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 04/05/23

CONTEXTO NORMATIVO

NORMA	OBSERVACIONES
HISTÓRICO	
Ley orgánica 5/1992 de tratamiento automatizado de datos personales. **Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.** **Ley Orgánica 15/1999, de protección de datos de carácter personal** **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.**	Derogado
ACTUALIDAD	
Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (RGPD)	
Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del derecho español a la normativa de la unión europea en materia de protección de datos.	Aprobado por el Gobierno con medidas urgentes a aplicar hasta la aprobación de la Ley Orgánica que debido a causas políticas no había podido abordarse en tiempo.
Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.	Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal Deroga el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. Deroga cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.
Real Decreto-Ley 14/2019, de 31 de octubre , por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.	Dentro del Capítulo III, artículo 5, en el que se modifica la Ley de Contratos del Sector Público, se establece la obligación de todo contratista con la administración de respetar la normativa nacional y europea de protección de datos.

POLÍTICA DE PROTECCIÓN DE DATOS

Una política de protección de datos tiene por objeto dar a conocer el modo en que una empresa u organismo obtiene, trata, y con qué medidas protege los datos personales que sus empleados, clientes o usuarios le facilitan o recogen a través de su sitio web, formularios y/o cookies, etc, así mismo, informa de los medios puestos a disposición para permitir ejercer los derechos a los propietarios de los datos.

RGPD

El RGPD gira alrededor del concepto de Registro de Tratamiento, en lugar de alrededor del concepto de la Inscripción de ficheros, como hacía la antigua Directiva y la LOPD ya derogada, esto queda reflejado en el artículo 30 del Reglamento.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental que aparece reflejado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

El Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

RÉGIMEN JURÍDICO

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

La Comisión, buscando evitar la fragmentación jurídica entre los Estados miembros, publica un Reglamento que no requiere transposición al derecho nacional, en cualquier caso, los Estados miembros pueden elaborar una ley aclarando o desarrollando aspectos que no contravengan lo indicado en el Reglamento, esta ley deberá ser una Ley Orgánica por ser la protección de las personas físicas en relación con el tratamiento de datos personales un derecho fundamental protegido por el artículo 18.4 de la Constitución española. En caso de conflicto entre la Ley Orgánica y el Reglamento prima el Derecho de la Unión, es decir el Reglamento.

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 los datos personales de una tabla y guardarlos en otra tabla, y que esas dos tablas se relacionen por un ID generado a través de un HASH que solo podrá descubrir aquel que tenga permisos para ello.
- 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

El Reglamento General de Protección de Datos señala un conjunto de principios que los responsables y encargados del tratamiento deben observar al tratar datos personales:

- Principio de **licitud**, **transparencia** y **lealtad**.
- Principio de **limitación de la finalidad**, que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de **minimización de datos**, es decir, que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Principio de **exactitud**, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.
- Principio de **limitación del plazo de conservación** por el que debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o desprovistos de todo elemento que permita identificar a los interesados.
- Principio de **integridad y confidencialidad**, que impone a quienes tratan datos la obligación de actuar proactivamente en la protección frente a cualquier riesgo que amenace su seguridad.
- y el principio denominado de **responsabilidad proactiva**, según el cual los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento se lleva a cabo de conformidad con el Reglamento.

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 EN EL RGPD

- Transparencia (art. 12): El responsable deberá facilitar al interesado la información indicada cuando este ejerza sus derechos, este tendrá **un mes** para responder a las solicitudes, en caso contrario se podrá presentar una reclamación ante la autoridad pertinente (AEPD). La información facilitada, preferiblemente por medios electrónicos, será de carácter **gratuito** a no ser que sea excesivamente repetitivo o haya generado costes administrativos.
- Derecho de acceso (art. 15).
- Derecho de rectificación (art. 16).
- Supresión - Derecho al olvido (art. 17).
- Limitación del tratamiento (art. 18).
- Portabilidad (art. 20).
- Oposición de características (art. 21).
- Y el derecho a no ser objeto de decisiones basadas en el tratamiento automatizado (art. 22).

El responsable del tratamiento tiene obligación de dar respuesta a toda solicitud sobre el ejercicio de derechos en el **plazo máximo de un mes** desde su recepción, salvo que, dada la complejidad o el número de solicitudes, no pueda atenderse, en cuyo caso se podrá prorrogar hasta dos meses. En dicho caso, el responsable, en el plazo de un mes desde que reciba la solicitud, y sin dilación indebida, tendrá que informar al interesado de dicha circunstancia e indicar las razones de la dilación.

OBLIGACIONES

Obligaciones de responsabilidad

- En base al principio de responsabilidad, existe la obligación del responsable del tratamiento a la hora de cumplir el presente Reglamento y de demostrar su observancia, incluso mediante la adopción de políticas y mecanismos internos que garanticen dicha conformidad.
- La protección de datos desde el diseño y por defecto por parte del Responsable.

- Cada responsable llevará un **registro de las actividades de tratamiento** (art. 30) efectuadas bajo su responsabilidad, no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales.
- El responsable y el encargado del tratamiento cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Seguridad de los datos personales (art. 32)

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.

Evaluación de impacto (EIPD, artículo 35)

Es una Metodología de evaluación de riesgos y adopción de las medidas necesarias para la protección de los datos, evitando y minimizando el impacto. Es necesario llevarlo a cabo en los siguientes tratamientos:

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.
El contenido de una EIPD es el siguiente (ver la guía de elaboración de EIPD de la AEPD):

- Descripción de las operaciones de tratamiento previstas, los fines del tratamiento.
- Medidas para afrontar los riesgos y mecanismos que garanticen la protección de los datos personales

Análisis de 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.

En relación con las medidas de seguridad en el ámbito del sector público, en la Disposición adicional primera de la Ley Orgánica 3/2018, se señala que los responsables deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas vinculadas a los mismos sujetas al Derecho privado.

Transferencias Internacionales

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.

IMPACTO DEL RGPD EN LAS AAPP

El Esquema Nacional de Seguridad y el RGPD establecen la obligación de que las Administraciones Públicas realicen análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicables.

En este sentido, la AEPD ha publicado un documento (https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf) (disponible también en la carpeta Contenidos) en el que pone de manifiesto que esas medidas de seguridad −en el caso de las AAPP− estarán marcadas por los criterios establecidos en el Esquema Nacional de Seguridad.

ASSI – RGPD

Es una aplicación que permite a cada Responsable de Tratamiento de Datos Personales la ejecución de las siguientes actividades, para cada uno de los Tratamientos:

- Realizar el análisis de riesgos y la evaluación de impacto. Esto determinará el conjunto de medidas de seguridad del Esquema Nacional de Seguridad (ENS), Medidas ENS Tipo I o Medidas ENS Tipo II, a aplicar para securizar el tratamiento de datos personales (TDP).
- Proporcionar la información necesaria de cada TDP que hay que incluir en el Registro de Actividades de Tratamiento exigido por el Reglamento General de Protección de Datos (RGPD).
- Verificar el cumplimiento del resto de aspectos normativos del RGPD.

Los responsables de tratamiento cumplimentan unos cuestionarios y a partir de estos ofrece un conjunto de informe y documentos que le ayudan al cumplimiento de las obligaciones que establece el RGPD.

SANCIONES

Sanción por una falta grave: multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual, lo que resulte mayor en cuantía.

Sanción por una falta muy grave: multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual, lo que resulte mayor en cuantía.

INFORMACIÓN ADICIONAL

Si se dispone de tiempo se puede visualizar: Jornada INAP "Novedades en materia de Protección de Datos"

Adicionalmente, en la Agencia de Protección de datos se dispone de información adicional sobre la aplicación del Reglamento en España, que puede ser de utilizada para el opositor, además de encontrarse constantemente actualizada por la Agencia. http://www.aepd.es

LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES

ASPECTOS MÁS IMPORTANTES

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

Se regulan los datos referidos a las **personas fallecidas**, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido.

La Ley facilita que los ciudadanos puedan ejercitar sus derechos al exigir, en particular, que los medios para hacerlo sean fácilmente accesibles. Además, se regula el modo en que debe informarse a las personas acerca del tratamiento de sus datos optándose, específicamente en el ámbito de internet, por un **sistema de información por capas** que permita al ciudadano conocer de forma clara y sencilla los aspectos más importantes del tratamiento, pudiendo acceder a los restantes a través de un enlace directo.

Se reconoce específicamente 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 medida limita el ejercicio de estos derechos cuando el fallecido lo hubiera prohibido.

En cuanto a los menores, la Ley fija en **14 años para prestar consentimiento de manera autónoma**. Se regula expresamente el derecho a solicitar la supresión de los datos facilitados a redes sociales u otros servicios de la sociedad de la información por el propio menor o por terceros durante su minoría de edad.

La Ley refuerza las obligaciones del **sistema educativo** para garantizar la formación del alumnado en el uso seguro y adecuado de internet, incluyéndola de forma específica en los currículums académicos y exigiendo que el profesorado reciba una formación adecuada en esta materia. A tal efecto, el Gobierno deberá remitir en el plazo de un año desde la entrada en vigor de la Ley un proyecto de ley dirigido a garantizar estos derechos y las administraciones educativas tendrán el mismo plazo para la inclusión de dicha formación en los currículums.

El texto regula el **derecho al olvido en redes sociales y servicios de la sociedad de la información** equivalentes. Excepto cuando hubieran sido facilitados por terceros en el ejercicio de actividades personales o domésticas.

Se recoge los **sistemas de denuncias internas anónimas**, para poner en conocimiento de una entidad privada la comisión de actos que pudieran resultar contrarios a la normativa. Esto es imprescindible para que las personas jurídicas puedan acreditar la diligencia necesaria para quedar exentas de responsabilidad penal permitiendo conciliar su propio derecho con el derecho a la protección de datos de las personas.

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, complementando la regulación ante la utilización de sistemas de geolocalización en el ámbito laboral, de los que deberán ser informados.

Otra novedad es la referida a la **regulación de los sistemas de información crediticia** o ficheros de morosos, que reducen de 6 a 5 años el periodo máximo de inclusión de las deudas. Se exige una cuantía mínima de 50 euros para la incorporación de las deudas a dichos sistemas.

Se modifica la **Ley de competencia desleal**, regulando como prácticas agresivas las que tratan de suplantar la identidad de la Agencia o sus funciones y las relacionadas con el asesoramiento conocido como 'adaptación a coste cero' a fin de limitar asesoramientos de ínfima calidad a las empresas.

Cabe destacar la novedad de la Ley al proponerse "**garantizar los derechos digitales de la ciudadanía** conforme al mandato establecido en el artículo 18.4 de la Constitución" (art. 1.b), a través del Título décimo "Garantía de los derechos digitales", compuesto de 19 artículos (del 79 al 97).

Este título remarca que corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos digitales de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales.

Es importante destacar la modificación que realiza la LO 3/2018 de la Ley 39/2015.

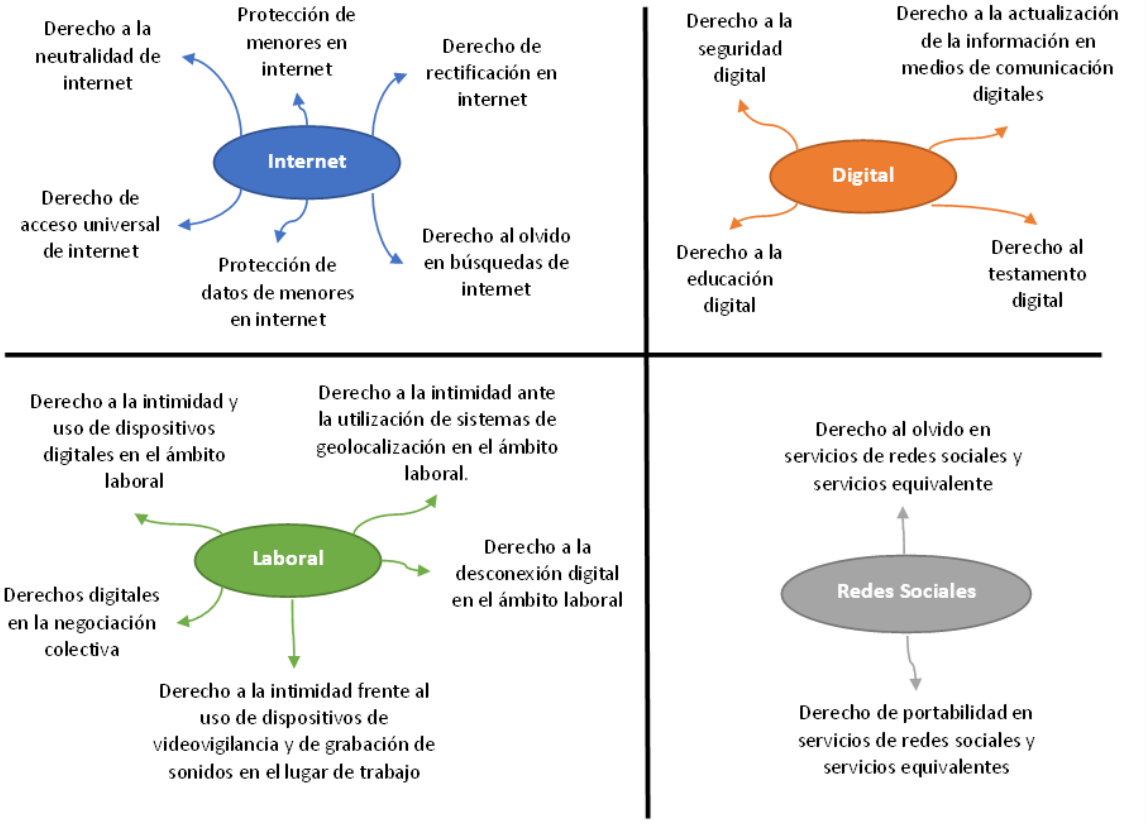
Se recomienda la lectura de los documentos pdf de la carpeta de Contenidos:

- Novedades LOPD Ciudadanos.pdf
- Novedades LOPD Sector privado.pdf
- Novedades LOPD Sector público.pdf

GARANTÍA DE DERECHOS DIGITALES

Incluidos en el Título X Garantía de Derechos Digitales:
- 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.

Para facilitar la memorización los organizamos en cuatro bloques:



Los derechos en la era digital (art. 79)

Establece que los derechos y libertades consagrados tanto en la Constitución, como en los Tratados y Convenios Internacionales en los que España sea parte, son plenamente aplicables en internet.

Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar la aplicación de tales derechos.

Derecho a la neutralidad de Internet (art. 80)

Se reconoce a los usuarios de internet el derecho a que los proveedores de servicios de Internet proporcionen una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Derecho de acceso universal a Internet (art. 81)

Se garantizará que el acceso a Internet sea universal, asequible, de calidad y no discriminatorio para toda la población, incluidas las personas con necesidades especiales, además de procurar la superación de las brechas de género y generacional y atenderá a la realidad específica de los entornos rurales.

Derecho a la seguridad digital (art. 82)

Se declara que los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet y los proveedores de servicios de Internet deberán informar de estos.

Derecho a la educación digital (art. 83)

El sistema educativo debe asegurar la plena inserción del alumnado en la sociedad digital y su aprendizaje de un uso seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales de los medios digitales.

Para ello, se formará al profesorado, incluido el universitario, en competencias digitales y para la enseñanza y transmisión de los valores y derechos.
Además, las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y de protección de datos.

Protección de los menores en Internet (art. 84)
Los padres y madres, tutores, curadores o representantes legales de los menores deberán procurar que los menores hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la Sociedad de la información, a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y derechos fundamentales.
El Ministerio Fiscal deberá instar las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, cuando la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes puedan implicar una intromisión ilegítima en sus derechos fundamentales.
Relacionados también los artículos 92 y 94.3.

Derecho de rectificación en Internet (art. 85)
Los responsables de redes sociales y servicios equivalentes adoptarán protocolos para posibilitar el ejercicio del derecho de rectificación con un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Este derecho está relacionado con el Derecho a la actualización de informaciones en medios de comunicación digitales (art. 86).

Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87)
Reconoce que tanto los trabajadores como los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.
Los empleadores deberán establecer e informar de los criterios de utilización de dichos dispositivos, incluyendo los usos autorizados y la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados, así como de las posibilidades de acceso por el empleador al contenido de esos dispositivos digitales.

Derecho a la desconexión digital en el ámbito laboral (art. 88)
A fin de garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar, y que deberá incluirse en una política interna.

Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89)
El tratamiento de las imágenes obtenidas solo podrá realizarse para el ejercicio de las funciones de control de los trabajadores o los empleados públicos. Los dispositivos de grabación nunca podrán estar instalados en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, como vestuarios, aseos o comedores, y siempre requerirá la previa información, expresa, clara y concisa, a los trabajadores y sus representantes.
Solo se admite la utilización de sistemas de grabación de sonidos en el lugar de trabajo en caso de riesgos relevantes para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y respetando los principios de proporcionalidad e intervención mínima.

Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90)
Autorizando el uso a los empleadores el tratamiento de los datos obtenidos a través de sistemas de geolocalización solo para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas en su marco legal y con los límites inherentes al mismo y previa información expresa, clara e inequívoca a los trabajadores o los empleados públicos y a sus representantes.

Derechos digitales en la negociación colectiva (art. 91)
Estos derechos se consideran la condición de mínima, pero los convenios colectivos podrán establecer garantías adicionales.

Protección de datos de los menores en Internet (art. 92)
Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad deberán contar con el consentimiento del menor o sus representantes legales en los casos en que la publicación o difusión de sus datos personales fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes.

Derecho al olvido en búsquedas de Internet (art. 93)
Toda persona tiene derecho a que se eliminen de las listas de resultados la información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, todo ello teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
Este derecho no se puede ejercer frente a un medio de comunicación o utilizando criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Derecho al olvido en servicios de redes sociales y servicios equivalentes (art. 94)
Mediante una simple solicitud, ya hubiesen sido facilitados en primera persona o por terceros cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, o cuando las circunstancias personales que invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.
En el caso de que los datos hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión.

Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (art. 95)
Los usuarios tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Derecho al testamento digital (art. 96)
Esta no es una nueva forma de testamento, sino una forma de incluir en el testamento tradicional indicaciones sobre los bienes de información gestionados por prestadores de servicios de la sociedad de la información, y a los que las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión, siempre que la persona fallecida no lo hubiese prohibido expresamente o así lo establezca una ley.

Políticas de impulso de los derechos digitales (art. 97)
El Gobierno en colaboración con las comunidades autónoma, deberá elaborar dos documentos:

- un “Plan de Acceso a Internet” orientado a superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos.
- Un "Plan de Actuación" dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

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, garantías y mandatos y de las medidas necesarias para promover su impulso y efectividad.

PRESCRIPCIÓN DE LAS SANCIONES

Artículo 78. Prescripción de las sanciones.

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

El artículo 47 de la Ley Orgánica 3/2018, regula las funciones y potestades de la Agencia, entre ellas, corresponde a esta **autoridad administrativa independiente** “supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679” ejerciendo las funciones que tiene establecidas en el mismo y en la ley orgánica.

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.

Sin embargo, según el artículo 2 de la Ley, quedan fuera de su ámbito de aplicación los artículos 79 a 88 y 95 a 97, es decir, no tiene competencias respecto a los “derechos en la Era digital”, los cuales se asignarán como competencia de otro organismo según el pendiente desarrollo normativo.

HERRAMIENTAS DE LA AEPD

La herramienta Facilita RGPD ha sido puesta a disposición por la AEPD para cualquier empresa o profesional para que, con tan solo tres pantallas de preguntas permite valorar su situación con respecto del tratamiento de datos personales que lleva a cabo. De esta forma puede determinar si se adapta para utilizar Facilita RGPD o si debe realizar un análisis de riesgos.

Esta herramienta es una ayuda, y por tanto, la documentación resultante deberá estar adaptada y actualizada a la situación de los tratamientos que se lleven a cabo en su entidad. La obtención de estos documentos no implica el cumplimiento automático del RGPD.

PROTECCIÓN DE DATOS Y EL PROCEDIMIENTO ADMINISTRATIVO COMÚN

La LO 3/2018 **modifica** en su Disposición final duodécima **el artículo 28 de la Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas indicando que no aportar documentos es un derecho del interesado, en lugar que no estarán obligados, 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. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.
>
> Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
>
> Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento 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 de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Por último, la Disposición adicional octava, establece la **Potestad de verificación de las Administraciones Públicas**. Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

EL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS

Nombramiento y Características

- 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 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 y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- Supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales,
- Supervisar la asignación de responsabilidades,
- Supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento,
- Supervisar las auditorías correspondientes;
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos,
- Supervisar su aplicación de conformidad con el artículo 35 del Reglamento;
- Cooperar con la autoridad de control;
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y
- Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos debe contar con una cualificación profesional, que puede ser otorgada por un conjunto de empresas acreditadas por la Entidad Nacional de Acreditación (ENAC) para otorgar estas certificaciones en función de los criterios establecidos por la Agencia Española de Protección de Datos

El nombramiento y cese del delegado en Protección de Datos debe ser comunicado a la AEPD.

En concreto, los aspectos en relación al **Delegado de Protección de Datos en las AAPP** pueden consultarse en el documento funciones-dpd-en-aapp.pdf de la carpeta Contenidos, entre ellas las más destacadas son:

- 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. Asimismo, el nivel del puesto de trabajo debe ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones.
- 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.