

**PRAXIS SOBRE PROTECCIÓN DE DATOS  
EN LAS ENTIDADES LOCALES**

OTROS TITULOS DE LA MISMA COLECCIÓN:

94. Génesis y realidad de la Ley 27/2013, de 27 de diciembre, de Racionalización y Sostenibilidad de la Administración Local: ¿una nueva reforma económica local?  
LORENZO MELADO RUIZ
95. Lecciones Teórico-Prácticas de Organización Administrativa.  
VICENTE MARÍA GÓNZALEZ-HABA GUIASADO.
96. La trasposición de la Directiva de Servicios: licencias, autorizaciones ambientales, comunicaciones previas y declaraciones responsables  
JOSÉ IGNACIO MARTÍNEZ GARCÍA y JUAN FERNANDO GRANADOS RODRÍGUEZ (Coord.)
97. Las nuevas Diputaciones Provinciales de régimen común: asistencia, prestación y coordinación de servicios municipales  
M<sup>a</sup> ÁNGELES GONZÁLEZ BUSTOS (Coord.)
98. La Hacienda Local ante la Ley de Racionalización y Sostenibilidad de la Administración Local. Dimensión económico-financiera de la Ley.  
JOSÉ MANUEL FARFÁN PÉREZ (Dir.)
99. Aproximación al nuevo procedimiento administrativo común de la Ley 39/2015: reflexiones y claves para su aplicación  
MARÍA JESÚS GALLARDO CASTILLO (Dir.)
100. La Ley 10/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y las Administraciones Locales  
HUMBERTO GOSÁLBEZ PEQUEÑO (Dir.)
101. Singularidades del poder tributario local y gravamen fiscal sobre las Entidades locales.  
MARIA JOSÉ FERNÁNDEZ PAVEZ (Dir.)
102. Compliance en la Administración Pública: dificultades y propuestas.  
CONCEPCIÓN CAMPOS ACUÑA
103. Nuevos enfoques en la gestión de los servicios públicos locales.  
VALENTIN MERINO ESTRADA y PILAR ORTEGA JIMÉNEZ.
104. Planificación, fomento y gestión del turismo por las entidades locales.  
HUMBERTO GOSÁLBEZ PEQUEÑO (Dir.)
105. Vademécum práctico sobre derecho de la Unión Europea.  
JAIME PINTOS SANTIAGO
106. Contaminación Acústica. Gestión del ruido por las Corporaciones Locales. Aspectos jurídicos, técnicos y sanitarios.  
JAIME GALBARRO MUÑOZ, JOAQUÍN HERRERA DEL REY, ANTONIO PEIDRO CUADROS, JOSE LUIS RODRÍGUEZ LAÍN
107. Planificación en entidades locales. Desde la planificación estratégica a la implementación de proyectos.  
PATRICIA MOLINA HERNÁNDEZ
108. Derecho del patrimonio histórico y cultural. Gestión estatal, autonómica y local.  
JAVIER BERMÚDEZ SÁNCHEZ
109. Reflexiones en torno a la figura del Directivo Público Local.  
GUSTAVO GARCÍA-VILLANOVA ZURITA
110. El funcionamiento de los Órganos Colegiados Locales  
FERNANDO GÓMEZ GARRIDO y GUILLERMO LAGO NÚÑEZ

# PRAXIS SOBRE PROTECCIÓN DE DATOS EN LAS ENTIDADES LOCALES

CAROLINA GOÑI MURUZABAL

LOURDES OROZ VALENCIA

*Máster en Derecho de Tecnologías de la Información  
y Protección de Datos*

*Abogadas, Socias de Eulza Consultoría (Pamplona)*



**CEMCi**

GRANADA, 2021

© Autoras  
© CEMCI Publicaciones  
Plaza Mariana Pineda, 8. 18009-Granada  
[www.cemci.org](http://www.cemci.org)  
[publicaciones@cemci.org](mailto:publicaciones@cemci.org)

ISBN: 978-84-16219-46-9  
Depósito legal: GR-802-2021

Impreso: Imprenta Diputación de Granada  
Impreso en España - Printed in Spain

El editor no se hace responsable de las opiniones expresadas por  
sus colaboradores.



# ÍNDICE

<b>Presentación .....</b>	<b>17</b>
<b>Prólogo .....</b>	<b>21</b>
<b>Acrónimos .....</b>	<b>25</b>
<b>CAPÍTULO PRIMERO. LEGISLACIÓN APLICABLE.....</b>	<b>27</b>
1. Introducción: marco normativo en materia de protección de datos.....	29
2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE.....	34
3. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.....	57
4. Objetivos para la adaptación al RGPD y LOPDGDD para las entidades locales .....	63
5. ¿Está derogada la LOPD (Ley Orgánica 15/1999) y su Reglamento de desarrollo RD 1720/2007? .....	65

**CAPÍTULO SEGUNDO. PRINCIPIOS Y CONCEPTOS  
BÁSICOS EN LA NORMATIVA DE PROTECCIÓN DE DATOS ...69**

- 1. Principios que legitiman el tratamiento de los datos .... 71
- 2. Datos de carácter personal ..... 80
- 3. Categorías especiales de datos ..... 92
- 4. Aplicabilidad: excepciones ..... 97
- 5. Tratamiento ..... 101

**CAPÍTULO TERCERO. FIGURAS INTERVINIENTES .....105**

- 1. Responsable del tratamiento ..... 107
  - 1.1. Normativa que desarrolla la obligación ..... 107
  - 1.2. ¿Quién asume el rol de responsable de tratamiento? ..... 108
  - 1.3. Principales obligaciones del Responsable de Tratamiento ..... 109
- 2. Corresponsables del tratamiento ..... 111
- 3. Encargado de tratamiento ..... 116
  - 3.1. Normativa que desarrolla la figura ..... 116
  - 3.2. La definición del encargado de tratamiento y las obligaciones propias de los encargados ..... 118
  - 3.3. Las garantías que debe aportar el encargado de tratamiento ..... 120
  - 3.4. Relación entre responsable y encargado de tratamiento, Contrato de encargado de tratamiento ..... 124
  - 3.5. Encargado del tratamiento en virtud de competencias ..... 128
  - 3.6. ¿El encargado de tratamiento de una administración puede llegar a ser responsable de tratamiento? ..... 129
  - 3.7. Contrato de encargado de tratamiento firmados con antelación a la plena aplicación del RGPD ..... 129
  - 3.8. Conclusiones ..... 130

4. Autoridades de control.....	131
4.1. Normativa que la desarrolla y definiciones.....	131
4.2. Agencia Española de Protección de Datos .....	132
4.3. Autoridades autonómicas .....	135
5. Delegado de protección de datos o DPD .....	136
5.1. Normativa que desarrolla la obligación .....	136
5.2. Nombramiento del delegado de protección de datos.....	138
5.3. Capacitación.....	138
5.4. Posición .....	138
5.5. Funciones .....	139

**CAPÍTULO CUARTO. EL REGISTRO DE  
ACTIVIDADES DE TRATAMIENTO ..... 143**

**Registro de actividades y su publicación por  
medios electrónicos ..... 145**

1. Actuaciones para identificar las actividades de tratamiento .....	147
2. Publicación del registro de actividades, por medios electrónicos .....	150
3. Aspectos prácticos sobre el trabajo de obtención del registro de actividades.....	152
4. Referencia a algunos tratamientos.....	153
4.1. El tratamiento de las denuncias anónimas .....	153
4.2. Tratamiento de datos con fines de archivo en interés público por parte de las administraciones públicas.....	165
4.3. Tratamiento de datos de personas fallecidas ....	168
4.4. Tratamientos sometidos a la Directiva (UE) 2016/680 prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la Ley	

Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.....	171
---	-----

**CAPÍTULO QUINTO. TRANSPARENCIA, EJERCICIO DE DERECHOS, BRECHAS DE SEGURIDAD..... 187**

1. Cumplimiento del principio de transparencia en el tratamiento de datos de carácter personal.....	189
1.1. Normativa de aplicación.....	189
1.2. Información que se debe facilitar y forma de hacerlo .....	190
1.3. Aspectos prácticos sobre el deber de transparencia.....	195
2. Atención al ejercicio de derechos de las personas afectadas.....	195
2.1. Normativa de aplicación.....	195
2.2. Disposiciones generales sobre el ejercicio de los derechos .....	196
2.3. Procedimiento para atender el ejercicio de los derechos .....	199
2.3.1. Ejercicio derecho de acceso de la persona interesada .....	201
2.3.2. Ejercicio derecho de rectificación .....	204
2.3.3. Ejercicio derecho de supresión (derecho al olvido).....	205
2.3.4. Ejercicio derecho de oposición.....	211
2.3.5. Ejercicio derecho de portabilidad.....	212
2.3.6. Ejercicio derecho limitación de tratamiento .....	213
2.4. Aspectos prácticos para atender al ejercicio de derechos.....	214

3. Brechas de seguridad.....	214
3.1. Normativa de aplicación.....	214
3.1.1. Concepto y definición de violación o brecha de seguridad.....	217
3.1.2. Detección de la brecha de seguridad, registro y clasificación.....	219
3.1.3. Obligaciones derivadas de la existencia de una brecha o violación de seguridad para el responsable del tratamiento y para el encargado del tratamiento.....	221
3.1.4. Tipos de las brechas .....	229
3.1.5. Creación de procedimiento para prevenir una brecha de seguridad .....	231

**CAPÍTULO SEXTO. OBLIGACIONES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO.....235**

1. Análisis de riesgos.....	237
1.1. Normativa de aplicación.....	237
1.2. El análisis de riesgos para identificar medidas de seguridad .....	238
1.3. Aspectos prácticos en relación con el análisis de riesgos.....	241
2. Evaluación de impacto .....	242
2.1. Normativa de aplicación.....	242
2.2. ¿En qué consiste una evaluación de impacto? ...	243
2.3. Tabla resumen de una evaluación de impacto ...	260
3. Medidas de protección de datos desde el diseño y por defecto.....	262
3.1. Normativa de aplicación.....	262
3.2. La filosofía de la protección de datos desde el diseño y por defecto.....	263
3.3. Principios que rigen la Protección de datos desde el diseño y por defecto.....	264

3.4. Guías de la Agencia Española de Protección de datos en relación con la protección de datos desde el diseño y por defecto.....	267
3.5. Aplicación práctica .....	272
4. Nombramiento de delegado de protección de datos (DPD) .....	274
4.1. Normativa de aplicación.....	274
4.2. Nombramiento de delegado de protección de datos y su comunicación ante la Agencia Española de Protección de datos. ....	275
5. ¿Están previstas sanciones para las administraciones Públicas por el incumplimiento de las obligaciones en materia de protección de datos? .....	277
<b>CAPÍTULO SÉPTIMO. LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES EN LAS ENTIDADES LOCALES .....</b>	<b>281</b>
1. Análisis de las bases que legitiman el tratamiento..	283
1.1. Normativa de aplicación.....	283
1.2. Licitud del tratamiento, condiciones para del tratamiento de datos de carácter personal.....	284
1.2.1. El Consentimiento como base legitimadora del tratamiento.....	287
1.2.2. Cumplimiento de una obligación legal, realización de una misión en interés público o ejercicio de poderes conferidos al responsable del tratamiento .....	290
1.2.3. Interés legítimo .....	293
1.2.4. Datos de características especiales .....	294
2. Aspectos prácticos de la legitimación del tratamiento .....	298

2.1. ¿Qué se considera una “obligación legal”? .....	300
2.2. Ejemplos de normas con rango de ley que legitiman el tratamiento .....	300
2.3. Cesión de datos.....	304
2.3.1. Cesión de datos entre Administraciones Públicas.....	304
3. Supuestos Concretos .....	308
3.1. Ley 39/2015, de 1 de octubre, del Procedimiento administrativo común de las Administraciones Públicas, artículo 28.2 modificado por la LOPDGDD.....	308
3.2. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.....	314
3.3. Notificaciones en procesos de concurrencia competitiva.....	319
3.3.1. Valoración del consentimiento como una base que legitima el tratamiento en los procesos de selección.....	321
3.3.2. Conflicto entre transparencia y protección de datos.....	322
3.3.3. Conclusiones/recomendaciones.....	323
3.4. Cesión de datos a particulares.....	325
3.5. Acceso a la información por parte de las personas que integran la corporación municipal ....	329
3.6. Base legitimadora de la interoperabilidad entre las administraciones .....	338
3.7. La transparencia de las administraciones versus la protección de datos personales.....	340
3.8. Breve referencia a los plazos de conservación de la documentación.....	353
3.9. Reutilización de la información .....	355
3.10. Salidas de datos de carácter personal.....	360

3.11. Uso de datos biométricos .....	361
3.11.1. ¿Qué se entiende por datos biométricos? ...	362
3.11.2. ¿Será necesario realizar una evaluación de impacto? .....	365
3.12. La videovigilancia por las fuerzas y cuerpos de seguridad del estado .....	370
3.12.1. Normativa de aplicación.....	370
3.12.2. Consideraciones previas .....	371
3.12.3. La videovigilancia de espacios públicos ...	374
3.12.4. Comisión de videovigilancia en la Delegación del Gobierno.....	375
3.12.5. Imágenes para el control, regulación, vigilancia y disciplina del tráfico.....	376
3.12.6. Cámaras móviles .....	379

**CAPÍTULO OCTAVO. MEDIDAS DE SEGURIDAD  
APLICABLES A LAS ENTIDADES LOCALES SEGÚN EL  
ESQUEMA NACIONAL DE SEGURIDAD. LA  
CIBERSEGURIDAD.....381**

1. Normativa de aplicación .....	383
2. Introducción al Esquema Nacional de Seguridad.....	385
2.1. Sujetos obligados .....	389
2.2. Principios básicos .....	392
2.3. Objetivos .....	394
2.4. Plazo de adecuación.....	395
2.5. Esquema Nacional De Interoperabilidad (ENI) ...	395
3. Fases en la implantación del ENS .....	396
3.1. Política de seguridad y definición de roles.....	398
3.2. Roles que intervienen .....	400
3.2.1. Responsable de la información.....	401
3.2.2. Responsable del Servicio .....	402

3.2.3. Responsable de Seguridad.....	402
3.2.4. Incompatibilidades a la hora de ejercer las funciones entre las figuras establecidas en el ENS.....	403
3.2.5. Incompatibilidad entre la figura de DPD y Responsable de Sistemas.....	406
3.3. Identificación de la información del sistema y categorización del sistema.....	407
3.4. Análisis de riesgos.....	409
3.4.1. Fases del análisis de riesgos.....	410
3.5. Declaración de aplicabilidad y medidas compensatorias.....	411
3.6. Plan de adecuación y medidas de seguridad.....	412
3.6.1. Marco organizacional.....	414
3.6.2. Marco operacional.....	415
3.6.3. Medidas de protección.....	422
3.7. Mejora continua.....	428
4. ENS e ISO 27001.....	431
5. Centro Criptográfico Nacional promueve la ciberseguridad en las entidades locales.....	432
6. Ciberseguridad.....	436
<b>Bibliografía.....</b>	<b>445</b>



## PRESENTACIÓN

El Plan General de Acción del CEMCI para el año 2021, tras un 2020 especialmente complicado debido a la crisis sanitaria generada por el Covid-19, incluye en sus diferentes pilares de actuación acciones que contribuyan a afrontar los procesos de recuperación económica y social a los que las Administraciones Públicas, y en particular las Entidades Locales, se ven abocadas, junto a aquellos otros procesos de mejora y prestación de servicios que le son propios.

En cualquier caso, el CEMCI continuará actuando bajo parámetros de excelencia, calidad, innovación, modernización y perfeccionamiento, buscando siempre su posicionamiento como centro de referencia en sus campos de actuación principales: formación, investigación, documentación y publicaciones.

El Programa de Documentación y Publicaciones seguirá manteniendo una estrecha vinculación con los Programas de Formación e Investigación para la selección de los temas a publicar, teniendo en cuenta incluir temáticas de actualidad, normativa que afecte de forma directa al ámbito local, con una visión no solo teórica sino

también práctica, así como temas relacionados con la gestión pública local.

Para la elaboración de la obra *Praxis sobre protección de datos en las Entidades Locales* hemos contado con la colaboración de CAROLINA GOÑI MURUZABAL y LOURDES OROZ VALENCIA, abogadas, colegiadas en el M.I. Colegio de Abogados de Pamplona, socias de Eulza Consultoría, dedicada al derecho tecnológico y cumplimiento normativo, con más de más de 15 años de experiencia en asesoramiento en materia de protección de datos en entidades locales, así como autoras en diversas publicaciones especializadas, y docentes en diferentes organismos y entidades locales.

Las autoras hacen una magnífica exposición sobre la normativa de protección de datos, no sólo desde un punto de vista teórico, sino también práctico incorporando supuestos concretos, puesto que la normativa tiene un carácter transversal para la actividad de las entidades locales y se debe considerar en múltiples facetas de la gestión diaria municipal.

A lo largo de ocho capítulos, se muestran los principios y conceptos básicos aplicables de la normativa de protección de datos, las figuras intervinientes en el tratamiento de los datos, el registro de actividades y su publicación por medios electrónicos, el cumplimiento del principio de transparencia en el tratamiento de datos de carácter personal, la figura del Delegado de Protección de Datos, para finalizar con las medidas de seguridad aplicables a las entidades locales según el Esquema Nacional de Seguridad.

Consideramos que éste es un trabajo de gran interés para las administraciones locales, y confiamos en que tenga buena acogida entre nuestros lectores.

Agradecemos a las autoras el trabajo realizado, y a todos los usuarios del CEMCI, el interés demostrado en las actividades y publicaciones que este Centro lleva a cabo.

*CEMCI*



## PRÓLOGO

Este libro surge de la petición que nos realizaron desde el Centro de Estudios Municipales, tras la primera edición del curso “Marco normativo y de gestión de la protección de datos y sus efectos en las Entidades Locales”, en la primavera de 2019 que realizamos en esta organización.

Los objetivos que nos han guiado durante la escritura de este libro son dos, por una parte ampliar la materia que se imparte en el curso y el segundo objetivo es la aportación de nuestra experiencia en la aplicación de la normativa de protección de datos, descender a cuestiones prácticas, exponiendo las razones jurídicas, teniendo en consideración diferentes sentencias, y especialmente resoluciones y dictámenes de las diferentes autoridades de control, la Agencia Española de Protección de Datos, la Agencia Vasca de Protección de Datos, la Autoridad de Protección de Datos Catalana y el Consejo de Transparencia y Protección de Datos de Andalucía.

En nuestra experiencia profesional hemos constatado que esta normativa tiene un carácter trasversal para

la actividad de las entidades locales y se debe considerar en múltiples facetas de la gestión diaria municipal.

Además, como se trata de una normativa relativamente joven, se produce un hecho constante que es la adecuación y el ajuste de la misma, para ello se hace uso de los diversos informes de las autoridades de control que van ayudando a aclarar conceptos, así como de sentencias que sirven de guía para una mejor interpretación de la normativa.

Hace mucho tiempo que constatamos, que esta normativa, que suele ser un "arma arrojadiza" según se quiera defender las diferentes posturas, es habitual que, al iniciar las formaciones presenciales, comencemos con la pregunta ¿qué se entiende por la protección de datos?, para acto seguido dar una respuesta con la que pretendemos que las personas que asisten a nuestro curso tomen conciencia del mal uso que se hace en muchas ocasiones de esta normativa, así que nuestra respuesta es: **Se trata de la excusa perfecta cuando no se quiere dar la información solicitada.** Se utiliza tanto en circunstancias en las se hace la petición es un proyecto urbanístico sin datos personales, o cuando los datos hacen referencia a personas jurídicas.

La normativa de protección de datos tiene una compañera de viaje que es la normativa sobre transparencia y no siempre resulta fácil el encaje entre ambas, ahora bien, todos sabemos que están "condenadas" a entenderse. Para llegar a ese entendimiento y resolver las dudas de aplicación concreta nos van ayudando los diferentes criterios de los Consejos de Transparencia, elaborados en algunas ocasiones de forma conjunta con las autoridades de control.

Si bien el Reglamento General de Protección de datos, tiene aproximadamente el 60 % de medidas de

seguridad de tipo jurídico, esta materia se encuentra vinculada a la aplicación de medidas de seguridad de tipo informático, razón por la cual hemos considerado de interés dedicar un capítulo al Esquema Nacional de Seguridad.

Hay temas en los que nos hemos detenido con más detalle, suelen ser cuestiones que hemos tenido que informar a nuestros clientes y que afectan a la mayoría de las entidades locales, otros temas los hemos desarrollado a "riesgo y ventura" de la futura trasposición de la directiva, como es el caso del canal de denuncias, que al tratarse de un tema novedoso, no hemos querido dejar de hacer referencia. Otros temas nos hemos limitado a realizar breves consideraciones ya que un desarrollo mayor supone tener que adentrarse en otras normativas que van más allá que el objeto de este libro, como es el caso de los plazos de conservación de la información y la normativa de archivos y documentos, que las administraciones han de tener en consideración para cumplir con el principio de limitación del plazo conservación

Las personas que lean este libro no van a encontrar respuesta a todas las dudas sobre la aplicación de esta normativa que puedan tener, aunque hemos expuesto una gran variedad de casos prácticos, también, hemos pretendido exponer criterios generales que permitan hacer la propia composición de lugar ante las posibles dudas de aplicación que surjan en el día a día, y en todo caso, nos sometemos a cualquier mejor criterio fundado en derecho.

Agradecemos a los lectores que se han aventurado en este libro y en especial a los alumnos de los cursos que nos han aportado muchos supuestos reales a los que hemos tenido que dar respuesta y que nos ha permitido incorporarlos a este libro.



## ACRÓNIMOS

AEPD	Agencia Española de Protección de Datos
ARSOL	Ejercicio de los derechos de acceso, rectificación, supresión, oposición y limitación
CCN-Cert DPD/DPO	Centro Criptológico Nacional Delegado de protección de datos/ Data Protection Officer
EELL	Entidades Locales
ENI	Esquema Nacional de Interoperabilidad
ENS	Esquema Nacional de Seguridad
INCIBE	Instituto Nacional de Ciberseguridad
FEMP	Federación Española de Municipios y Provincias
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales
PYMES	Pequeñas y medianas empresas
RD	Real Decreto

RD 1720/2007	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE
SAI	Sistema de Alimentación Interrumpida de corriente
VPN	Red privada virtual

# **CAPÍTULO PRIMERO**

## **LEGISLACIÓN APLICABLE**



## LEGISLACIÓN APLICABLE

### 1. INTRODUCCIÓN: MARCO NORMATIVO EN MATERIA DE PROTECCIÓN DE DATOS

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental que se encuentra ya recogido en la Constitución de 1978 donde regula en el artículo 18 el derecho al honor, a la intimidad personal y familiar y a la propia imagen; la inviolabilidad del domicilio y el secreto de las comunicaciones, previendo el propio artículo 18.4 que *“el legislador limitará el uso de la informática para proteger los derechos fundamentales de los ciudadanos.”*

De esta manera, la Constitución Española fue una de las primeras normas en introducir la limitación del uso de la informática para proteger el honor y la intimidad personal y familiar de los ciudadanos.

Por su parte, el Tribunal Constitucional, proclamó en su Sentencia 292/2000<sup>1</sup> que el derecho a la protección

<sup>1</sup> Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

de datos es un verdadero derecho fundamental, autónomo y claramente diferenciado de los demás que se garantizan en el mismo artículo 18 de la Constitución Española.

Establece la sentencia de forma explícita que se trata de 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.

De forma previa el Tribunal Constitucional en su Sentencia 94/1998<sup>2</sup> garantizó a la persona el control sobre sus datos, cualesquiera datos personales, y 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 aquel que justificó su obtención.

Por lo tanto, se trata de un derecho **fundamental y autónomo**, situado en el máximo nivel de protección jurídica, y que al encontrarse regulado en el Título 1, Capítulo 2º, sección Primera, entre otras medidas de protección, debe ser desarrollado mediante ley orgánica.

<sup>2</sup> Sentencia del Tribunal Constitucional 94/1998, de 4 de mayo

**El origen de la regulación se encuentra en la Declaración Universal de los Derechos Humanos y en la normativa de la Unión Europea.**

**La Declaración Universal de los Derechos Humanos<sup>3</sup> de 1948 establece en el artículo 12 que *"nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*.**

Dos años después, el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa, más conocido como la Convención Europea de Derechos Humanos, de 1950, establece en su artículo 8 que *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"*.

En tercer lugar, en el año 1981 se elaboró el Convenio 108 del Consejo de Europa con la finalidad de proteger a los individuos respecto al tratamiento automatizado de sus datos de carácter personal.

Por otra parte, la Carta de los Derechos Fundamentales de la Unión Europea, recoge en el artículo 8<sup>4</sup> que

<sup>3</sup> <http://www.un.org/es/universal-declaration-human-rights/>

<sup>4</sup> Artículo 8: Protección de Datos de Carácter Personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

*"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".*

En **España**, la regulación comienza en el año 1992 con la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (**LORTAD**). El objetivo de esta norma era principalmente desarrollar lo recogido en el artículo 18 de la Constitución Española de 1978 y establecer, por primera vez, la limitación del uso de la informática para garantizar la intimidad personal. La LORTAD marcó un hito histórico en nuestro país al ser la primera norma en materia de protección de datos aprobada.

Un aspecto que destacar de la LORTAD es que únicamente regulaba los tratamientos de datos personales que se realizaban en **soportes informatizados**, excluyendo el tratamiento de datos en formato papel.

El desarrollo reglamentario de la LORTAD llegó siete años después, con el Real Decreto 994/1999, de 11 de junio: Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (**RD 994/1999**), que como se ha señalado, únicamente establecía las medidas de seguridad para los ficheros informatizados dejando sin regular toda la información que se encontraba en formato papel.

En este periodo de tiempo, fue aprobada 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

---

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

(**Directiva 95/46/CE**), en la que se establece el marco jurídico en el que se desarrolló la LOPD.

Con el fin de llevar a cabo la trasposición de la directiva, en diciembre de 1999 se promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**LOPD**), que adaptó la legislación española a la Directiva Europea.

Su objetivo era regular el tratamiento de los datos y ficheros de carácter personal, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los tratan. Esta ley afectaba a todos los datos que referentes a personas físicas registrados independientemente del soporte en el que se encontraran, informático o papel.

Posteriormente fue aprobado el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**RLOPD**), que desarrolla los principios de la LOPD y las medidas de seguridad a aplicar en los sistemas de información. Se aplica al igual que la LOPD tanto a ficheros en soporte automatizado como en cualquier otro tipo de soportes, estableciendo medidas específicas para el tratamiento de los datos en papel.

Durante el año 2012 se comenzó a trabajar a nivel europeo en una nueva norma, que entró en vigor en mayo de 2016 y es aplicable desde el 25 de mayo de 2018. El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (**Reglamento General de Protección**

**de Datos o RGPD**). Esta norma supera el marco de la directiva, siendo de aplicación directa en todo el territorio de la UE, por lo que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación.

Por último, en diciembre de 2018 se publicó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de Derechos Digitales que, además de desarrollar algunos de los preceptos del RGPD, regula los derechos digitales tratando de "*garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución*".

## **2. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE<sup>5</sup>**

El proyecto de modificación de la normativa de protección de datos fue impulsado por la Comisión Europea en el año 2012, casi veinte después de la aprobación de la Directiva 95/46/CE.

Las razones para abordar la actualización de la normativa europea de protección de datos en especial para atender y regular los retos que se han planteado por:

<sup>5</sup> <https://www.boe.es/buscar/doc.php?id=DOUE L-2016-80807>

- La rápida evolución tecnológica.
- La globalización.

Estas dos realidades tenidas en cuenta por el legislador han dado lugar, tal y como lo expone el Considerando 6 del RGPD a:

El aumento del intercambio de datos personales, así como el aumento de la recogida de los datos de una forma muy significativa.

La evolución de la tecnología, con la consiguiente reducción de costes y la facilidad de utilización, que está permitiendo que las organizaciones, tanto públicas como privadas, puedan hacer uso de datos personales para realizar sus actividades en una escala que no había sido conocida anteriormente.

Existe otra realidad, vinculada con la actividad de las personas físicas, y es la difusión de información personal haciendo uso, en esencia, de las redes sociales.

- La evolución tecnológica afecta tanto a la economía como a la vida social, y según se indica en el propio RGPD facilitará más la libre circulación de los datos personales dentro de la UE, fuera a países terceros u organizaciones, debiendo elevar el nivel de protección.

Los cambios y avances expuestos necesitaban de un marco jurídico que garantizara de forma coherente la protección de los datos personales en la UE, era preciso reforzar la seguridad jurídica y práctica tanto de las personas físicas, que deben tener el control de sus propios datos personales, como de las organizaciones, públicas o privadas.

Por otra parte, el legislador es consciente, y así lo expone en el Considerando 9, que la protección de datos en la UE se ha aplicado de forma fragmentada en los distintos países a pesar de ser conscientes de la existencia de riesgos importantes para la protección de las personas físicas, en especial en todas las actividades que se realizan en línea, que se han incrementado sensiblemente.

Así mismo el diferente nivel de protección de los derechos y libertades ha dado lugar a dificultades para la libre circulación de los datos. ...*“Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE. (Considerando 9)”*.

Por estas razones y según se expone en el Considerando 10<sup>6</sup>, se optó por una norma de alcance general,

<sup>6</sup> 10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, 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 presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros

un Reglamento, que es de aplicación directa en todos los países de la Unión Europea, de forma que unifica los derechos y los deberes de la ciudadanía independientemente del país en el que se encuentren, estableciendo un nivel de protección equivalente en todos los Estados Miembros.

Si bien en el mismo Considerando 10 se recoge el reconocimiento de un margen de maniobra para que los estados miembros especifiquen sus propias normas.

El 27 de abril de 2016 se aprobó el **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (en adelante RGPD)** que entró en vigor el 24 de mayo de 2016, y es de obligado cumplimiento desde el **25 de mayo de 2018**.

La razón principal de este periodo de dos años para su plena aplicación, estuvo en facilitar a los Estados y a las organizaciones la adaptación a la nueva normativa, que en el caso de nuestro país supone un cambio sustancial, no tanto desde el punto de vista de adopción de medidas de seguridad, (el Real Decreto 1720/2007, identificaba muchas de las medidas que era necesario

---

cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

aplicar) como del cambio cultural que supone este reglamento, el cambio desde una aplicación reactiva, a una cultura de la proactividad, con lo que ello supone de aplicar la protección de datos desde el diseño y por defecto, la realización de análisis de riesgos, o la evaluación de impacto.

En algunos casos, no ha sido suficiente el periodo de adaptación, porque hoy podemos comprobar que muchas organizaciones no cumplen con lo exigido.

El RGPD persigue varios objetivos:

- la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal,
- garantizar la libre circulación de estos datos entre los Estados miembros, de forma que esta no puede ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en el tratamiento de sus datos personales.

En la Comunicación de la Comisión al Parlamento Europeo y al Consejo *“Las normas de protección de datos como facilitador de la confianza en la UE y más allá, haciendo balance”*, publicado el 24/07/2019 se indica que: *“Uno de los objetivos fundamentales del Reglamento era eliminar un panorama fragmentado de 28 leyes nacionales diferentes que existían en virtud de la anterior Directiva sobre protección de datos y proporcionar seguridad jurídica a particulares y empresas de toda la UE. Ese objetivo se ha cumplido en gran medida.”*

Como ya se ha señalado, el RGPD supone un nuevo paradigma en la protección de datos, un cambio en

la forma en que las organizaciones han de abordar el cumplimiento de esta normativa, se ha de atender a al principio de responsabilidad proactiva, principio que proviene la cultura anglosajona, en la que no se indica las medidas a cumplir, con el grado al que estábamos habituados en nuestra normativa.

En la aplicación del principio proactividad es la propia organización la que debe llevar a cabo un análisis de riesgos de los tratamientos de datos que realiza y atendiendo a dicho análisis debe definir las medidas técnicas, organizativas y legales que considere adecuadas para garantizar y acreditar que cumple con los principios y obligaciones que indica el RGPD, así como para atender los ejercicios de derechos relativos a esta materia que puedan presentar las personas interesadas ante la organización.

Las principales novedades que introduce el RGPD se enumeran, de forma breve, a continuación, y serán desarrolladas posteriormente con más detalle a lo largo de los diferentes capítulos<sup>7</sup>:

### **Ámbito de aplicación**

El Reglamento amplía el ámbito de aplicación territorial a los responsables y a los encargados del tratamiento no establecidos en la UE, cuando sus actividades

<sup>7</sup> Basado en el documento ¿Cuáles son las principales novedades del Reglamento General de Protección de Datos? de la Autoridad Catalana de Protección de Datos y en la Guía del Reglamento General de Protección de Datos para responsables de Tratamiento: <http://apdcat.gencat.cat/es/documentacio/RGPD/novetats/>

<https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>

ofrezcan bienes y servicios a personas que se encuentran en la UE (artículo 3-3 RGPD).

Se pretende evitar que empresas de fuera de Europa argumenten que no les aplica la normativa de protección de datos europea, al estar fuera del espacio europeo.

Con el RGPD siempre y cuando sus servicios se presten a ciudadanos que están en la UE se debe cumplir con la normativa de protección de datos.

Como curiosidad se puede observar a algunos periódicos norteamericanos informan que no es posible su conexión desde Europa para evitar la adaptación a la normativa europea.

### **Principios**

Hay que destacar que el RGPD incluye dos nuevos principios que ya se han señalado y sobre los que se profundizará posteriormente:

- Principio de responsabilidad proactiva, y
- Enfoque de riesgo.

Más adelante, en este mismo capítulo se desarrollan todos los principios que han de cumplirse para el tratamiento de los datos personales.

### **Nuevas categorías de datos**

Posteriormente, en el capítulo 2, se expondrá qué datos son especialmente sensibles para los individuos y cómo en la normativa anterior no se encontraban dentro de esta categoría el tratamiento de datos genéticos y datos biométricos.