

TEMA 27. LA POLÍTICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

**RÉGIMEN JURÍDICO. EL REGLAMENTO UE
2016/679, DE 27 DE ABRIL, 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.**

**PRINCIPIOS Y DERECHOS. OBLIGACIONES.
EL DELEGADO DE PROTECCIÓN DE DATOS
EN LAS ADMINISTRACIONES PÚBLICAS. LA
AGENCIA ESPAÑOLA DE PROTECCIÓN DE
DATOS.**

Actualizado a 04/05/2023

1. REGLAMENTO GENERAL DE PROTECCION DE DATOS

El RGPD entró en vigor en mayo de 2016, siendo de plena aplicación desde mayo de 2018.

Al ser un reglamento, no requiere transposición al derecho nacional, en cualquier caso, los Estados miembros pueden elaborar una ley aclarando aspectos que no lo contravengan, pero en caso de desarrollarse una ley está deberá ser una Ley Orgánica, por ser la protección de datos personales un derecho fundamental. Por último, en caso de conflicto entre la Ley Orgánica y el Reglamento prima el Derecho de la Unión Europea.

Ámbito de aplicación material:

- Se aplica al **tratamiento total o parcialmente automatizado de datos personales**, así como al **tratamiento no automatizado** de datos personales contenidos o destinados a ser incluidos en un fichero.
- **Excepto:**
 - Actividad **no comprendida** en el ámbito de aplicación del Derecho de la Unión.
 - Efectuado por una persona física en el ejercicio de actividades exclusivamente **personales o domésticas**.
 - Por parte de las **autoridades** competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

Ámbito territorial:

Se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, **independientemente de que el tratamiento tenga lugar en la Unión o no**.

DEFINICIONES

- Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- Datos personales: toda información sobre una **persona física identificada o identificable** («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador.
- Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física.
- Seudonimización: Proceso por el que los datos ya no pueden atribuirse a una persona sin información adicional. Ejm: Quitar poner una id a los datos guardar en otro lado los personales.
- Anonimización: Tratamiento por el cual se disocian los datos haciendo imposible ser atribuidos a una persona.
- Responsable de tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**.
- Encargado de tratamiento: La persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales** por cuenta del responsable del tratamiento.

PRINCIPIOS

- Licitud, transparencia y lealtad.
- Limitación de la finalidad.
- Minimización de datos.



- De exactitud.
- Limitación del plazo de conservación.
- De integridad y confidencialidad.
- Y el de responsabilidad proactiva.

LICITUD DEL TRATAMIENTO

El tratamiento será lícito si se da alguna de las siguientes condiciones (art. 6):

- Hay consentimiento.
- Necesario para cumplir un contrato.
- Hay obligación legal.
- Necesario para intereses vitales.
- Hay interés público.
- El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

CATEGORÍAS DE DATOS ESPECIALES

Son origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Queda **prohibido el tratamiento excepto**, entre otras, si se da una de las siguientes (art. 9):

- Hay consentimiento explícito.
- Necesario para el cumplimiento de obligaciones y el ejercicio de derechos.
- Para proteger intereses vitales.
- Asociaciones, partidos políticos, sindicatos, etc.
- Si el interesado los ha hecho manifiestamente públicos.
- Interés público esencial.

DERECHOS

- Transparencia
- Derecho de acceso
- Derecho de rectificación
- Supresión - Derecho al olvido
- Limitación del tratamiento
- Portabilidad
- Y la oposición de características

OBLIGACIONES

- A la protección de datos desde el diseño y por defecto por parte del Responsable del tratamiento.
- Las responsabilidades de los corresponsables lo serán en función de su relación interna y en relación con el interesado, para lo que será aconsejable la firma de un contrato que lo determine.
- Los responsables no establecidos en la Unión Europea, cuando el Reglamento se aplique a sus actividades de tratamiento, deberán designar un representante en la Unión.

- Cada responsable llevará un **registro de las actividades de tratamiento**.
- El responsable y el encargado del tratamiento cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.
- El responsable y el encargado del tratamiento **aplicarán medidas técnicas y organizativas apropiadas** para garantizar un nivel de seguridad adecuado al riesgo. **En caso de violación** de la seguridad de los datos personales, el responsable del tratamiento la notificará a la **autoridad de control** competente y, de ser posible, a más tardar **72 horas** después de que haya tenido constancia de ella, si supone un riesgo para los derechos y libertades de las personas, y a los interesados si supone un alto riesgo.
- Con objeto de determinar las medidas de seguridad a aplicar será necesario una **evaluación del riesgo**, una vez evaluado el riesgo será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.
- El Responsable del tratamiento deberá realizar una evaluación de impacto cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un **alto riesgo** para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.
- Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica. Cuando no esté en las listas de UE será posible también cuando el responsable ofrezca las garantías adecuadas.

2. LEY ORGANICA 3/2018 DE PROTECCIÓN DE DATOS Y GARANTIA DE DERECHOS DIGITALES

La ley orgánica sigue en todo momento lo establecido en el Reglamento, destacando:

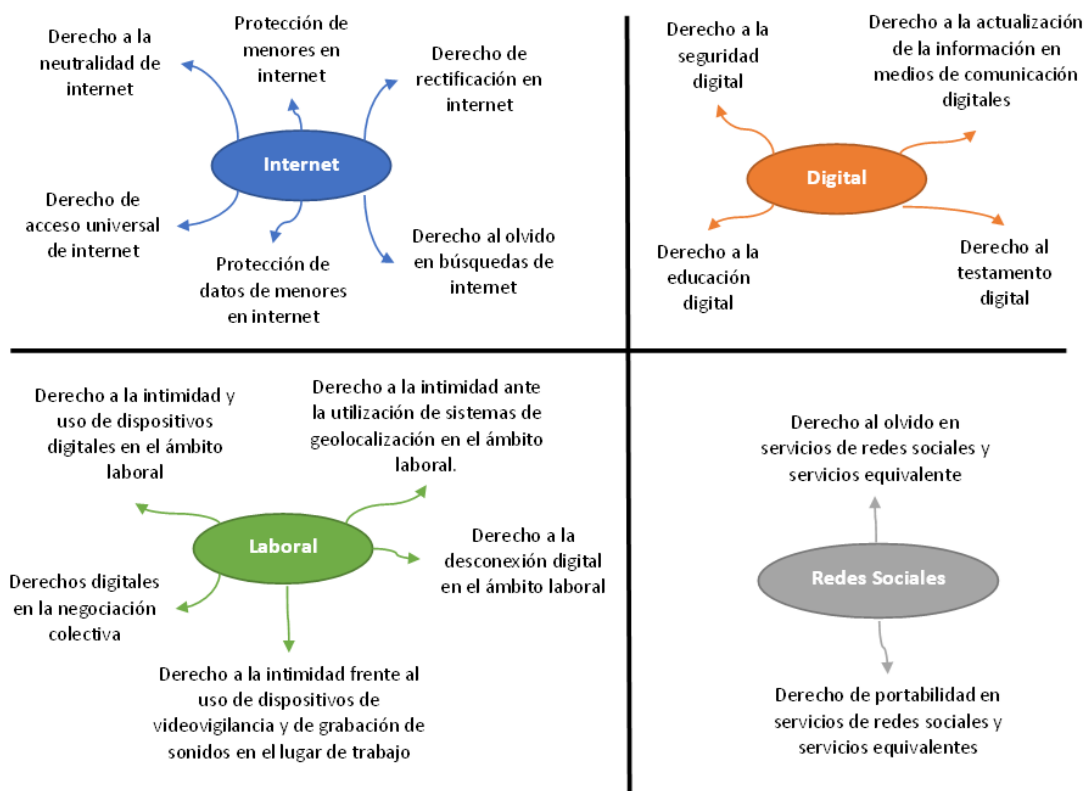
- Se regulan los datos referidos a las **personas fallecidas**.
- La Ley facilita que los ciudadanos puedan ejercitar sus derechos al exigir que los medios sean fácilmente accesibles y que se den a conocer con un **sistema de información por capas**.
- Se reconoce el **derecho de acceso y, en su caso, de rectificación o supresión** por parte de quienes tuvieran vinculación con personas fallecidas por razones familiares o de hecho y a sus herederos.
- La Ley fija en **14 años la edad para prestar consentimiento de manera autónoma**.
- La Ley refuerza las obligaciones del **sistema educativo** para garantizar la formación del alumnado en el uso seguro y adecuado de internet.
- El texto regula el **derecho al olvido en redes sociales y servicios de la sociedad de la información**.
- Se recoge los **sistemas de denuncias internas anónimas**.
- La Ley actualiza las garantías del **derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación** de sonidos en el lugar de trabajo y en relación con el uso de dispositivos digitales puestos a disposición de los empleados.
- Se **regulan los sistemas de información crediticia**.
- Cabe destacar que la Ley propone **garantizar los derechos digitales de la ciudadanía**.
- Se remarca que los poderes públicos deberán impulsar políticas que hagan efectivos los derechos digitales de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos.
- Es importante destacar la modificación que realiza la LO 3/2018 de la Ley 39/2015.

GARANTÍA DE DERECHOS DIGITALES

Incluida en el Título X Garantía de Derechos Digitales y se divide en:

- Derechos generales de los ciudadanos en internet: este bloque incluye los arts. 79 a 82, 96 y 97.
- Derechos específicos relacionados con los menores: arts. 83, 84, 92 y 97.2 (en parte).
- Derechos relacionados con el ámbito laboral: arts. 87 a 91.
- Derechos relacionados con los medios de comunicación digitales: arts. 85 y 86.
- Derecho al olvido en internet: arts. 93 y 94.
- Derecho a la portabilidad en las redes sociales: art. 95.
- Derecho al testamento digital (art. 96)
- Políticas de impulso de los derechos digitales (art. 97)

Para facilitar la memorización de los derechos los organizamos en cuatro bloques:



El Gobierno deberá presentar un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados dando cuenta de la evolución de los derechos, las garantías, los mandatos y de las medidas necesarias para promover su impulso y efectividad.

3. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La AEPD debe supervisar la aplicación de la ley orgánica y del Reglamento (UE) 2016/679, y quedan fuera de su ámbito de aplicación los artículos respecto a los derechos en la Era digital, los cuales se asignarán como competencia de otro organismo según el pendiente desarrollo normativo.

El Real Decreto 389/2021 aprueba el Estatuto de la Agencia Española de Protección de Datos por el cual se adapta la organización y funcionamiento de la Agencia Española de Protección de Datos.

4. PROTECCIÓN DE DATOS Y EL PROCEDIMIENTO ADMINISTRATIVO COMÚN

La LO 3/2018 **modifica la Ley 39/2015** indicando que no aportar documentos es un derecho del interesado, tanto si el documento lo tiene la administración actuante como cualquier otra. Las Administraciones deberán recabarlos utilizando sus redes corporativas, la plataforma de intermediación u otros sistemas electrónicos habilitados al efecto, salvo que el interesado se oponga a ello, lo que no podrá hacerse en caso de procedimientos sancionadores o de inspección.

La Disposición adicional séptima de la LO 3/2018 sobre la Identificación de los interesados en las **notificaciones por medio de anuncios y publicaciones de actos administrativos**, indica que:

1. Se identificará mediante su nombre y apellidos, añadiendo cuatro cifras aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o equivalente.
2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros.

Por último, la Disposición adicional octava, establece la **Potestad de verificación de las Administraciones Públicas**.

5. EL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS

- Figura responsable de la privacidad, con una función preventiva y proactiva.
- Conocimientos especializados de Derecho.
- Responsable y Encargado del tratamiento son los que designarán la nueva figura.
- Las entidades deberán designar un DPD, siempre que:
 - ✓ Administraciones públicas
 - ✓ Tratamiento de datos a gran escala
 - ✓ Tratamiento de categorías especiales de datos; o bien relativos a condenas e infracciones penales.

El Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento,
- Supervisar el cumplimiento de lo dispuesto en el Reglamento,
- Supervisar la asignación de responsabilidades,
- Supervisar la concienciación y formación,
- Supervisar las auditorías correspondientes,
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto,
- Cooperar con la autoridad de control,
- Actuar como punto de contacto de la autoridad de control.

En particular en relación con el Delegado de Protección de Datos en las AAPP:

- El RGPD prevé que cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público se pueda designar un único delegado de protección de datos para varios de



estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño. Su adscripción dentro de la estructura de la organización debe hacerse a órganos o unidades con competencias y funciones de carácter horizontal.

- El DPD podrá desarrollar su actividad a tiempo completo o a tiempo parcial y podrá formar parte de la plantilla o desempeñar sus funciones en el marco de un contrato de servicios.
- En entidades de menor tamaño será posible que el DPD compagine sus funciones con otras. Si éste es el caso, debe tenerse en cuenta la necesidad de evitar conflictos de intereses.