitucionales supone la reserva al Estado de potestades ejecutivas.

En este sentido, la Ley Orgánica 5/1992 (LORTAD) fue objeto de los recursos de inconstitucionalidad números 201/1993, 219/1993, 226/1993 y 236/1993, planteados por los Diputados del Partido Popular, el Defensor del Pueblo, el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento de Cataluña. En el caso de los recursos de la Comunidad Autónoma de Cataluña, la inconstitucionalidad de diversos preceptos se fundamentó en razones competenciales, aunque referidas a la vulneración de funciones ejecutivas. En concreto, se criticaba que se reconociese solamente a las Comunidades Autónomas el control de los ficheros de su propia administración, reservando la

tutela administrativa de los ficheros privados o de los pertenecientes a la Administración Local al Estado, a través de la Agencia de Protección de Datos, considerándose que, no siendo los ficheros automatizados una materia competencial en si mismos, sino un instrumento para realizar determinadas actividades, las Comunidades Autónomas o el Estado serán competentes, respectivamente, sobre aquellos ficheros automatizados relacionados con materias en las que uno u otro sean a su vez competentes. También reclamaba Cataluña que se debía hacer referencia a las autoridades de control competentes en las Comunidades Autónomas y a los registros creados por estas y no meramente a la Agencia de Protección de Datos y al Registro General de Protección de Datos.

Los recursos contra la Ley Orgánica 5/1992 fueron resueltos por la Sentencia 290/2000, que declaró la pérdida sobrevenida del objeto de las cuestiones que no afectan al orden de distribución de competencias -como son las relacionadas con el derecho a la intimidad o la reserva de Ley- tras la derogación de la LORTAD por la LOPD, mientras que desestimó el recurso respecto de las infracciones del orden constitucional de competencias entre el Estado y las Comunidades Autónomas.

Concretamente, el Tribunal Constitucional ha reconocido la constitucionalidad de la existencia de una Agencia estatal con funciones en materia de protección de datos, al señalar que: “A este fin la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros” (FJ. 14). Y concluye el Tribunal que “En definitiva, es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos y el Registro Central de Protección de Datos puede ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada radicados en Cataluña” (FJ. 15).

Posteriormente, las Comunidades Autónomas han comenzado al asumir funciones ejecutivas en materia de protección de datos. El primer hito de este proceso lo constituye la Ley Orgánica 15/1999 (artículos 41 y 42), que no fue recurrida ante el Tribunal Constitucional, previó la creación, por parte de las Comunidades Autónomas, de organismos de control (Agencias de Protección de Datos), que ejercerán las funciones de la Agencia Española de Protección de Datos (a excepción de las que se refieren a las transferencias internacionales de datos) cuando afecten a ficheros de datos de carácter personal creados o



gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial y, por los órganos correspondientes de cada Comunidad Autónoma, limitando así las competencias autonómicas a los denominados ficheros de titularidad pública. Asimismo se declara que las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

Más recientemente, las últimas reformas de los Estatutos de Autonomía han incorporado referencias expresas a la materia de protección de datos de carácter personal y han asumido ciertas competencias:

- El Estatuto de Autonomía de Illes Balears atribuye a esta Comunidad Autónoma el desarrollo y ejecución en relación con “la protección de datos de carácter personal respecto de los ficheros de titularidad de las Administraciones públicas de la Comunidad Autónoma y los entes u organismos de cualquier clase vinculados o dependientes de éstas” (artículo 31.14)

- En virtud de lo previsto en el artículo 156 del Estatuto de Cataluña, “corresponde a la Generalitat la competencia ejecutiva en materia de protección de datos de carácter personal que, respetando las garantías de los derechos fundamentales en esta materia, incluye en todo caso:

- a) La inscripción y el control de los ficheros o los tratamientos de datos de carácter personal creados o gestionados por las instituciones públicas de Cataluña, la Administración de la Generalitat, las administraciones locales de Cataluña, las entidades autónomas y las demás entidades de derecho público o privado que dependen de las administraciones autonómica o locales o que prestan servicios o realizan actividades por cuenta propia a través de cualquier forma de gestión directa o indirecta, y las universidades que integran el sistema universitario catalán.

- b) La inscripción y el control de los ficheros o los tratamientos de datos de carácter personal privados creados o gestionados por personas físicas o jurídicas para el ejercicio de las funciones públicas con relación a materias que son competencia de la Generalitat o de los entes locales de Cataluña si el tratamiento se efectúa en Cataluña.

- c) La inscripción y el control de los ficheros y los tratamientos de datos que creen o gestionen las corporaciones de derecho público que ejerzan sus funciones exclusivamente en el ámbito territorial de Cataluña.

- d) La constitución de una autoridad independiente, designada por el Parlamento, que vele por la garantía del derecho a la protección de datos personales en el ámbito de las competencias de la Generalitat”

- De acuerdo con el artículo 82 de su Estatuto, “corresponde a la Comunidad Autónoma de Andalucía la competencia ejecutiva sobre protección de datos de carácter personal, gestionados por las instituciones autonómicas de Andalucía, Administración autonómica, Administraciones locales, y otras entidades

de derecho público y privado dependientes de cualquiera de ellas, así como por las universidades del sistema universitario andaluz”.

- Finalmente, Aragón ha asumido la competencia compartida en materia de “protección de datos de carácter personal, que, en todo caso, incluye la regulación, inscripción y el tratamiento de los mismos, el control de los ficheros creados o gestionados por las instituciones públicas de Aragón y, en especial, la creación de una Agencia de protección de datos de Aragón” (artículo 75.5 del Estatuto de Autonomía). A este respecto, el artículo 75 del Estatuto especifica que “en el ámbito de las competencias compartidas, la Comunidad Autónoma de Aragón ejercerá el desarrollo legislativo y la ejecución de la legislación básica que establezca el Estado en normas con rango de ley, excepto en los casos que se determinen de acuerdo con la Constitución, desarrollando políticas propias”.

## **C) Impacto económico**

### **c.1) Impacto económico general**

Dada la materia objeto de regulación, se identifica un claro impacto económico de carácter general positivo. La inexistencia de régimen jurídico armonizado, o lo que es lo mismo, la existencia de diversos regímenes jurídicos en los diferentes EEMM pretende ser superado con la eficacia directa del Reglamento y remover, a su vez, los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la Directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Pues bien, la remoción de este distinto tratamiento y la existencia de un régimen armonizado en toda la UE tendrán un efecto claro en un aspecto económico concreto como es la ubicación de empresas y operadores económicos en el territorio de la UE al margen de esta cuestión; es decir, que el distinto tratamiento de este tipo de protección ya no será un aspecto relevante de cara a la decisión de implantación de las empresas puesto que, con independencia del EM en el que se ubiquen y actúen, el régimen de garantía y responsabilidad será el mismo en los aspectos esenciales.

### **c.2) Efectos sobre la competencia.**

Este proyecto no tiene efectos sobre la competencia en el mercado, dado que no limita el número o la variedad de los operadores en el mercado, ni la

capacidad de los operadores para competir, o reduce los incentivos de los operadores para competir.

### **c.3) Cargas administrativas.**

A efectos de la Memoria, se consideran cargas administrativas aquellas actividades de naturaleza administrativa que deben llevar a cabo las empresas y ciudadanos para cumplir con las obligaciones derivadas de la normativa. Dentro de esta definición se entienden incluidas aquellas actividades voluntarias de naturaleza administrativa derivadas de una diligente gestión empresarial (solicitud de subvenciones, inscripción en registros voluntarios, solicitudes de claves de servicio...).

En el caso de las empresas, las cargas administrativas son los costes que aquéllas deben soportar para cumplir las obligaciones de facilitar, conservar o generar información sobre sus actividades o su producción, para su puesta a disposición y aprobación, en su caso, por parte de autoridades públicas o terceros, y constituyen un subconjunto de los costes administrativos de las empresas, ya que éstos engloban también, además de las cargas, las actividades administrativas que las empresas continuarían realizando si se derogase la normativa.

En el estudio y cuantificación de las cargas del texto, se ha de resaltar que quedan reducidas únicamente a lo concerniente a las cuestiones que no vengan ya determinadas por el reglamento UE, lo que a todos los efectos es prácticamente inexistente.

## **D) Impacto presupuestario.**

### **d.1) Consideraciones Generales**

La adaptación al Reglamento general de protección de datos que implica esta ley orgánica, incluye el cumplimiento de la obligación de establecer el régimen de las Autoridades de control independientes, que habrán de velar por la adecuada salvaguarda del derecho fundamental a la protección de datos de carácter personal, y dentro de este, en particular, la determinación del estatuto aplicable a quienes desempeñen en las mismas las funciones que lleven aparejada la toma de decisiones.

Por lo que respecta al régimen de la Agencia Española de Protección de Datos no cabe duda de que la misma se encuadra necesariamente dentro de lo que la Ley 40/2015, de 1 de octubre, de Régimen jurídico del sector público, denomina "Autoridades Administrativas Independientes", quedando así sometida a su normativa específica y supletoriamente, y en cuanto sea compatible con su plena independencia, a lo establecido en las normas generales del Derecho Administrativo.

Cabe recalcar la “total independencia” con la que el Reglamento general de protección de datos inviste a las autoridades, conforme a las exigencias contenidas en la Carta de Derechos y Libertades Fundamentales de la Unión Europea. Este principio determina que la independencia excede de la meramente funcional para evitar que la injerencia de los poderes públicos afecte al adecuado cumplimiento de las funciones y potestades que se le encomienden.

En este sentido destacar que esta “total independencia” se materializa en la necesidad de dotar a la Autoridad de control de los medios necesarios para el cumplimiento efectivo de sus funciones, tal y como impone expresamente a los Estados miembros el apartado 4 del artículo 52 del Reglamento general de protección de datos.

Por este motivo, la plena aplicación de las previsiones legales va a requerir un cierto esfuerzo presupuestario en la misma línea del que se está siguiendo en el resto de los Estados miembros.

#### **d.2) Impacto en los Presupuestos Generales del Estado**

La evaluación del impacto presupuestario se concreta en los siguientes parámetros:

A) De implantación y dotación de medios (mobiliarios, informáticos, etc) se considera sin efecto presupuestario ya que podrían asumirse con los remanentes de los distintos capítulos del Presupuesto de la Agencia.

B) Gastos recurrentes de personal:

Se evaluará el posible coste de creación de los puestos necesarios para la transformación de la AEPD y adaptación para la asunción de las nuevas funciones previstas por el RGPD.

C) Créditos recurrentes de gastos corrientes. Se consideran sin efecto presupuestario ya que podrían asumirse con los remanentes de los distintos capítulos del Presupuesto de la Agencia.

Siendo la Agencia actual un organismo que se autofinancia y no recibe ninguna transferencia del Estado, podría ser asumido con su remanente de Tesorería.

#### **d.3) Actuaciones en otros Estados Miembros**

A continuación se recoge la información disponible hasta la fecha de las actuaciones que se están realizando, ya dentro del periodo transitorio iniciado con la aprobación del RGPD, en otros Estados Miembros de la Unión Europea para dotar a sus autoridades de control de los medios necesarios para afrontar los nuevos retos que implica la aplicación del RGPD.

### **Francia**

La autoridad francesa es en la actualidad una de las mejor dotadas en términos de recursos humanos, contando con 195 empleados.

En principio ha solicitado 21 nuevos empleados, de los que ya se han concedido 5 en 2016.

La solicitud de nuevas contrataciones está vinculada al aumento de tareas derivado del futuro Reglamento Europeo, como consecuencia de la ampliación de su ámbito de aplicación (ámbito territorial y responsabilidad de encargados de tratamiento), la “europeización” de los procedimientos (“ventanilla única”, asistencia mutua, coherencia, Comité Europeo de Protección de Datos), la adición de áreas de actuación (consultas de responsables tras Evaluaciones de Impacto, notificación de quiebras de seguridad), así como de las tareas vinculadas al futuro Reglamento de ePrivacy.

### **Alemania**

La Autoridad Federal, que tiene unas competencias muy limitadas, ya que la supervisión de entidades privadas y de las administraciones públicas regionales corresponden a las autoridades de supervisión de los Länder, tiene una plantilla actualmente de 110 efectivos y ha solicitado un incremento de 32 puestos de trabajo (38,9% de su plantilla actual) para el período 2017/2018: 12 puestos para 2017 y 20 para 2018.

Igualmente disponen de un estudio realizado por la Universidad de Kassel a petición de las autoridades de protección de datos de los Länder en el que se evalúan las necesidades adicionales medias de estas autoridades. Según este estudio (<http://suche.transparenz.hamburg.de/dataset/gutachten-zum-zusaetzlichen-arbeitsaufwand-fuer-die-aufsichtsbehoerden-der-laender-durch-d-2017>), la autoridad de supervisión de cada Land debería incrementar sus recursos humanos entre 24 y 33 personas. Ello supondría aumentos superiores al cien por cien de los efectivos actuales, que se sitúan, dependiendo de los Länder, entre 20 y 30 personas.

### **Irlanda**

Disponemos de información tanto de las actuaciones presupuestarias realizadas como de las que se están llevando a cabo en materia de personal.

A nivel presupuestario: El presupuesto anual aumentó en un 62% desde 4,7 a 7,5 millones de Euros en 2017.

Incremento de recursos humanos: La autoridad irlandesa espera alcanzar la cifra de 100 empleados para finales de 2017, lo que supone un aumento de 35 personas. Este incremento se suma al ya experimentado a lo largo de los tres últimos años, en los que la autoridad ha doblado prácticamente su personal.

La autoridad irlandesa informa de que han recibido indicaciones por parte de su gobierno sobre nuevos incrementos presupuestarios en 2018, que entre otras cosas se traducirán en contrataciones adicionales.

### **Hungría**

Las cifras, tanto de presupuesto como de personal, reflejan el compromiso asumido por el gobierno húngaro con la autoridad de protección de datos solo pendiente de aprobación parlamentaria (en el momento en el que trasladaron esta información), para la que consideran que en principio no habrá ningún obstáculo.

Incremento presupuestario: Se ha planteado por el gobierno un incremento presupuestario del 66% que debe hacerse efectivo en dos años, con un 80% en 2018 y un 20% en 2019.

Incremento de recursos humanos: La plantilla de la autoridad se verá incrementada en 30 personas, desde 75 hasta 105, es decir, un 40% de la plantilla existente.

### **Holanda**

La autoridad de supervisión no ha establecido aún sus necesidades concretas en relación con la aplicación del Reglamento Europeo. Sin embargo, asumen que se requerirá un incremento en su personal y han encargado un estudio en profundidad a una empresa consultora especializada en recursos humanos.

### **Reino Unido**

La autoridad de Reino Unido tiene una importante plantilla, con un total de 409 empleados (aunque es también autoridad de acceso a información pública). Durante 2016 se ha realizado un primer incremento de su plantilla del 3,4% (14 personas).

La Comisionada británica ha anunciado públicamente, y específicamente durante una sesión en la Cámara de los Lores, que ha solicitado al gobierno un

aumento de 200 puestos de trabajo para hacer frente a las necesidades derivadas del nuevo Reglamento Europeo.

### **E) Impacto por razón de género.**

En todos aquellos casos en los que la norma propuesta pueda tener efectos, directos o indirectos, sobre personas físicas, se realizará una previsión sobre los resultados de la aplicación de la misma y se analizarán sus efectos para los hombres y mujeres que sean sus potenciales destinatarios.

La valoración del impacto de género calificará los resultados previstos en relación con la eliminación de desigualdades entre mujeres y hombres y el cumplimiento de los objetivos de políticas de igualdad.

En este sentido, se considera que este Anteproyecto tiene impacto por razón de género nulo, es decir, dado que la finalidad es regular el ejercicio del derecho fundamental de las personas físicas a la protección de datos de carácter personal, sin que se establezca ninguna distinción jurídica, ni real, en este sentido.

### **F) Impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.**

La norma proyectada tiene un impacto nulo en materia de igualdad de oportunidades, no discriminación por las razones expuestas en el epígrafe anterior.

### **G) Impacto en la infancia (exigida en el artículo 22 quinquies de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor)**

En este sentido, se considera que este Anteproyecto tiene impacto por razón de la infancia positivo, es decir, dado que la finalidad es regular el ejercicio del derecho fundamental de las personas físicas a la protección de datos de carácter personal, además de que establece regulaciones adicionales especiales para menores (derivadas directamente del reglamento europeo).

En concreto, aparte de las garantías que otorga que la regulación de este derecho fundamental, el Reglamento General de protección de datos incluye salvaguardias para los menores en su artículo 6.1.j), o en el mismo artículo 8 que prevé que cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Por

otro lado, permite que los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

Respecto de la fijación de dicha edad mínima en el artículo 8, al amparo de la habilitación concedida a los Estados por el RGPD, es importante destacar algunos argumentos esgrimidos a favor de esta opción en el trámite de información pública:

1) Mayores posibilidades para el desarrollo: Desde una aproximación de derechos de la infancia, la Convención de los Derechos del Niño establece la necesidad de protección del menor (niñas, niños y adolescentes), al mismo tiempo que su articulado pone de manifiesto otros dos objetivos importantes:

- Posibilitar su pleno desarrollo
- Promover la participación activa en la sociedad.

Una restricción mayor en el acceso a Internet y sus servicios mediante la elevación de la edad mínima por encima de los trece años podría mermar en sus posibilidades de desarrollo y, en consecuencia, en la obtención de capacidades y destrezas para afrontar los retos de la vida digital.

2) Cumplimiento supuesto con la obligación de escuchar su opinión: El enfoque de derechos de infancia establece la necesidad de escuchar la voz de niños y niñas especialmente en aquellas cuestiones que les afectan.

3) Reducción de escenarios irreales y de efecto adversos: La limitación por edad del uso de servicios online es muy difícil de gestionar. No por ello se debe renunciar a establecer límites, pero al mismo tiempo es preciso tener en cuenta las posibilidades reales y las demandas sociales a este respecto, máxime teniendo en cuenta que la edad de trece años bastará en la mayoría de los países de nuestro entorno para prestar el consentimiento al tratamiento de datos personales.

4) Mayores posibilidades de acceder a servicios globales: En línea con lo indicado, si la edad mínima en España es superior a la edad mínima establecida en otro país (europeo o no) se hace indispensable que las entidades prestadoras de servicios globales (en otros países además de España) requieran a los usuarios españoles su ubicación para, en función de la misma y confirmada ésta, le permitan o no acceder al servicio. Este dato de ubicación o bien es solicitado expresamente o bien obtenido por procedimientos automáticos en cuyo caso también requiere consentimiento del usuario para no transgredir su derecho a la protección de datos personales. Así, cuando la edad establecida no es la mínima, ocurriría que no se le puede dar el servicio porque es necesario preguntarle su localización, lo cual ya transgrede su derecho a la protección de datos personales.

5) Fomento de la autonomía y la madurez: El desarrollo de la autonomía, y con ella la madurez, requiere capacidad de tomar decisiones. Así, en las políticas



europeas no se habla ya tanto de evitar riesgos sino de afrontarlos con éxito y el programa “Safer Internet” es ahora “Better Internet”. La exposición al riesgo es inevitable.

#### **H) impacto en la familia, de acuerdo con lo previsto en la disposición adicional décima de la Ley 40/2003, de 18 de noviembre, de protección a las familias numerosas.**

En este sentido, se considera que este Anteproyecto tiene impacto por razón de la familia nulo, es decir, dado que la finalidad es regular el ejercicio del derecho fundamental de las personas físicas a la protección de datos de carácter personal, sin que se establezca ninguna distinción jurídica, ni real, en este sentido.

#### **I) Impacto en Administraciones Públicas (RGPD).**

El artículo 26.3 de la Ley 50/1997, de 27 de noviembre, del Gobierno, permite que la Memoria del Análisis de Impacto Normativo incluya cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente. En consecuencia, se recoge en este apartado el estudio sobre el impacto en las Administraciones Públicas, realizado y publicado por la Agencia Española de Protección de Datos en su portal web.

Las Administraciones Públicas (AAPP) actúan como responsables y encargados de tratamientos de datos personales en el desarrollo de muchas de sus actividades. Consecuentemente, se van a ver afectadas por las previsiones del nuevo Reglamento general de protección de datos (RGPD) de la Unión Europea. En muchos casos, los efectos del RGPD serán los mismos que para cualquier otro responsable o encargado. En algunas áreas, sin embargo, existen especificidades para el sector público.

El RGPD fue publicado en mayo de 2016 y entró en vigor en ese mismo mes. Sin embargo, será aplicable a partir del 25 de mayo de 2018. Las modificaciones que deberán realizarse para alinear la normativa y la práctica de las AAPP con las previsiones del RGPD habrán de estar listas para aplicarse, a más tardar, en esa fecha de 2018.

El impacto del RGPD sobre las AAPP puede sintetizarse en los siguientes puntos:

1. Necesidad de identificar con precisión las finalidades y la base jurídica de los tratamientos que llevan a cabo. Esta obligación no deriva sólo de la necesidad de cumplir con el principio de legalidad establecido en el RGPD, sino que viene impuesta por el hecho de que las finalidades o la base jurídica de los tratamientos

son informaciones que deben proporcionarse a los interesados (arts. 13 y 14 RGPD) y recogerse en el registro de actividades de tratamiento.

La identificación de finalidades y base jurídica tiene exigencias adicionales en los casos en que se traten datos de los considerados como objeto de especial protección, que incluyen, entre otros, los datos sobre salud, ideología, religión o pertenencia étnica. El tratamiento de estos datos está, con carácter general, prohibido, y sólo podrá llevarse a cabo si es aplicable alguna de las excepciones previstas en el art. 9.2 del RGPD. Entre ellas pueden destacarse, a los efectos de este documento, el que el tratamiento sea necesario para satisfacer un interés público esencial, el que sea necesario para fines de prevención, asistencia sanitaria o salud pública, o que sea necesario para la gestión de los servicios de asistencia social, en todos los casos en los términos que establezca la legislación española o de la Unión Europea. 2

2. En el caso de la actividad de las AAPP será muy habitual que la base jurídica de los tratamientos sea el cumplimiento de una tarea en interés público o el ejercicio de poderes públicos. Tanto el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma de rango legal.

3. En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el RGPD, que exige que sea informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa. Los consentimientos conocidos como “tácitos”, basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad.

4. Necesidad de adecuar la información que se ofrece a los interesados cuando se recogen sus datos a las exigencias del RGPD (arts. 13 y 14). El RGPD obliga a ofrecer una información que es más amplia que la actualmente exigida por la Ley Orgánica de Protección de Datos. Obliga, además, a que esta información se proporcione de forma “concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo”. Tanto esta obligación como la recogida en el siguiente punto requerirán la modificación de los documentos que actualmente recogen estas cláusulas informativas y la adaptación de los que se utilicen en el futuro en circunstancias como, por ejemplo, las convocatorias de subvenciones o de pruebas selectivas.

5. Necesidad de establecer mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos. Estos mecanismos, en particular cuando se trate del ejercicio por medios electrónicos, deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.

6. Necesidad de establecer procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD. En algunos casos será preciso valorar la necesidad de que sean los encargados del tratamiento con los que se haya contratado la prestación de determinados servicios los que colaboren en la atención a las solicitudes de los interesados. En estos casos, esa colaboración debe incluirse en los contratos de encargo de tratamiento.

7. Necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD. El RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones de cumplir con el RGPD.

8. Necesidad de adecuar los contratos de encargo que actualmente se tengan suscritos a las previsiones del RGPD. El RGPD establece que la relación entre responsables y encargados deberá formalizarse mediante un contrato o un acto jurídico que vincule al encargado. En el caso de las AAPP será frecuente que el encargo de tratamiento se establezca mediante actos jurídicos, por ejemplo en la norma de creación de órganos encargados de la prestación de servicios informáticos. El RGPD exige expresamente que tanto los contratos como los actos jurídicos deberán tener un contenido mínimo que excede del actualmente previsto por la normativa española de protección de datos.

9. Necesidad de hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen. El RGPD hace depender la aplicación de todas las medidas de cumplimiento que prevé para responsables y encargados del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados. Por ello, todo tratamiento, tanto los ya existentes como los que se pretenda iniciar, deben ser objeto de un análisis de riesgos. En el contexto de las AAPP se dispone de metodologías de análisis de riesgos focalizadas principalmente en la seguridad de la información. Esas metodologías deben ampliarse para incluir riesgos asociados al incumplimiento de las disposiciones del RGPD.

10. Necesidad de establecer un Registro de Actividades de Tratamiento. Este registro sustituye, en parte, a la obligación de notificar los ficheros y tratamientos a las autoridades de protección de datos. El RGPD establece un contenido mínimo de ese registro, tanto para responsables como para encargados de tratamiento. El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes. El registro deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.

11. Necesidad de revisar las medidas de seguridad que se aplican a los tratamientos a la luz de los resultados del análisis de riesgo de los mismos. La normativa española de protección de datos contiene previsiones específicas sobre

medidas de seguridad atendiendo básicamente al tipo de datos que se tratan. El RGPD, sin embargo, deja sin efecto esas previsiones, en la medida en que exige que las medidas de seguridad se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes. Puede ocurrir que, tras un análisis de riesgo, y tomando en cuenta todos los demás factores, las medidas de seguridad sean las mismas que la normativa española prevé para un tipo determinado de datos. Pero en todo caso la aplicación de esas medidas no puede derivarse automáticamente de que se traten unos datos u otros, sino que ha de ser la consecuencia de un análisis de riesgos específico para cada tratamiento. En el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad.

12. Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas, en particular para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados y para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados. El RGPD establece, asimismo, la obligación de mantener un registro de todos los incidentes de seguridad, sean o no objeto de notificación.

13. Necesidad de valorar si los tratamientos que se realizan requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y de disponer de una metodología para llevarla a cabo. El RGPD establece que, con anterioridad a su puesta en marcha, los tratamientos que sea probable que supongan un alto riesgo para los derechos y libertades de los afectados deberán ser objeto de una Evaluación de Impacto sobre la Protección de Datos. El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo. También contempla un contenido mínimo de las Evaluaciones de Impacto.

En el caso de tratamientos basados en la consecución de fines de interés público o vinculados al ejercicio de poderes públicos, el RGPD prevé que pueda no llevarse a cabo la Evaluación de Impacto, pese a tratarse de tratamientos de alto riesgo, cuando la norma de base regule la operación o conjunto de operaciones de tratamiento y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de esa norma de base.

14. Necesidad de designar un Delegado de Protección de Datos (DPD). El RGPD prevé que todas las “autoridades u organismos públicos” nombrarán un DPD. También establece cuáles habrán de ser los criterios para su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que

en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa. En consecuencia, como medida previa deben identificarse las unidades en que se integran el DPD dentro de cada órgano u organismo, su posición en la estructura administrativa y los mecanismos para asegurar que los DPD designados reúnen los requisitos de cualificación y competencia establecidos por el RGPD. La designación del DPD debe comunicarse a las autoridades de protección de datos. Asimismo, deben establecerse mecanismos para que los interesados puedan contactar con el DPD.

15. Necesidad de adaptar los instrumentos de transferencia internacional de datos personales a las previsiones del RGPD. El RGPD mantiene el modelo de transferencias internacionales ya existente, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que no requerirán de autorización previa de las autoridades de protección de datos. Entre estos instrumentos se incluyen los jurídicamente vinculantes y exigibles entre autoridades y organismos públicos. También prevé expresamente que requerirán autorización las transferencias basadas en acuerdos no jurídicamente vinculantes.