Análisis de la legislación sobre protección de datos personales

Resumen

La legislación sobre Protección de Datos marca una serie de límites a la utilización de los datos personales. Esto afecta a todas las empresas de nuestro país ya que, en mayor o menor medida, todas tratan o manejan datos de carácter personal de personas físicas (clientes, proveedores, empleados, colaboradores, accionistas...).

Todas las empresas deben adaptarse a la legislación teniendo en cuenta que deben conjugar, por un lado, los derechos que poseen los ciudadanos sobre el uso, tratamiento y destino de sus datos y, por otro, las medidas de tipo organizativas y técnicas que debemos establecer en nuestra organización para garantizar la seguridad de la información.

El cumplimiento de las obligaciones legales en materia de protección de datos es imprescindible; la LOPD establece unas sanciones económicas a los titulares de los ficheros y a los responsables del tratamiento de los datos, para los casos en que no se cumpla con la legislación sobre Protección de datos, siendo estas sanciones las más elevadas de nuestro entorno europeo.

La Agencia Española de Protección de datos (AEPD), organismo encargado de velar por el adecuado cumplimiento de la legislación vigente, cuenta con un amplio cuerpo de inspectores que tienen la consideración de autoridad pública en el desempeño de sus funciones. Actúan de oficio o mediante denuncia de cualquier afectado y, de no cumplirse con la legislación, imponen elevadas multas que pueden llegar hasta los 600.000 €.

- EL DESCONOCIMIENTO DE LA LEY NO EXIME DE SU CUMPLIMIENTO.
- EL TITULAR DE LOS DATOS NO ES QUIEN LOS POSEE EN UN FICHERO, SINO EL INDIVIDUO AL QUE SE REFIEREN LOS DATOS.
- LAS SANCIONES APLICADAS HASTA EL MOMENTO POR LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS OSCILAN DE MEDIA ENTRE LOS 60.000 € Y LOS 300.000 €.

Sumario

1. INTRODUCCIÓN A LA PROTECCIÓN DE DATOS

El artículo 18.4 de la Constitución dice que “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”.

Con la intención de hacer realidad este artículo nace la Ley Orgánica 5/1992, conocida como LORTAD, para posteriormente ser derogada por la vigente Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, conocida como LOPD.

No se puede poner en tela de juicio las enormes ventajas que nos reporta el uso de la informática en nuestra actividad empresarial, mejorando y aumentando tanto la productividad personal como la de las empresas. Sin embargo, quién no se ha preguntado alguna vez si aquellas empresas que tratan sus datos, con ordenadores cada vez más potentes y con bases de datos con mayor volumen de información, no tendrán demasiada información sobre su vida privada y qué uso harán de la misma.

Como ciudadanos nos preocupa relativamente el tratamiento de los datos de carácter personal cuando son de carácter básico (nombre, dirección, teléfono...), pero ¿y cuando se trata de datos más sensibles? (renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual...).

Toda esta información nos ofrece perfiles y hábitos precisos sobre las personas, perfiles que en algunos casos ni el propio titular de los datos conoce y que pueden ser utilizados de manera inadecuada. Sólo debemos valorar la información que se puede obtener de una persona conociendo sus movimientos bancarios, obteniendo información precisa sobre sus actividades de ocio y gustos, vida familiar, capacidad económica y un largo etcétera; o si analizamos la factura telefónica cruzando los datos que posee el operador de telefonía con las llamadas que realiza.

La intimidad es un valor que se reconoce de forma unánime en todo el mundo civilizado desde el siglo XX, los límites sobre la tenencia y utilización de los datos de carácter personal, así como el tráfico de los mismos quedan reflejados en la Legislación sobre Protección de datos, afectando a todas las organizaciones que constituyen el tejido empresarial de nuestro país, ya que todas manejan datos de este tipo (clientes, proveedores, empleados, asesores externos...).

Es por ello que todas las empresas deben adaptarse a la legislación teniendo en cuenta que deben conjugar, por un lado, los derechos que poseen los ciudadanos sobre el uso, tratamiento y destino de sus datos y, por otro lado, las medidas de tipo organizativo□técnico que debemos conferir a dichos datos en nuestra organización.

El planteamiento de este dossier es facilitar a nuestro colectivo la correcta comprensión de la Ley, así como las obligaciones que se establecen y deben adoptar.

2. NORMATIVA BÁSICA REGULADORA

- Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, también conocida como LOPD. A través de sus 49 artículos la presente ley tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

- El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. Tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados y no automatizados, centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

- Las Recomendaciones dictadas por el Director de la Agencia con objeto de adecuar el funcionamiento de ciertos sectores de actividad a la normativa española de protección de datos. Son elaboradas tras la realización de los Planes Sectoriales de Inspección de Oficio que anualmente desarrollan.

- Las instrucciones dictadas por la Agencia Española de Protección de Datos, cuya finalidad es aclarar y apoyar la interpretación de la ley con el fin de adecuar los tratamientos a sus principios.

3. A QUIÉN AFECTA ESTA NORMATIVA

Aplicable a todos los profesionales liberales, empresas y organizaciones públicas o privadas que almacenen, utilicen o traten datos de carácter personal registrados en soporte físico y que los haga susceptibles de tratamiento.

Considerándose "datos de carácter personal" a cualquier información concerniente a personas físicas identificadas o identificables. Todas las empresas manejan este tipo de datos en el desarrollo de su actividad; debemos tener en cuenta que una relación de clientes o proveedores de una base de datos o la relación de trabajadores de su empresa, son ficheros de carácter personal, afectados por las normativas anteriormente citadas.

Uno de los principios básicos en los que deben apoyar su comprensión de la legislación en materia de protección de datos, es que los datos que tratan en su empresa no son propiedad de la misma, sino de sus titulares, por lo que para la correcta aplicación de la normativa debemos tener en cuenta las tres fases en las que se estructura el tratamiento de los datos en la empresa:

a. El momento de la recogida de los datos.
b. El momento del tratamiento de los mismos.
c. El momento de la utilización y cesión o comunicación a terceros.

Las obligaciones de las empresas no se reducen a un momento puntual; es un proceso constante en el tiempo que afecta a su actividad empresarial.

4. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Su misión es la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. Es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Además de la Agencia Española de Protección de Datos (en adelante AEPD), en la actualidad algunas Comunidades Autónomas han creado Agencias Autonómicas de Protección de Datos, como son las de Madrid, Cataluña o el País Vasco, estando en fase de constitución otras, como la Gallega; estas agencias sólo tienen competencia sobre los ficheros públicos de sus respectivas comunidades.

La AEPD, además de otras funciones, atiende las peticiones y reclamaciones formuladas por las personas afectadas, ejerciendo la potestad inspectora y sancionadora. Cualquier ciudadano podrá conocer, solicitando en el Registro General de Protección de Datos, a través de la web de la AEPD (www.agpd.es), la existencia de los ficheros de carácter personal inscritos en España, sus finalidades y la identidad del Responsable del tratamiento; siendo la consulta pública y gratuita.

Dentro del reconocimiento de los derechos de los ciudadanos de acceso, rectificación, cancelación y oposición de sus datos personales, todos tenemos derecho a dirigirnos a cada una de las empresas u organismos públicos, de las que sabe o presume que tienen sus datos, solicitando información sobre qué datos tienen y cómo los han obtenido (derecho de acceso) y la rectificación o cancelación de los mismos.

Cualquier actuación contraria a las obligaciones contenidas en la LOPD puede ser objeto de denuncia ante la AEPD, estableciéndose las posibles infracciones en leves, graves y muy graves, con un abanico de sanciones que van desde los 600 a los 600.000€.

NIVEL	TIPOS DE DATOS	SANCIONES
LEVE	Todos los ficheros que contengan datos de carácter personal	De 601 a 60.101 €
GRAVE	Servicios Financieros, Hacienda Pública, Comisión de Infracciones Administrativas o Penales, Solvencia Patrimonial y Crédito…	De 60.101 a 300.506 €
MUY GRAVE	Salud, Vida Sexual, Ideología, Creencias, Afiliación Sindical, Origen Racial…	De 300.506 a 601.012 €

A modo de ejemplo, podemos señalar que no dar de alta un fichero en la AEPD es sancionado
con una multa mínima de 600 € que puede llegar, según los casos, hasta los 60.000 €.

Asimismo, no tener establecidas las medidas de seguridad que ordena el RDLOPD se sanciona con una multa mínima de 60.000 €, que puede llegar hasta los 300.000 €.

Es importante tener en cuenta que la cuantía de las sanciones económicas va a parar a la Administración y no al afectado, aunque éste luego tenga derecho a solicitar a la compañía una
indemnización si considera que han existido perjuicios.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de anti juridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. OBLIGACIONES DE LAS EMPRESAS

Las obligaciones más reseñables a cumplir por parte de la empresa (responsable del fichero) y cuya finalidad es impedir el mal uso o abuso de la información, se pueden resumir en dos apartados: Registro de Ficheros, Desarrollo y Aplicación de Medidas de Seguridad sobre los mismos:

5.1. Registro de Ficheros

Siempre que se proceda al tratamiento de datos personales, definidos en el artículo 3 de la Ley como "cualquier información concerniente a personas físicas identificadas o identificables", y que suponga la inclusión de dichos datos en un fichero, cualquiera que sea su forma, creación, almacenamiento o acceso, dicho fichero se encontrará sometido a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos.

5.1.1. Análisis de los datos tratados

La primera fase que debemos llevar a cabo consiste en analizar el tipo de datos que se manejan y si éstos se encuentran dentro de los llamados "datos de carácter personal", entendiendo que la mayor parte de las organizaciones de una forma u otra disponen de este tipo de datos dentro de sus sistemas informáticos (clientes, proveedores, empleados, colaboradores ...).

Una vez analizada la naturaleza de la información, se clasificarán los ficheros en tres niveles: Nivel Básico, Nivel Medio y Nivel Alto, aplicándose sobre estos ficheros una serie de medida de seguridad que garanticen su confidencialidad e integridad; no es lo mismo tratar datos identificativos como nombre y apellidos, DNI, dirección o profesión, que datos de carácter sensible como son cuestiones relacionadas con salud, solvencia u orientación sexual.

Datos de Nivel Básico

Identificativos
Circunstancias Sociales
Características Personales
Académicos y Profesionales
Empleo y puestos de trabajo
Información comercial

Datos de Nivel Medio

Servicios Financieros
Hacienda Pública
Seguridad Social
Solvencia Patrimonial y Crédito
Infracciones Penales y Administrativas
Personalidad y/o Comportamiento
Operadores Comunicaciones Electrónicas

Datos de Nivel Alto

Salud
Ideología
Vida Sexual
Religión
Creencias
Afiliación Sindical
Origen Racial
Violencia de Género

5.1.2 Inscripción de los ficheros

Una vez llevado a cabo el análisis de los datos tratados por la organización se procederá a la inscripción de los ficheros, de los que le empresa es titular, en el Registro General de Protección de Datos. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles, en caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. Se debe tener en cuenta que la AEPD no desea conocer los datos concretos que contienen los ficheros, sino la tipología de los datos que contienen.

La notificación de solicitud de inscripción debe contener necesariamente los siguientes datos: responsable del fichero, finalidad del fichero, ubicación, tipo de datos de carácter personal que contiene, medidas de seguridad, con indicación del nivel básico, medio o alto exigible y cesiones o transferencias de datos de carácter personal que se prevean realizar.

Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos.

Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

En la actualidad, la inscripción se realiza a través de los modelos normalizados proporcionados por la Agencia, siendo éstos soporte papel, magnético o telemático (Internet).

5.2. Aplicación de Medidas de Seguridad

El principio de seguridad y confidencialidad de los datos impone al Responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, y que a su vez se encuentran desarrolladas en el Reglamento de desarrollo de la LOPD (RD 1720/2007, de 21 de diciembre).

Este Reglamento de desarrollo de la LOPD resultará de aplicación sólo a los ficheros que contengan datos de carácter personal. Sus disposiciones definen las distintas medidas que habrán de adoptarse sobre los ficheros de datos de carácter personal, automatizados o no, resultando las mismas aplicables a la totalidad del sistema de información en que se aloja cada fichero, siendo de obligado cumplimiento.

Especialmente, debe recordarse que el Reglamento establece reglas específicas en materia de
control de accesos, gestión de soportes y elaboración de copias de respaldo, debiendo además constar todas estas medidas en el documento de seguridad, al que nos referiremos con más detalle en otro apartado.

5.2.1. Niveles de Seguridad y su aplicación

El RDLOPD establece niveles de seguridad atendiendo a la naturaleza de la información tratada y a la mayor o menor necesidad de garantizar su confidencialidad e integridad, siendo tres los niveles definidos:

Básico: Se aplicará a todos los ficheros que contengan datos de carácter personal.
Medio: Afecta a todos los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, solvencia patrimonial y crédito. Reunirán, además de las medidas de seguridad de nivel básico, las calificadas como de nivel medio.
Alto: Aplicable a ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de los afectados; reunirán, además de las medidas básicas y medias, las calificadas de nivel alto.

5.2.2. Tipos de Medidas: Organizativas y Técnicas

Resumen de Medidas por niveles:

Medidas Organizativas

Documento de Seguridad
Funciones y obligaciones del personal
Responsable de seguridad
Registro de incidencias
Controles de acceso físico
Gestión, distribución y custodia de soportes
Auditoría
Criterios y procedimiento de archivo
Almacenamiento de la información

Medidas Técnicas

Control de acceso Lógico
Identificación y autenticación
Copias de respaldo y recuperación
Registro de accesos
Telecomunicaciones

5.2.3. Documento de Seguridad

La organización elaborará, con carácter obligatorio, un documento de seguridad de obligado cumplimiento para el personal que tenga acceso a los datos y a los sistemas de información, conteniendo las medidas técnicas y organizativas que se desarrollarán, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos.

El documento deberá contener, como mínimo:

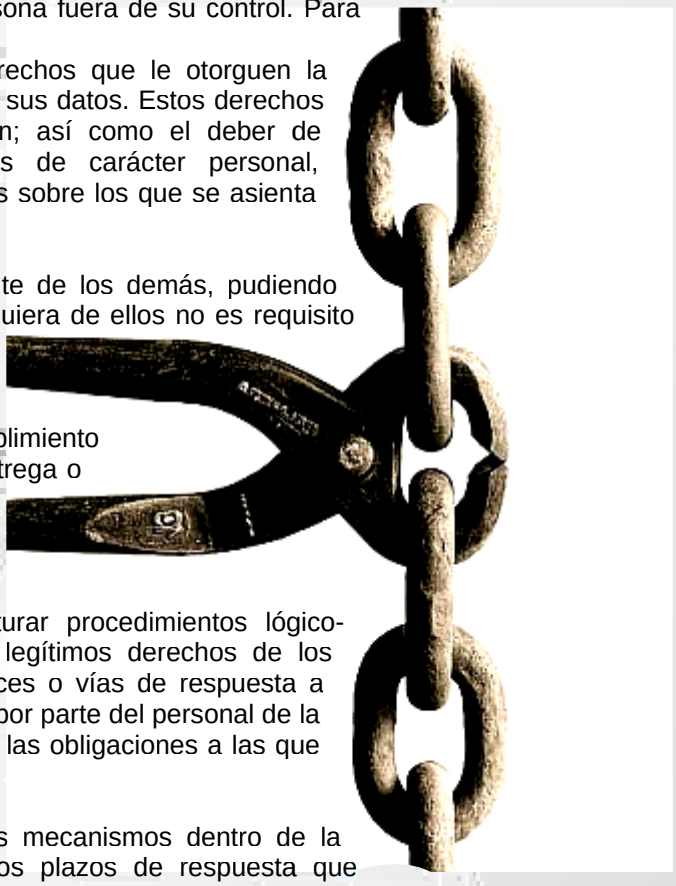
- Ámbito de aplicación, con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares que garanticen los niveles de seguridad.
- Funciones y obligaciones del personal.
- Estructura de los ficheros y descripción de los sistemas que los tratan.
- Procedimientos de notificación, gestión y respuesta ante incidencias.
- Procedimientos de realización de copias de respaldo y recuperación de datos.
- Medidas para el transporte de soportes y documentos, así como para su destrucción o reutilización.

El documento se deberá mantener en todo momento actualizado y revisado con los cambios que se produzcan, tanto en los sistemas de información como en la organización, siendo adaptado a la normativa vigente en cada momento.

MEDIDAS	BÁSICO	MEDIO	ALTO
Documento de Seguridad	*	*	*
Funciones y obligaciones del personal	*	*	*
Registro de Incidencias	*	*	*
Identificación y autenticación	*	*	*
Gestión de soportes	*	*	*
Control de acceso lógico	*	*	*
Copias de respaldo y recuperación	*	*	*
Política de gestión documental	*	*	*
Responsable de seguridad		*	*
Auditoría		*	*
Control de acceso físico		*	*
Distribución de soportes			*
Telecomunicaciones			*
Registro de accesos			*
Almacenamiento			*

5.3. Atención a los derechos del ciudadano

El tratamiento de los datos de carácter personal puede suponer una acumulación de información que posibilite definir un perfil de la persona fuera de su control. Para minimizar este riesgo, se conceden a los ciudadanos derechos que le otorguen la facultad de poder ejercer un control sobre el uso de sus datos. Estos derechos son: acceso, rectificación, cancelación y oposición; así como el deber de información previo al tratamiento de sus datos de carácter personal, considerándose todos ellos principios fundamentales sobre los que se asienta la ley.



Cada uno de los derechos es independiente de los demás, pudiendo ejercerse libre y gratuitamente; el ejercicio de cualquiera de ellos no es requisito previo para el ejercicio de otro.

Para ejercitar estos derechos es necesario, por parte del titular de los datos, el cumplimiento de unos requisitos formales básicos, como es la entrega o envío de una solicitud al responsable del fichero que contenga los nombre y apellidos, fotocopia del DNI y la petición en la que se concreta la solicitud.

El Responsable del Fichero debe estructurar procedimientos lógico-administrativos que posibiliten el ejercicio de los legítimos derechos de los ciudadanos, preocupándose de establecer los cauces o vías de respuesta a dichas solicitudes, así como el debido conocimiento por parte del personal de la empresa a través de formación o concienciación de las obligaciones a las que están sometidos.

Es sumamente importante establecer estos mecanismos dentro de la organización de una manera efectiva debido a los plazos de respuesta que establece la ley para estas solicitudes, ya que la ausencia o demora de respuesta en los plazos establecidos posibilita al titular de los datos a interponer denuncia por vulneración de sus derechos ante la Agencia Española de Protección de datos, estando ésta obligada a asegurarse de la procedencia o improcedencia de la denuncia, teniendo un plazo máximo de 6 meses para dictar la resolución de la tutela de los derechos y las consiguientes sanciones si se ha incurrido en infracción.

5.4. Deber de Secreto

El artículo 10 de la Ley Orgánica exige al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de los datos, tanto personal propio como externo (externalización de servicio, como por ejemplo confección de nóminas), a guardar secreto profesional sobre los datos, subsistiendo la obligación aún después de finalizar su relación con el responsable del fichero. Además, los datos de carácter personal objeto del tratamiento no podrán usarse para fines incompatibles con aquellos para los que fueron recogidos.

5.5. Funciones y obligaciones del personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas de acuerdo con lo establecido en la ley.

El Responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

Es clave dentro de la correcta adaptación a la LOPD, la concienciación y formación de los usuarios que tengan acceso a datos de carácter personal, haciéndolos conocedores de la importancia y seriedad de la normativa y formándolos sobre las funciones, obligaciones y normas que deben cumplir; sin la consecución de estos puntos la adaptación no será exitosa.

La adaptación puntual de la compañía a la LOPD y la Seguridad informática no es una vacuna que protegerá indefinidamente sus sistemas, por lo que se deben auditar y corregir de manera permanente las medidas, procedimientos y sistemas de información establecidos.

La falta de un proceso de concienciación y formación adecuados provocan, con mucha frecuencia, que nuestro propio personal de forma voluntaria o involuntaria sea la principal fuente de errores en materia de protección de datos y seguridad, de tal modo que una parte muy importante de las sanciones de la Agencia están provocadas por una mala praxis del personal de la organización.

6. CONCLUSIONES

- 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.

- El uso generalizado de la informática ha hecho que los Estados legislen para salvaguardar la intimidad de sus ciudadanos. España ha reaccionado imponiendo estrictos requisitos y fuertes sanciones, de las más elevadas de la Unión Europea; como consecuencia, las empresas deben optar por gestionar prudentemente los datos personales que obran en su poder.

- La aplicación de la LOPD en las organizaciones viene dada por un motivo fundamental que consiste en evitar las elevadísimas sanciones previstas en la LOPD (de hasta 600.000 €), pero no debemos olvidar que al cumplir la ley, no sólo mejoramos la seguridad y procedimientos de nuestra organización, sino también la imagen frente a nuestros clientes, proveedores y empleados, respetando la privacidad y el derecho a su intimidad.

- Conviene tener presente que los servicios de consultoría externos asisten, ayudan y complementan al empresario a una personalizada y rápida adaptación a la legislación en materia de Protección de Datos, pero nunca pueden sustituirle en la responsabilidad del cumplimiento de la normativa implementada en su organización.