Aspectos legales de la Seguridad en los Sistemas de Información

Índice:

1. Introducción

Siglas

LO	Ley Orgánica
LOR	Ley ORgánica
TAD	Tratamiento Automatizado de Datos
PDP	Protección de Datos Personales: Ley LORTAD Ley LOPDP Ley **GDPR/RGPD (Vigente desde el 25 de mayo de 2018)**
APD	Agencia de Protección de Datos

Protección de datos personales

Derecho fundamental:

- necesidad de **consentimiento** para el tratamiento de los datos personales,
- a **conocer la existencia de ficheros** donde se recojan datos que nos afectan,
- de **acceso** a su contenido,
- de **rectificación** de los incorrectos y de **oposición y cancelación**.

Se basa en el artículo 18.4 de la Constitución Española. Derecho a la intimidad.

Normas sobre PDP (España)

Año 1992

LORTAD: Ley Orgánica 5/1992, de 20 de octubre, de Tratamiento automatizado de Datos de Carácter Personal.

Año 1999

LOPDP: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La LOPDP derogó y amplió la LORTAD para incluir la protección de cualquier tipo de tratamiento de datos personales en cualquier soporte físico, automatizado o no, y para adaptarse al Derecho Comunitario europeo. Se centra exclusivamente en los datos relativos a personas físicas.

La protección de los datos de las personas jurídicas no tiene la preferencia de la tutela de los derechos fundamentales ni de la Agencia de Protección de Datos (APD).

GDPR: El 25 de mayo de 2018 entra en vigor en toda Europa una nueva ley de protección de datos: GDPR (*General Data Protection Regulation*). Norma que afecta a todas aquellas empresas que traten datos de los ciudadanos europeos aunque sean de Estados Unidos, como Google o Facebook. Se trata de la primera norma sobre esta materia que afecta a todos los países de la Unión Europea y **unifica, por tanto, tanto los derechos como las obligaciones**.

Se espera que en unos meses se apruebe una nueva ley (actualmente en proceso de tramitación parlamentaria) que facilite la aplicación del Reglamento. Esta nueva ley no puede contradecir a GDPR, pero sí que definirá mejor algunos de sus aspectos (cuando un usuario es considerado menor, por ejemplo).

Determina que **todas las empresas**, independientemente de su país de origen o de actividad, deberán cumplirla si recogen, guardan, tratan, usan o gestionan algún tipo de dato de los ciudadanos de la Unión Europea. Es decir, que Apple o Amazon (por poner algunos ejemplos) también están sujetas a ella. Y, por supuesto, afecta a todas las personas que residen en la Unión Europea.

Recoge y reconoce, **derechos importantes y novedosos, como al olvido y el derecho a la portabilidad**.

Normas de protección de datos (Unión Europea)

Año 1995

Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, 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

Año 2012

Propuesta 2012/0011 de Reglamento del Parlamento Europeo y del Consejo 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.

LOPDP (Definiciones)

Artículo 3

- **Datos de carácter personal**: los referidos a una persona identificada o que permiten identificarla, cualquiera que sea su formato o forma de presentación o constancia (voz, imágenes fijas o móviles, huellas digitales, datos genéticos,…) .

- **Ficheros**: conjuntos de datos ordenados y estructurados conforme a ciertos criterios lógicos para facilitar el acceso a los datos personales .

- **Responsable del fichero / encargado del tratamiento**: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

- **Consentimiento**: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- **Fuentes accesibles al público**: ficheros cuya consulta puede ser realizada por cualquier persona. Su enumeración es taxativa: censo promocional, repertorios telefónicos, listados de profesionales colegiados, diarios y boletines oficiales y los medios de comunicación

LOPDP (Ámbito de aplicación)

Artículos 2 y 3

La LOPDP se aplica a los datos personales registrados en soporte físico que los haga susceptibles de tratamiento.

Se excluyen ciertos tipos de ficheros de datos personales: de ámbito doméstico, sobre materias clasificadas, sobre terrorismo y delincuencia, guías de servicios de telecomunicaciones.

Nota. Hay ficheros de datos personales con relevancia pública con regulación específica: materia electoral, estadística pública, registro civil, fuerzas y cuerpos de seguridad del estado y fuerzas armadas.

Ficheros de titularidad privada

La LOPDP establece (a empresas y profesionales) el deber formal de notificar la existencia de ficheros con datos personales a la Agencia de Protección de Datos (APD) para su inscripción en el Registro General de Protección de Datos. (https://www.agpd.es)

- El registro es público y gratuito.
- Es un instrumento para que los titulares de datos personales puedan localizar los ficheros que puedan contener datos sobre su persona (no los datos concretos).
- La notificación se puede realizar con el sistema NOTA de notificaciones telemáticas.

En la resolución de 12 de julio de 2006, de la APD, se aprobó el sistema de NOtificaciones Telemáticas a la AEPD (NOTA) a través de internet, en soporte informático o en papel para efectuar las solicitudes de inscripción en el Registro General de Protección de Datos (BOE 31 de julio de 2006).

Ficheros de titularidad privada (Agencia de Protección de Datos)

Los ficheros inscritos en el Registro General de Protección de Datos detallan la siguiente información:

- Nombre o razón social del responsable del fichero.
- Nombre del fichero.
- Finalidad y usos declarados.
- Dirección en la que el interesado puede ejercitar los derechos de oposición, acceso, rectificación y cancelación de la información contenida en el fichero.

Información más detallada:

- Datos del responsable del fichero.
- Derechos de oposición, acceso, rectificación y cancelación.
- Identificación y finalidad del fichero .
- Origen y procedencia de datos.
- Tipos de datos, estructura y organización del fichero.
- Cesión y comunicación de datos.
- Transferencias internacionale.

Ficheros de titularidad pública (Agencia de Protección de Datos)

Los responsables son:

- **Administración Central** (Administración General del Estado, entidades y Organismos de la Seguridad Social, Organismos Autónomos y Entes Públicos del Estado).
- **Administración, Entes y Organismos Públicos de las comunidades Autónomas.**
- **Administración Local, Entes y Organismos Públicos de Entidades Locales.**
- **Otras Personas Jurídico Públicas.**

Principios generales de la protección de datos

a.- Calidad de los datos (en la recogida y en el uso posterior).

b.- Seguridad de los datos: Reglamento de desarrollo de la LOPD.

c.- Consentimiento informado (inequívoco: tácito o escrito).

d.- Derechos básicos del titular: de acceso, rectificación, cancelación y oposición.

El procedimiento para el ejercicio de los derechos es por escrito acreditando el envío y la recepción, con posibilidad de reclamación ante la APD.

Reglamento de desarrollo de la LOPD

Año 2007

En el RD 1720/2007, de 21 de diciembre, se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE n. 17 de 19/1/2008).

Artículo 9

Obligación del responsable del fichero de adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal.

El reglamento se aplica a todos los ficheros automatizados y no automatizados (papel) con datos de carácter personal.

Reglamento de desarrollo de la LOPD (**RD 1720/2007, de 21 de diciembre**)

- Regula el procedimiento para garantizar que cualquier persona pueda tener un pleno conocimiento de la utilización que se vaya a hacer de los datos.
- Exige al responsable del fichero de datos que conceda al interesado un medio sencillo y gratuito que le permita ejercitar sus derechos de acceso, rectificación, cancelación y oposición.
- Hace especial énfasis en la necesidad de protección de los datos y en la **asignación de responsabilidades** de todas las personas con acceso a ellos.
- Se fijan criterios específicos sobre las medidas de seguridad, *organizativas y técnicas*, de los ficheros.
- Establece medidas de obligado cumplimiento para todos los ficheros que contengan datos de carácter personal, y un **régimen de infracciones y sanciones**.
- Regula los procedimientos tramitados por la Agencia Española de Protección de Datos.

Figuras personales creadas por la Ley Orgánica 15/1999 y el Reglamento RD 1720/2007

- **Afectado o interesado**: persona física titular de los datos que sean objeto del tratamiento.
- **Responsable del fichero o del tratamiento**: persona física o jurídica que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.
- **Responsable de seguridad**: persona a la que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- **Encargado del tratamiento**: persona física o jurídica que, sola o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero.
- **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos.

Niveles de Seguridad

Las medidas de seguridad exigibles se clasifican en tres niveles en atención a la naturaleza de la información:

- Nivel básico: todos los ficheros que contengan datos de carácter personal.
- Nivel medio: ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, servicios de información sobre solvencia patrimonial y crédito, datos tributarios, de entidades financieras, de Seguridad Social y aquellos que contengan un conjunto de datos de carácter personal que puedan definir la personalidad o evaluar el comportamiento de los ciudadanos.
- Nivel alto: ficheros que contengan datos (especialmente protegidos) de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas, datos derivados de actos de violencia de género o de los operadores que presten servicios de comunicaciones electrónicas.

Medidas de Seguridad

- Técnicas.
- Organizativas.

Art. 44.3 h y Art. 45.2 de la LOPDP

La falta de aplicación de las medidas de seguridad constituye una falta grave, sancionada con multa de entre 60000 y 300000 €.

Seguridad: Medidas Técnicas

- Control de acceso (lógico).
- Identificación y autenticación.
- Registro de incidencias.
- Gestión de soportes y documentos.
- Copias de respaldo y recuperación.
- Telecomunicaciones.
- Auditoría.

Seguridad: Medidas Organizativas

- Documento de seguridad.
- Funciones y obligaciones del personal.
- Responsable de seguridad.
- Registro de incidencias.
- Control de acceso (físico).
- Gestión y distribución de soportes.

- Auditoría

Medidas de seguridad de nivel básico (aplicables a ficheros y tratamientos automatizados)

1. Documento de seguridad.
2. Régimen de funciones y obligaciones del personal.
3. Registro de incidencias.
4. Identificación y autenticación de usuarios.
5. Control de acceso.
6. Gestión de soportes y documentos.
7. Copias de respaldo y recuperación.

Medidas de seguridad de nivel medio (aplicables a ficheros y tratamientos automatizados)

1. Medidas de seguridad de nivel básico.
2. Responsable de seguridad.
3. Auditoría bianual.
4. Medidas adicionales de identificación y autenticación.
5. Control de acceso físico.
6. Medidas adicionales de gestión de soportes y documentos.
7. Registro de incidencias.

Medidas de seguridad de nivel alto (aplicables a ficheros y tratamientos automatizados)

1. Medidas de seguridad de nivel básico y medio.

2. Seguridad en la gestión y distribución de soportes.
3. Copias de respaldo y de los procedimientos de recuperación en lugar diferente.
4. Registro de accesos.
5. Cifrado de telecomunicaciones.

Medidas de seguridad aplicables a ficheros y tratamientos NO automatizados

Medidas de seguridad de nivel básico:

1. Documento de seguridad.
2. Criterios de archivo.
3. Dispositivos de almacenamiento.
4. Custodia de soportes.

Medidas de seguridad de nivel medio:

1. Medidas de seguridad de nivel básico.
2. Responsable de seguridad.
3. Auditoría bianual.

Medidas de seguridad de nivel alto:

1. Medidas de seguridad de nivel básico y medio.
2. Almacenamiento de la información.
3. Copia o reproducción.
4. Acceso a la documentación.
5. Traslado de documentación.

Documento de seguridad (aspectos mínimos que debe contener)

a) Ámbito de aplicación y recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad .

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias .

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos .

g) Las medidas necesarias para el transporte, destrucción o reutilización de soportes y documentos.

h) Las medidas de seguridad adoptadas respecto de los ficheros o tratamientos no automatizados.

El documento deberá mantenerse actualizado y revisarse cuando se produzcan cambios relevantes en el sistema de información o en la organización.

Administración electrónica

Firma electrónica (España)

Año 1999

Real Decreto-Ley 14/1999 de 17 de septiembre sobre firma electrónica.

Año 2003

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Objetivo: dinamizar el mercado de la prestación de certificación.

Art. 1.1.

Su principal finalidad es la regulación de “la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación”.

Firma electrónica (Europa)

Año 1999

Directiva europea 1999/93/CE de 13 de diciembre de 1999 de armonización de la firma electrónica.

Firma electrónica (Concepto general)

La Ley 59/2003, establece, en su artículo 3, apartado 1:

“conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”

Tipos:

- Firma electrónica avanzada.
- Firma electrónica reconocida.

Firma electrónica avanzada

Ley 59/2003, establece, en su artículo 3, apartado 2

“la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control”.

Se pretende:

- garantizar la autenticación;
- evitar el rechazo en origen de los mensajes electrónicos;
- salvaguardar la integridad.

Firma electrónica reconocida

Ley 59/2003, establece, en su artículo 3, apartado 4 “la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”.

La firma electrónica reconocida tiene el mismo valor que la firma manuscrita.

Diferencias entre firma electrónica reconocida y avanzada

- La firma electrónica reconocida es una firma electrónica avanzada.
- El certificado en el que se basa (la reconocida) debe haber sido expedido por un prestador de servicios de certificación.
- El dispositivo de creación de firma debe ser seguro.

Firma electrónica

LEY 59/2003. Novedades Legislativas

Artículo 15. Documento Nacional de Identidad electrónico.

“el DNI que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.”

En el artículo 2 del RD 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, se establece el valor de dicho documento electrónico, igual que con el DNI tradicional, para acreditar la identidad y los datos personales de su titular que en él se consignen.

Artículos 3.5 y 3.6. Regulan el documento electrónico.

“el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.”

LEY 59/2003. Novedades Legislativas

- La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel (artículo 3.4).
- Se suprime el registro de prestadores de servicios de certificación.
- Amplía al sector privado la prestación de servicios de certificación.
- Establece el régimen aplicable a la actuación de personas jurídicas como firmantes (artículo 7).

Delitos informáticos

Los delitos informáticos son aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y Sistemas de Información, y ello sin perjuicio de que, además, puedan suponer una puesta en peligro o lesión de bienes jurídicos distintos. En España no existe tipo penal alguno que haga referencia expresamente al delito informático

Tipos de delitos informáticos

- El acceso no autorizado a Sistemas Informáticos.
- La estafa Informática.
- Delitos contra la intimidad.
- El espionaje industrial.
- El sabotaje informático.
- La denegación de servicio

Acceso no autorizado a Sistemas Informáticos

- Conforme a la legislación vigente en España, el mero acceso no autorizado a un sistema informático no es delito, pues no está tipificado como tal.
- En casi todos los países de nuestro entorno el acceso no autorizado constituye delito y está, por tanto, castigado.

Estafa Informática

El artículo 248.2 del Código Penal (Ley Orgánica 10/1995 modificada por la Ley Orgánica 5/2010), tipifica el delito de estafa informática:

"También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna **manipulación informática** o artificio semejante consigan una **transferencia no consentida de cualquier activo patrimonial** en perjuicio de otro."

Delitos contra la intimidad

Los artículos 197 a 201 del código Penal. Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

Espionaje industrial

Los artículos 278 a 286 del Código Penal, bajo la rúbrica “de los **delitos relativos al mercado y a los consumidores**” tipifican delitos que pueden ser delitos informáticos al poder realizarse a través de procedimientos informáticos.

Sabotaje informático

El delito de sabotaje informático o daños informáticos se encuentra tipificado en el artículo 264.2 del Código Penal.

Artículo 264

- 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, **programas informáticos o documentos electrónicos ajenos**, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.

- 2. El que por cualquier medio, sin estar autorizado y de manera grave **obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno**, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

Denegación de servicio

Un ataque de denegación de servicio (DoS) es, básicamente, un intento de impedir el uso legítimo de un servicio por parte de sus usuarios y puede llevarse a cabo bien agotando los recursos de un sistema, bien destruyendo o alterando la configuración o bien destruyendo o alterando físicamente los componentes de la red.

Recursos:

- el ancho de banda,
- el espacio en discos y memoria,
- tiempo para la CPU,
- acceso a otras redes

- acceso a otros elementos del entorno como suministro eléctrico, aire fresco o, incluso, agua

Determinación espacial de la ley aplicable (aspectos procesales de la delincuencia informática)

Artículo 23 de la Ley Orgánica del Poder Judicial.

Principio de la territorialidad

“ corresponde a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españolas.”

Teoría de la ubicuidad

“se entiende que un delito ha sido cometido en territorio español cuando la acción o parte de ella tenga lugar en territorio español e, igualmente, cuando, aún realizándose dicha acción en el extranjero, el resultado de la misma se produzca en España.