GUÍA RÁPIDA FRANCIS LEFEBVRE

Protección de datos
Aplicación del RGPD

Actualizado a 25 de mayo de 2018

Es una obra realizada por iniciativa
y bajo la coordinación
de la Redacción de
Francis Lefebvre
sobre la base de un estudio técnico
cedido a la editorial por

Coordinador:
EMILIO RAMÍREZ DE MATOS

Autores:

JESÚS COBOS TUBILLA
Consultor en sistemas de seguridad y privacidad.

IGNACIO DE LUIS OTERO
Abogado.

PABLO LINDE PUELLES
Abogado.

EMILIO RAMÍREZ DE MATOS
Doctor en Derecho. Abogado.

MARÍA RIUS PEÑA
Abogada.

Lefebvre-El Derecho, S. A.
Monasterios de Suso y Yuso, 34. 28049 Madrid. Teléfono: (91) 210 80 00. Fax: (91) 210 80 01
www.efl.es
Precio: 33,28 € (IVA incluido)

ISBN: 978-84-17317-41-6
Depósito legal: M-17990-2018

Impreso en España
por Printing'94
Paseo de la Habana, 9-11. 28036 Madrid

Plan general

Abreviaturas

AEAT	Agencia Estatal de la Administración Tributaria
AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
APDCAT	Autoridad Catalana de Protección de Datos
ARCO	Acceso, Rectificación, Cancelación y Oposición
art.	artículo
CC	Código Civil (RD 24-7-1889)
CDAE	Código Deontológico de la Abogacía Española
CGAE	Consejo General de la Abogacía Española
CGPJ	Consejo General del Poder Judicial
Const	Constitución
Dir	Directiva
DPD	Delegado de Protección de Datos
EDJ	El Derecho Jurisprudencia
EEE	Espacio Económico Europeo
EGAE	Estatuto General de la Abogacía Española
GT29	Grupo de Trabajo del artículo 29
Inf	Informe
L	Ley
LEC	Ley de Enjuiciamiento Civil (L 1/2000)
LGT	Ley General Tributaria (L 58/2003)
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999)
LOPJ	Ley Orgánica del Poder Judicial (LO 6/1985)
LSSI	Ley de servicios de la sociedad de la información y de comercio electrónico (L 34/2002)
ONIF	Equipo Central de Información de la Oficina Nacional de Investigación del Fraude
Proyecto	Proyecto 121/000013 de Ley Orgánica de Protección de Datos de Carácter Personal
RD	Real Decreto
Resol	Resolución
RGPD	Reglamento 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 (Rgto UE/2016/679)
Rgto	Reglamento
RLOPD	Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RD 1720/2007)
SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias
TCo	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
Tratado FUE	Tratado de Funcionamiento de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea

CAPÍTULO 1

Consideraciones previas

1. Principales novedades

- ✓ La **regulación** del derecho a la protección de datos es ahora **uniforme** en la Unión Europea.
- ✓ Se aplica directamente la normativa del Reglamento General de Protección de Datos.
- ✓ En España está pendiente de aprobarse una **nueva ley orgánica** que sustituya a la LOPD, para aclarar y dar coherencia al sistema normativo, y, en su caso, un nuevo reglamento de desarrollo.

2. Derecho fundamental a la protección de datos de carácter personal

(Const art.18.1 y 4)

En el ordenamiento jurídico español el derecho a la protección de datos de carácter personal es un derecho constitucional fundamental de las personas físicas, que el Tribunal Constitucional, cuya doctrina ha sido esencial en la configuración del derecho, deriva de la Const art.18.4:
«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».
Inicialmente se vino hablando de «**libertad informática**». El Tribunal Constitucional entendió que la Const art.18.4 contenía un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, constituye en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática», por lo que se dio en llamar «libertad informática» (TCo 253/1993; reiterado luego en TCo 143/1994; 11/1998; 94/1998; 202/1999).
La garantía de la **vida privada de la persona** y de **su reputación** tienen una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad y que se traduce en un derecho de control sobre los datos relativos a la propia persona (Const art.18.1).
La llamada «libertad informática» se definió como el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*), comprendiendo el derecho a la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (TCo 11/1998).
Es en la sentencia de 30 de noviembre de 2000, en la que define con fortuna el derecho constitucional a la protección de datos y su contenido (TCo 292/2000).

Poder de disposición y de control El derecho fundamental a la protección de datos implica un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos puede proporcionarse a un tercero, sean las Administraciones públicas o un particular, o cuáles puede este ter-

cero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.
Estos **poderes de disposición y control** sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.
Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como **complementos** indispensables:
– la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y
– el poder oponerse a esa posesión y a su uso.
El derecho fundamental a la protección de datos es un **derecho** relacionado con otros derechos, pero **autónomo**.
Señalaba el Tribunal Constitucional que el derecho fundamental a la intimidad (Const art.18.1) no aporta por sí solo una protección suficiente frente a la realidad derivada del progreso tecnológico y la informática y que con la inclusión del vigente art.18.4 Const el constituyente puso de relieve que era consciente de los **riesgos** que podría entrañar el **uso de la informática** y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona (TCo 292/2000).
Esto es, incorporando un **instituto de garantía** «como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona», pero que es también, «en sí mismo, un derecho o libertad fundamental» (TCo 254/1993).
De manera que el constituyente quiso garantizar mediante el actual art.18.4 Const no solo un **ámbito de protección específico** sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el referido art.18.1.
El art.18.4 de la Const fue esgrimido por primera vez en el caso de un ciudadano a quien le denegó el Gobierno Civil de Guipúzcoa información sobre los datos que sobre su persona poseía (resuelto por TCo 254/1993). Y lo dicho en esta pionera Sentencia se fue aquilatando en las posteriores:
1. La relativa a las **normas reguladoras del número de identificación fiscal** (TCo 143/1994).
2. La que declaró contrario a la libertad sindical (Const art.28), en relación con la Const art.18.4, el uso por una empresa del **dato de la afiliación sindical** para detraer haberes de los trabajadores con ocasión de una **huelga** promovida por determinado sindicato (TCo 11/1998, cuya doctrina ha sido reiterada en una larga serie de sentencias de este Tribunal resolviendo idéntica cuestión).
3. La que, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre **bajas por incapacidad temporal**, se apreció que el almacenamiento sin cobertura legal en soporte informático de los **diagnósticos médicos** del trabajador sin mediar su consentimiento expreso constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales (TCo 202/1999).
Dice el Tribunal Constitucional que este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad (Const art.18.1), con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art.18.4 Const debe limitar el uso de la informática:
a) Desarrollando el derecho fundamental a la protección de datos (Const art.81.1).
b) Regulando su ejercicio (Const art.53.1).
La **peculiaridad** de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su

distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.
La función del derecho fundamental a la intimidad de la Const art.18.1 es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (TCo 144/1999).
En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un **poder de control** sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.
El derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (TCo 134/1999; 144/1999; 98/2000; 115/2000), es decir, el poder de **resguardar su vida privada** de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del **acceso o divulgación indebidas** de dicha información.
Pero ese **poder de disposición** sobre los propios datos personales nada vale si el afectado desconoce:
– **qué** datos son los que se poseen por terceros,
– **quiénes** los poseen, y
– **con qué fin**.
De ahí la **singularidad del derecho a la protección de datos**, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por la Const art.18.1, sino a la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al **respeto de la dignidad personal** (TCo 170/1987) como el **derecho al honor**, citado expresamente en la Const art.18.4, e igualmente, en expresión bien amplia del propio art.18.4, al pleno ejercicio de los derechos de la persona.

Objeto de protección El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que tengan incidencia o sean relevantes para el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.
De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que la Const art.18.1 otorga, sino los datos de carácter personal.
Por consiguiente, también alcanza a aquellos **datos personales públicos**, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los **datos** amparados son todos aquellos **que identifiquen o permitan la identificación de la persona**, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Contenido De acuerdo con el Tribunal Constitucional, el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar de la Const art.18.1. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona

el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (TCo 73/1982 2-12-82; 110/1984; 89/1987; 231/1988; 197/1991; 134/1999; 144/1999; 115/2000), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio **impone a terceros deberes jurídicos**, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber:
a) Derecho a que se requiera el **previo consentimiento** para la recogida y uso de los datos personales.
b) Derecho a **saber y ser informado** sobre el destino y uso de esos datos.
c) Derecho a **acceder, rectificar y cancelar** dichos datos.
En definitiva, el poder de disposición sobre los datos personales (TCo 254/1993).
Son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los **derechos del afectado** a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del:
– derecho a ser informado de quién posee sus datos personales y con qué fin, y
– el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir:
• exigiendo del **titular del fichero** que le informe de qué datos posee sobre su persona,
• accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso,
• requerirle para que los rectifique o los cancele.

Precisiones A nivel europeo, también tiene la consideración de derecho fundamental:
– la Carta de los Derechos Fundamentales de la Unión Europea art.8.1 y
– el Tratado de Funcionamiento de la Unión Europea art.16.1 (en adelante, Tratado FUE).
Establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

3. Nuevo Reglamento General de Protección de Datos
(RGPD)

La Directiva 95/46/CE del Parlamento Europeo y del Consejo trató de armonizar 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 y garantizar la libre circulación de estos datos entre los Estados miembros.
El Tratado de Funcionamiento de la Unión Europea encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos (Tratado FUE art.16.2).
Actualmente, la regulación del derecho a la protección de datos es uniforme en la Unión Europea, toda vez que se encuentra regulado por un Reglamento, norma jurídica de Derecho comunitario con alcance general y eficacia directa, aplicable en todos los Estados de la Unión por cualquier autoridad o particular, sin que sea precisa ninguna norma jurídica de origen interno o nacional que la incorpore para completar su eficacia plena.
Si bien, en los casos en que el reglamento establezca que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del reglamento. Asimismo, puede ser invocada la **tutela jurisdiccional** ante los tribunales nacionales o comunitarios por los particulares.
Se trata del **Reglamento General de Protección de Datos**: Rgto UE/2016/679 del Parlamento Europeo y del Consejo de 27-4-16 relativo a la protección de las perso-

nas 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 Dir 95/46/CE (en adelante, RGPD), que entró en vigor el 25-5-2016 y ha comenzado a aplicarse dos años después de su entrada en vigor, el 25-5-2018.

Así, desde el 25-5-2018 la **regulación del derecho** a la protección de datos es **uniforme** en la Unión Europea.

El RGPD pretende con su **eficacia directa** superar los obstáculos que impidieron la finalidad armonizadora de la Dir 95/46/CE. La incorporación 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.

EL RGPD se justifica, pues, en la necesidad de establecer un **marco uniforme** más sólido y coherente para la protección de datos en la Unión Europea, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior.

El RGPD es una **repuesta a la rápida evolución tecnológica y** la **globalización** que han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa.

La **tecnología** permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha **transformado tanto la economía como la vida social**, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

Objeto y ámbito de aplicación Hay que destacar que el RGPD:

1. Protege a las personas físicas, **independientemente de su nacionalidad o** de su **lugar de residencia**, en relación con el tratamiento de sus datos personales.

2. Se aplica a toda la información relativa a una **persona física identificada o identificable**. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, se consideran información sobre una persona física identificable.

Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.

3. No se aplica a la protección de datos personales de **personas fallecidas**. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

4. No regula el tratamiento de datos relativos a **personas jurídicas**.

5. No se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una **actividad exclusivamente personal o doméstica** y, por tanto, sin conexión alguna con una actividad profesional o comercial.

Entre las actividades personales o domésticas cabe incluir:

- la correspondencia y la llevanza de un repertorio de direcciones, o
- la actividad en las redes sociales y
- la actividad en línea realizada en el contexto de las citadas actividades.

No obstante, el RGPD Reglamento se aplica a los **responsables o encargados del tratamiento** que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

6. Se aplica a todo tratamiento de datos personales realizados por una **persona jurídica o profesional autónomo** establecido en la Unión Europea, independientemente de que el tratamiento efectivo tenga lugar o no en territorio de la Unión. El estableci-

miento implica el ejercicio de manera efectiva y real de una actividad económica o profesional a través de modalidades estables.
La forma jurídica que revistan tales modalidades ya sea una sociedad, una sucursal de estas, otro tipo de personalidad jurídica o el ejercicio autónomo, no es el factor determinante al respecto.
7. Se aplica al tratamiento de datos personales de interesados que se encuentran en la Unión Europea por un **responsable o** un **encargado no establecido en la Unión** si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago.
Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera **accesibilidad del sitio web** del responsable o encargado o de un intermediario en la Unión, de una dirección de **correo electrónico** u otros datos de contacto, o el **uso de una lengua** generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que se encuentran en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.
8. Se aplica al tratamiento de datos personales de los interesados que se encuentran en la Unión por un responsable o encargado cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este **comportamiento tenga lugar en la Unión Europea**.
Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un **seguimiento en internet**, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

4. Normativa española

A nivel legislativo español, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la LO 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (conocida como LORTAD).
La LO 5/1992 fue reemplazada por la LO 15/1999, de 5 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), a fin de incorporar a nuestro Derecho la Dir 95/46/CE. Esta LO supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España. Esta fue desarrollada por el RD 1720/2007, 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 (en adelante, RLOPD).
Con el RGPD vigente, los Estados miembros de la Unión Europea tienen la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del RGPD. Tales disposiciones pueden establecer de forma más precisa **requisitos** concretos para el tratamiento de datos personales con otros fines por parte de las autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión.
El RGPD contiene un buen número de **habilitaciones**, cuando no imposiciones, **a los Estados miembros**, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos

tengan la posibilidad de incorporar al Derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

La adaptación al RGPD (aplicable desde 25-5-2018), según establece su art.99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la LOPD, para aclarar y dar coherencia al sistema normativo.

El **proyecto de la nueva Ley Orgánica de Protección de Datos de Carácter Personal** se publicó en el Boletín Oficial de las Cortes Generales de 27-11-2017, y, a fecha de publicación de esta Guía, continúa su tramitación parlamentaria.

CAPÍTULO 2

Nociones para la aplicación del RGPD

1. Principales novedades

Entre las principales novedades del RGPD, podemos destacar, a grandes rasgos las siguientes:

- ✓ Dos elementos de carácter general constituyen la mayor innovación del RGPD para los responsables se proyectan sobre todas las obligaciones de las organizaciones: el **principio de responsabilidad proactiva** y el **enfoque de riesgo**.
- ✓ La base principal para el tratamiento de datos es el **consentimiento inequívoco**. Aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.
  A diferencia del régimen anterior de la LOPD y del RLOPD, el RGPD no admite formas de consentimiento tácito o por omisión, ya que se basan en la inacción.
- ✓ Se establece una **lista exhaustiva de la información** que debe proporcionarse a los interesados (más amplia que la que actualmente contiene la LOPD) y se añade:
  • Base jurídica del tratamiento.
  • Intención de realizar transferencias internacionales.
  • Datos del Delegado de Protección de Datos (si lo hubiere).
  • Elaboración de perfiles.
- ✓ El responsable ha de poder probar que ha informado y que ha obtenido el consentimiento.
- ✓ El RGPD contiene **obligaciones** expresamente dirigidas a los **encargados**.
- ✓ Los **contratos de encargo** concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar este contenido, sin que sean válidas las remisiones genéricas al artículo del RGPD que los regula.

- ✓ El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. Todos los responsables deben realizar una **valoración del riesgo** de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de:
  - los tipos de tratamiento;
  - la naturaleza de los datos;
  - el número de interesados afectados;
  - la cantidad y variedad de tratamientos que una misma organización lleve a cabo.
- ✓ Responsables y encargados deben mantener un **registro de operaciones de tratamiento** en el que se contenga la información que establece el RGPD.
- ✓ Desaparece la obligación de inscribir los ficheros ante la AEPD.
- ✓ Protección de datos desde el **diseño y por defecto**:
  - Desde el inicio, los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD.
  - Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.
- ✓ Antes se determinaba con detalle las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento. En el RGPD, los responsables y encargados han de establecer las **medidas técnicas y organizativas** apropiadas para garantizar un nivel de seguridad adecuado **en función de los riesgos** detectados en el análisis previo.
  El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD no seguirá siendo válido de forma automática tras la fecha de aplicación del RGPD.
- ✓ Los responsables de tratamiento deben realizar una **Evaluación de Impacto sobre la Protección de Datos** (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un **alto riesgo para los derechos y libertades** de los interesados.
- ✓ Cuando se produzca una **violación de la seguridad** de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.
- ✓ El RGPD establece la figura del **Delegado de Protección de Datos** (DPD), que será obligatorio en:
  - Autoridades y organismos públicos.
  - Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
  - Responsables o encargados que tengan entre sus actividades principales el tratamiento a **gran escala** de datos sensibles y de **datos relativos a condenas e infracciones penales**.

2. Guía de cumplimiento. Documentos de la AEPD

Una vez introducidos en el marco normativo actual de la protección de datos de carácter personal, hemos de dibujar una **guía de cumplimiento**; y es que, a nuestro entender, el RGPD deja abiertas áreas de aplicación y procesos de adecuación, si

bien es cierto que las **autoridades de control** han de facilitar la labor estableciendo guías de cumplimiento.
En este sentido la Agencia Española de Protección de Datos (AEPD) ha elaborado un conjunto de **documentos relevantes, de acceso libre** en su página web (www.agpd.es) entre los que cabe destacar:
– Guía del Reglamento General de Protección de Datos para responsables de tratamiento.
– Guía para el cumplimiento del deber de informar.
– Directrices para la elaboración de contratos entre responsables y encargados del tratamiento.
– Guía Práctica de Análisis de Riesgos.
– Guía Práctica de Evaluaciones de Impacto.
– Listado de Cumplimiento Normativo.
Ahora nosotros pretendemos ayudar a marcar esa senda utilizando el RGPD y, para entender cómo se ha de dibujar, partimos de tres elementos básicos:
a) Los **principios** relativos al tratamiento de datos.
b) El **diseño** del tratamiento de datos.
c) Los **intervinientes** en el tratamiento de datos.

3. Principios y condiciones

(RGPD art.4, 5 y considerando 15)

Primero, y antes de entrar en los principios básicos, hemos de acercarnos a la definición de «tratamiento de datos» y ello desde una perspectiva evolutiva, ya que, y en palabras del RGPD, «la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas» (RGPD considerando 15); ello obedece a la vertiginosa evolución tecnológica y a la globalización.
Debe extenderse la protección que pretende el RGPD, tanto al **tratamiento automatizado** de datos como a su **tratamiento manual**, y ello cuando los datos figuren en un fichero o estén destinados a ser incluidos en él.
Podemos aproximarnos a una definición de «tratamiento automatizado» como el que comprende cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (RGPD art.4.2).
La génesis, el **punto de partida** en el tratamiento de datos de carácter personal, está en los pilares que legitiman su tratamiento; sus principios.