ISSN: 1988-2629. No. 15. Nueva Época. Septiembre-Noviembre, 2013

Una aproximación para empresas a la Ley Orgánica de Protección de Datos

Marta Núñez López[1]
María del Mar Ferreiro[2]

Resumen

La protección de datos en España constituye un fenómeno relativamente reciente en el panorama jurídico español. A la primera regulación establecida en la LORTAD le siguió, por razones de adaptación a la normativa europea, la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su reglamento de desarrollo.
Esta ley, cuya regulación se centra de manera especial en el tratamiento de datos en ficheros automatizados, posee una dificultad técnica considerable, en la que conceptos, derechos, ámbito de aplicación, e incluso el régimen sancionador merecen un análisis simplificador. Este constituye el objeto del presente escrito, en el que, además, se tendrán en cuenta las medidas de seguridad establecidas por el RD 1720/2007, de 21 de diciembre, al objeto de alcanzar una visión más completa del actual sistema de protección de datos español.

Abstract

Data protection is a relatively recent phenomenom in the Spanish legal system. The first regulation through the LOTARD was followed, due to adaptation to European legal system, by the current Ley Orgánica 15/1999, September, the 13th, of Personal Type Data Protection and its regulation and development. This law, whose regulation is especially focused on the handling of automatized files, has a considerable technical difficulties. Its concepts, rights, sphere of application, and even the penalizing scope deserve a simplifying analysis.
This is the aim of this article, which will also take into account the security measures established by RD 1720/2007, December, 21th, so as to reach a more comprehensive insight into the current Spanish Data Protection System.

Palabras clave

Protección de datos, ficheros, consentimiento, derechos de los afectados, medidas de seguridad.

Key words

Data protection, files, consent, rights of the affected, security measures.

[1] Marta Núñez López es Licenciada en Derecho y Máster en Asesoría Jurídica por la UDC y posee el Diploma de Estudios Avanzados. Ha llevado a cabo labores de docente en la UDC y la UNED, y actualmente es asesora jurídica en Cartolab y profesora en Lexgal Formación. E-mail: martanunezlopez@gmail.com
[2] Mª. del Mar Ferreiro Broz es licenciada en Derecho por la Universidad de A Coruña. Actualmente realiza tesis doctoral en Departamento de Derecho del Trabajo por la misma Facultad. Es abogada y funcionaria de la Xunta de Galicia, ocupando la dirección de la Residencia de Maiores de Carballo. E-mail: xacobea20@gmail.com

Sumario

1.- Introducción

El objeto del presente escrito es el de recoger por escrito la conferencia impartida el día 7 de agosto de 2013 en A Coruña, en el marco de unas Jornadas Formativas dirigidas a empresarios y autónomos organizadas por la Asociación de Empresarios Autónomos GREMA.

Es por esta razón por lo que este trabajo no pretende, ni mucho menos, ser una exhaustiva pieza de investigación, sino más bien un escrito con contenido divulgativo, cuyo ánimo es acercar al público menos versado en esta materia una aproximación a tan intrincada cuestión, la de la protección de datos.

Así fue planteada esta cuestión en su momento, a Pilar Cousido, editora del proyecto Derecom, de quien recogimos con entusiasmo su invitación a participar en esta Revista, y a quien agradecemos su confianza y ayuda.

En este sentido ha de interpretarse el presente docuemtno, que bebe de fuentes mucho más técnicas y autorizadas que las que pueden suponer las páginas que a continuación siguen y que, en ningún caso, pretende ser algo más de lo que en realidad es: "Una aproximación (para empresas) a la Ley Orgánica de Protección de Datos"

2.- Evolución normativa de la protección de datos en España

Podemos decir que la protección de datos es el derecho que tienen todos los ciudadanos a que sus datos personales no sean utilizados sin la autorización, seguridad y protección debidos.

El desarrollo de las Tecnologías de la Información y la Comunicación ha generado enormes beneficios y oportunidades, pero supone también un peligro para la salvaguarda de derechos que nos pertenecen en nuestra calidad de ciudadanos, ya que la invasión de nuestra privacidad ha llegado a unos límites impensables años antes.

Centrándonos en nuestro ordenamiento jurídico, el art. 18.4 de nuestra Carta Magna ya recoge 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". En este sentido, el propio Tribunal Constitucional, en su STC 290/2000, define la protección de datos como un derecho fundamental[3].

Es el Convenio 108[4] del Consejo de Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, ratificado por España, en

[3] Fundamento Jurídico 6: "(….) el derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado" (…) "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal".

[4] BOUREAU VERITAS FORMACIÓN. *Ley de protección de datos personales. Manual práctico para la protección de los datos personales de las personas físicas*. Primera edición. Madrid: Fundación Confemetal, 2009. 295p. ISBN-13: 978-84-92735-02-0

1984, el pionero en su ámbito, si bien hasta 1992 no se aprueba la primera ley en desarrollo del citado precepto constitucional (Hemos celebrado, recientemente, los 20 años de la protección de datos en España[5]). Era la L.O. 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (vigente hasta el 14 de enero de 2000). Ésta era una normativa más bien restrictiva para el uso de la informática, obligando a inscribir todos los ficheros automatizados y a implementar ciertas medidas de seguridad para protegerlos.

Se tardó mucho en desarrollar el art. 18.4 de la Constitución, publicándose la LORTAD cuando ya estaba escrita la Propuesta de Directiva y se adelantó a la misma, porque había transcurrido mucho tiempo desde el año 1978, pero también porque existía cierta litigiosidad en el Tribunal Constitucional sobre lo que más tarde se configuraría como Derecho de Acceso. Además, ya estaba en vigor el Acuerdo Schengen, así como el Convenio de Aplicación del mismo. La entrada en vigor de la Directiva 95/46/CE hizo necesario modificar la LORTAD, ya que era preciso extender su ámbito al tratamiento de los datos personales, aplicándose a todo tipo de soportes y formas de tratamiento.

De estos presupuestos surge la L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), cuyo desarrollo reglamentario se realiza años después mediante el Real Decreto 1720/2007, de 21 de diciembre.

Se han criticado diversos aspectos de la Ley, tales como el hecho de que carezca de Exposición de Motivos, la falta de observancia de la Ley 30/1992, de Régimen Jurídico de la Administración Estado y Procedimiento Administrativo Común o de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a la Administración, aspectos en los que no entraremos ahora mismo.

Actualmente se está tramitando una propuesta de Reglamento de Protección de Datos de la UE, que pretende sustituir a la vigente Directiva 95/46. Alguno de sus principales cambios radica en la necesidad de contar con un responsable en las organizaciones o entidades de más de 250 empleados, lo que se conoce como el Data Protection Officer. Además, se eleva sustancialmente la cuantía de las sanciones, que podrían llegar para casos muy graves al millón de euros y/o al 2% de la facturación mundial del grupo.

3.- Ámbito de aplicación de la Ley Orgánica de Protección de Datos

Tal y como señala el propio artículo art. 2 de la LOPD, esta norma será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

> a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
> b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
> c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En relación con este último supuesto, el Reglamento añade que el responsable del tratamiento deberá designar un representante establecido en territorio español, entendiendo por

[5] Véase SALVADOR MONTERO, Luis. 20 años de Protección de Datos. Privacidad legal en España (consultado el 29 de enero de 2013). Disponible en web: <http://www.privacidadlogica.es>

establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Aunque esto parezca claro y meridiano, la aplicación práctica no resulta tan sencilla. *Así, tras un procedimiento sancionador iniciado por la Agencia Española de Protección de Datos, como consecuencia de una denuncia presentada por un particular contra GOOGLE INC. y GOOGLE SPAIN, S.L.*[6]*, Google alega que "hay que separar la actividad mercantil de Google Spain, S.L. y de Google, INC. Esta última es la que gestiona el buscador "Google", pero al tener su domicilio en California está fuera del ámbito de aplicación de la normativa española y que solo está sometido a la jurisdicción norteamericana y a la normativa de protección de datos de EEUU, y respecto a Google, Spain S.L., entiende que no puede considerarse como un establecimiento a los efectos de aplicar ni la Directiva Comunitaria ni la normativa española en materia de protección de datos, pues su actividad no está relacionada con el tratamiento de datos sino que se limita a representar a Google, INC en su negocio que ésta desarrolla de vender el espacio publicitario disponible en su página web."*

Por exclusión, el régimen de protección de los datos de carácter personal que se establece en la Ley Orgánica no será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, a aquellos sometidos a la normativa sobre protección de materias clasificadas ni a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

Asimismo, se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.
e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Por lo que se refiere al ámbito objetivo de aplicación, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en su art. 2, nos dice que será aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Como consecuencia, el Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Asimismo, tampoco será de aplicación en relación con los datos de empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.

[6] SEMPERE SAMANIEGO, Francisco Javier. Caso "Google" sobre el derecho al olvido:¿Cómo afecta a la propuesta de Reglamento de Protección de Datos?. Privacidad legal en España (consultado el 25 de junio de 2013) Disponible en web: <http://www.privacidadlogica.es>

Tampoco será de aplicación este Reglamento a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Por su parte, y ya en relación directa con la naturaleza de los ficheros y no con los datos que éstos contengan, el régimen de protección de los datos de carácter personal que se establece en el Real Decreto no será de aplicación a los ficheros y tratamientos realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (En este sentido, sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares), a los sometidos a la normativa sobre protección de materias clasificadas y a aquellos establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en este último caso el responsable del fichero ha de comunicar con carácter previo a la Agencia Española de Protección de datos la existencia del mismo, sus características generales y la finalidad o finalidades que persigue.

4.- Conceptos básicos

En el artículo tercero de la LOPD se señalan los conceptos básicos a tener en cuenta en el estudio de la protección de datos. En este orden de cosas, podemos señalar como tales los siguientes[7]:

Datos de carácter personal: considerándose como tales cualesquiera informaciones concernientes a personas físicas identificadas o identificables mediante los mismos, de tal modo que se incluyen aquéllos que, sin ser directamente reflejo de la identidad de una persona, sirven para determinarlo mediante cualquier procedimiento.

Fichero: se considera fichero todo conjunto organizado de datos de carácter personal, cualquiera que sea su forma y el sistema de organización, acceso o almacenamiento que emplee.

Tratamiento de datos: serán todas aquellas operaciones y procedimientos que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, de los que nos encargaremos más adelante. Serán también considerados tratamiento de datos las cesiones que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: es la persona, física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. Sobre él recae el deber de su inscripción así como la responsabilidad por las posibles infracciones.
Afectado o interesado: tendrá esta consideración la persona física titular de los datos que sean objeto del tratamiento. Como ya hemos comentado más arriba, las personas jurídicas no están protegidas por la Ley.

Encargado del tratamiento: será 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. En este sentido no ha de confundirse con este último, dado que el encargado del tratamiento es un mero operador.

Consentimiento del interesado: como todo consentimiento admisible a efectos jurídicos, el consentimiento a efectos de la LOPD viene determinado por la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de sus

[7] Art 5 del Reglamento de Desarrollo de la LOPD. España. Boletín Oficial del Estado, 19 de enero de 2008, núm 17, p 4136

datos. La manifestación de este consentimiento varía en función del tipo de datos que se traten. Esta cuestión será analizada en el punto siguiente.

Cesión o comunicación de datos: se tendrá por tal toda revelación de datos realizada a una persona distinta del interesado.

Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

5.- Principios de la protección de datos

Presentados los conceptos básicos, es procedente el análisis de aquellos principios generales que atañen a toda la normativa de protección, y que, como tales, han de informarla, sirviendo como parámetros interpretativos de la misma. Estos principios son los siguientes[8]:

a) Principio de calidad de los datos personales

Los datos de carácter personal sólo se podrán recoger para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido. En esta línea, la calidad se refiere tanto a la recogida de los datos como al tratamiento de los mismos.

Por lo que se refiere a la recogida, los datos han de ser adecuados, pertinentes y no excesivos. Ha de señalarse la finalidad para la que se recogen los datos, siendo ésta clara, inequívoca y legal.

Respecto al tratamiento de los datos, éstos no pueden usarse para fines incompatibles con los que provocaron su recogida. Han de estar actualizados y han de cancelarse cuando dejen de ser necesarios o pertinentes por haber cumplido ya el fin para el que fueron recabados, o cuando los datos sean inexactos o incompletos

b) Principio de información en la recogida de datos

Cuando se recaban datos de carácter personal, los interesados tienen el derecho de que se les informe de la existencia de un fichero o tratamiento, de los derechos de acceso, rectificación, cancelación y oposición, y de la identidad del responsable o representante en España. En caso de que no se pueda deducir claramente por las circunstancias o naturaleza de los datos, será preciso informar también de la finalidad y destinatarios de los datos y de las consecuencias, tanto de suministrarlos, como de negarse a ello.

No serán aplicables estos requisitos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional o a la persecución de infracciones penales o administrativas.

c) Principio de consentimiento del afectado

Este principio hace alusión a la facultad que tienen los interesados de disponer de los datos, de controlar las informaciones relativas a su persona y la circulación de esta información. Como ya

[8] Título II Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (España. Boletín Oficial del Estado, 14 de diciembre de 1999, núm 298, p 43088) y Título II y Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se regula el Reglamento de desarrollo de la LOPD.

hemos dicho anteriormente, el consentimiento es toda manifestación de voluntad libre, inequívoca, específica e informada del interesado, a través de la cual consiente el tratamiento de sus datos. En este sentido, el consentimiento puede ser revocado en cualquier momento siempre que haya una causa justificada, no teniendo esta revocación efectos retroactivos.

Sin embargo, hay varias excepciones al consentimiento del interesado. Así, no se requerirá consentimiento:

- Cuando los datos sean recogidos para el ejercicio de las funciones de las Administraciones Públicas en el ejercicio de sus competencias.
- Cuando los datos se refieran a las partes del contrato o precontrato de una relación laboral, negocial o administrativa y sean necesarios para su cumplimiento o mantenimiento.
- Cuando el tratamiento de datos busque proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público.

En referencia a este principio, es necesario aludir a determinados datos especialmente protegidos cuyas exigencias en cuanto al consentimiento son de mayor calado. Así, el art. 16 de la Constitución señala que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan de esta obligación los ficheros mantenidos por partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisa siempre del previo consentimiento del afectado. Este consentimiento, ha de ser obligatoriamente expreso y por escrito.

Por su parte, los datos de carácter personal que hagan referencia al origen racial, a la salud o a la vida sexual, sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado lo consienta expresamente.
En relación a lo dicho, la ley establece la prohibición de aquellos ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico y vida sexual.

d) Principio de seguridad de los datos

De acuerdo con este principio, el responsable del fichero y el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. A este respecto, el Reglamento de Protección de Datos establece las medidas de seguridad pertinentes para el desarrollo de esta labor, al objeto de que la misma sea diligente, completa y documentada.

e) Deber de secreto

El deber de secreto implica que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

f) Principio de comunicación de datos

La regla general es que únicamente podrán ser objeto de tratamiento o cesión de datos si el interesado hubiera prestado previamente su consentimiento para ello. Sin embargo, se interponen una serie de excepciones a la necesidad del consentimiento cuando:

- Lo autorice una Ley o una norma de Derecho Comunitario
- Hayan sido recogidos de fuentes accesibles al público
- Sean parte de un procedimiento de una relación jurídica, *por ej. en una compraventa de una vivienda, la cesión de los datos de los intervinientes por parte de la Notaría al Registrador de la Propiedad*
- Tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal, a los jueces o Tribunales, al Tribunal de Cuentas o a los organismos autonómicos de carácter análogo, siempre que actúen en el ejercicio de sus funciones.
- Se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, o se recojan en el ejercicio de las funciones propias de las AAPP, en el ámbito que le atribuya una norma con rango de ley o una norma de Derecho Comunitario.
- Siendo relativos a la salud, la cesión sea necesaria para satisfacer una urgencia o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre la materia.
- Y, por último, cuando el tratamiento o la cesión tenga por objeto la satisfacción de un interés legítimo del responsable del fichero, siempre que esté amparado por una norma con rango de ley o una norma de Derecho Comunitario.

g) Principio de acceso a los datos por cuenta de terceros

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. Estos servicios los llevan a cabo normalmente empresas que prestan servicios de tratamiento de datos. Se exige que exista un contrato que pueda acreditar de algún modo la vinculación del que presta el servicio al cumplimiento de la Ley. Si el tercero incumple el contrato, será considerado responsable del tratamiento y responderá personalmente de las infracciones en las que incurra.

Según el art. 20 del Reglamento, el acceso a los datos por parte del encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la ley y en el reglamento. Igualmente, el encargado del tratamiento no incurrirá en responsabilidad, cuando por indicación expresa del responsable, comunique los datos a un tercero designado por aquel, al que hubiera encomendado la prestación del servicio.

6.- Derechos de los afectados

A efectos de la presente ley, son derechos de los afectados los siguientes[9]:

a) Derecho de acceso (Art. 27 Reglamento)

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que se esté realizando así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas.

[9] Título III LOPD

El afectado podrá obtener información de datos concretos o de la totalidad de los datos sometidos a tratamiento, a través del responsable del fichero.

El responsable del fichero deberá facilitar el acceso así como resolver la solicitud del acceso en el plazo de un mes a contar desde la recepción de la solicitud. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información disponible sobre el origen de dichos datos y las comunicaciones realizadas de los mismos, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

La denegación del acceso podrá realizarla el responsable del fichero cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo.

Podrá también denegarse cuando lo prevea una norma de Derecho Comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

b) Derecho de rectificación y cancelación

El derecho de rectificación consiste en la posibilidad de que el interesado exija del responsable del tratamiento que se modifiquen los datos, cuando éstos sean erróneos o incompletos. El derecho de cancelación es el derecho que tiene el afectado de que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme al Reglamento.

La solicitud de rectificación deberá indicar el dato erróneo y la corrección que deba realizarse, aportando a tal efecto la documentación justificativa de la rectificación solicitada. Por su parte, la solicitud de cancelación indicará si el afectado revoca el consentimiento otorgado, en los casos en que la revocación proceda o si se trata de un dato inexacto o erróneo, acompañado igualmente de la documentación justificativa.

Estos derechos deben hacerse efectivos por parte del responsable del fichero dentro de los diez días siguientes a la recepción de la solicitud. Si el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente en el plazo de diez días desde su recepción por un medio fehaciente. Transcurrido este plazo sin contestación, se entenderá la solicitud desestimada.

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero notificará al cesionario la rectificación o cancelación para que éste la lleve a cabo en su fichero y en idéntico plazo.

c) Derecho de oposición

Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo. El art. 6.4 de la LOPD establece que en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Cuando se trata de datos recabados de fuentes accesibles al público con fines de publicidad o prospección comercial, no harán falta motivos fundados y legítimos relativos a una concreta situación personal, bastando con el deseo del interesado de no recibir publicidad. Habrá de concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento.

En cualquier caso, el plazo máximo para dar respuesta al afectado por parte del responsable del fichero es de diez días desde la recepción de la solicitud.

Este derecho es lo que se viene llamando "derecho al olvido", y, como sabemos, no tiene carácter absoluto y a veces, en la práctica es difícil de ejercitar.

d) Impugnación de valores

El art. 13 LOPD establece que los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecta de manera significativa, basada únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

El problema está en el tratamiento automatizado de datos. Hoy en día existen programas informáticos que obtienen perfiles de los ciudadanos, pudiendo éstos, en virtud de los mismos, verse perjudicados. Un ejemplo claro sería el de una persona que solicita un crédito hipotecario a una entidad bancaria en virtud de su edad, estado civil, capacidad económica, número de hijos, etc, y el programa informático le deniega dicho préstamo.

Por ello, el interesado debe tener derecho, por lo menos, a una audiencia por parte del responsable del fichero, en la que pueda alegar otra serie de factores que maticen su situación, y asimismo a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

e) Derecho de consulta al Registro General de Protección de Datos

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

El Registro General será de consulta pública y gratuita. En la práctica, esta consulta se puede llevar a cabo a través del sitio web de la AEPD. Evidentemente, en dicho Registro se señala qué tipo de datos personales son tratados, pero no cuáles son éstos.

f) Derecho a indemnización

Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

7.- Clasificación de los datos y medidas de seguridad

Analizadas las cuestiones anteriores, y en un orden más práctico, es necesario analizar las medidas de seguridad que la ley prevé para la protección de los datos de carácter personal objeto de su regulación; lo que pasa por analizar, en primer lugar, la clasificación que en el mismo texto se hace de éstos a efectos de aplicarlas.

En este sentido, la LOPD, en su artículo 80, establece tres niveles de seguridad para los datos personales: nivel básico, medio y alto, que variarán en función del tipo de datos que se gestionen, siendo el nivel básico el general, en el que están incluidos todos los datos para los que no estén previstos los mecanismos de protección de los niveles medio y alto.
En este orden de cosas, podemos citar como datos que requieren exclusivamente el nivel de protección básica tales como el nombre, el DNI, la dirección postal, el teléfono, correo electrónico, direcciones web, etc.

En el nivel medio, según el artículo 81 del Reglamento, estarían aquellos datos relacionados con la Hacienda Pública, los servicios financieros, las infracciones administrativas o penales, la prestación de servicios de información sobre solvencia patrimonial y crédito y los ficheros con datos suficientes para poder evaluar la personalidad del individuo. Este último inciso que, a primera vista, podría resultar bastante abstracto es, en la práctica, un tipo de datos muy común dentro del tráfico mercantil, dado que podríamos claramente encuadrar dentro de este tipo de archivos, tal y como señala la propia Agencia Española de Protección de datos, los currícula de los trabajadores o los de posibles candidatos a un puesto de trabajo.

En el nivel alto, según el apartado 3 del artículo 85 del Reglamento, están datos especialmente sensibles como los policiales y los relacionados con la ideología, la sexualidad, afiliación política, religión, etnia, etc… además de aquellos relacionados con la violencia de género y los recabados para fines policiales sin consentimiento de los interesados. Estos datos requieren la mayor de las garantías y, por tanto, la protección que de los mismos ha de hacerse es muy exigente. Este nivel de seguridad no es muy habitual en las empresas pequeñas, dado que este tipo de datos no son precisos para el funcionamiento habitual de las mismas, por lo que el principio de proporcionalidad haría de muy difícil comprensión que éstos fueran requeridos.

Como excepción, sin embargo, en el caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, el Reglamento hace una excepción cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros; o se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. En este último caso, las medidas a aplicar serán las correspondientes al nivel básico.

Analizada la clasificación tripartita de los datos, procede ahora el estudio de las exigencias que para cada nivel de protección establece el Reglamento. Dicha regulación aparece desarrollada en los capítulos II, III y IV del Real Decreto 1720/2007, en los que se tratan respectivamente el documento de seguridad, las medidas de seguridad aplicables a los ficheros automatizados y las medidas de seguridad aplicables a los ficheros no automatizados.

Es necesario hacer especial hincapié en el hecho de que las medidas previstas para cada nivel tienen carácter acumulativo, por lo que los niveles más altos llevan siempre implícito el establecimiento de las medidas de seguridad de los niveles anteriores. De este modo, y en función de la clasificación antes mencionada, las medidas de seguridad que han de ser aplicables en el caso de protección de nivel básico son las que a continuación se señalan.

a) Medidas de seguridad de nivel básico

En primer lugar, y como cuestión de vital importancia, es precisa la elaboración del denominado Documento de Seguridad, al que el Reglamento dedica un capítulo independiente, dado que, más que una medida de seguridad en sí, podríamos definirlo como la manifestación escrita de la estructura organizativa de la protección de datos.

El Documento de Seguridad es de carácter interno y ha de estar siempre en manos del responsable del fichero o ficheros, por lo que no es necesaria su remisión a la AEPD. Tal y como se dispone en el artículo 88.2, en caso de pluralidad de ficheros a cargo de un mismo responsable, se puede elaborar un único documento para todos o un documento para cada uno de ellos o para grupos de ficheros que tengan características comunes.

Además, es muy importante tener en cuenta que el Documento de Seguridad es dinámico, es decir, ha de ir modificándose a lo largo del tiempo en la medida en que se produzcan cambios en el sistema de protección[10].

El contenido mínimo del documento de seguridad, que no único[11], dado que en él se pueden hacer constar otras cuestiones que se consideren de interés para la protección de los datos objeto de tratamiento, aparece reflejado en el apartado 3 del artículo 88 del Reglamento. De lo citado en este artículo, y que no reproduciremos literalmente, podemos destacar la obligación de definir de modo claro y detallado los recursos protegidos y su estructura, así como las obligaciones del personal autorizado para el tratamiento de los datos. También habrán de estar especificados los procedimientos de gestión de incidencias así como los de realización de copias de seguridad y recuperación de datos. En el documento de seguridad también habrá de constar, en el caso de que el tratamiento de los datos sea por terceros, el contrato con base en el cual este tratamiento se realiza así como la adopción de las medidas necesarias por parte de ese tercero para la protección de los datos[12].

Además del Documento de Seguridad, la sección primera del capítulo III del Reglamento establece la obligatoria implantación de las siguientes medidas para el nivel básico.
En primer lugar, señala el Reglamento que es necesario el establecimiento de un régimen de funciones y obligaciones del personal, en el que estén claramente definidos quién puede acceder a los datos, a cuáles y cómo. Dicha organización habrá de constar, como ya hemos mencionado, en el Documento de Seguridad, en el que también estará especificado el procedimiento para las autorizaciones de acceso a los datos, que ha de llevar a cabo el responsable del fichero.

Como cuestión de índole práctica, y en referencia a lo dicho, consideramos que es muy importante que todos los trabajadores de la empresa u organización y, en especial, aquellos cuyas funciones tengan incidencia sobre los datos, posean un conocimiento del sistema de protección de datos implantado, así como de los mecanismos para ejercitar los derechos de acceso, rectificación y cancelación por parte de los usuarios y el sistema de gestión de incidencias, de tal modo que ante un eventual problema sepan qué hacer o a quién informar.

Relacionado con este último inciso, el artículo 9 hace referencia a la obligatoriedad, dentro del sistema de protección de nivel básico, de creación y mantenimiento de un Registro de Incidencias. En este registro habrán de hacerse constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. Este registro ha de ser exhaustivo y llevarse con extrema diligencia dado que supone la clara manifestación fáctica de que se está procediendo de modo correcto en la gestión de los recursos encaminados a la protección de datos.

Igualmente se señalan en el Reglamento, como medidas de nivel básico la obligatoriedad de un debido control de acceso por parte de los usuarios a los recursos, en la medida que sólo puedan acceder a aquéllos que el responsable del fichero les haya autorizado. Del mismo modo,

[10] Art. 88.7 del RD 1720/2007 de 21 de diciembre. BOE núm. 17 de 19 de Enero de 2008.
[11] La Agencia Española de Protección de Datos proporciona un modelo de documento de seguridad al objeto de que sea más sencillo proceder a su elaboración. Dicho documento puede descargarse en https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php .
[12] Art. 88.5 del RD 1720/2007 de 21 de diciembre.

el acceso a los ficheros ha de estar implementado de tal forma que la identificación de los usuarios que acceden sea totalmente inequívoca, mediante un sistema de autenticación que, por lo general, se articula por medio de contraseñas. En el caso de que sea éste el método elegido, habrá de reseñarse en el documento de seguridad el procedimiento para su generación y la periodicidad de modificación de las mismas que, en ningún caso puede ser superior a un año.

Por su parte, y ya en referencia a los soportes en sí, debe llevarse a cabo una correcta gestión de los mismos, en la que se garantice su correcta identificación y facilidad de inventariado, así como la debida autorización por parte del responsable del fichero en caso de que los datos deban salir del lugar en el que están almacenados y para lo cual habrán de adoptarse las medidas necesarias con el fin de que no se produzca una pérdida accidental o una sustracción intencionada de los mismos. Se establece finalmente la obligatoriedad de realizar copias de respaldo de los ficheros con una periodicidad semanal y el establecimiento de un sistema de recuperación de datos para el caso de pérdida. Este sistema habrá de ser verificado cada seis meses por parte del responsable del fichero, quien, preferiblemente, habrá de llevar a cabo la comprobación con datos ficticios.

Analizadas las medidas de seguridad obligatorias en cualquier tratamiento de datos, sean éstos de la naturaleza que sean, es preciso destacar, como ya hemos dicho más arriba, que el Reglamento establece medidas adicionales en el caso de que los datos a tratar y proteger tengan un carácter más sensible. En este sentido, en el caso de aquellos datos considerados de nivel de protección media, además de las medidas señaladas, habrán de tomarse dos medidas adicionales así como intensificar algunas de las básicas.

Como medidas adicionales establecidas por el Reglamento en el Título II del Capítulo III se destacan la obligación del nombramiento de uno o varios Responsables de Seguridad y la de la realización de una auditoría bianual.

Por lo que se refiere al Responsable de Seguridad, su nombramiento habrá de estar recogido en el Documento de Seguridad, considerándose tal nombramiento como un requisito de contenido mínimo del mismo cuando se establezcan medidas de protección de nivel medio y alto. Su función es la de coordinar la aplicación de las medidas oportunas establecidas en dicho documento y controlar la efectiva aplicación de las mismas de tal modo que se garantice su cumplimiento. Este nombramiento, independientemente de que constituya un cargo de responsabilidad con respecto a la protección de datos, no exonera en ningún caso[13] de responsabilidad al responsable del fichero que, en todo caso, conserva su obligación de velar por el correcto funcionamiento del sistema establecido.

Por lo que se refiere a la auditoría bianual, ésta podrá ser tanto interna[14] como externa, cuyo resultado habrá de ser un Informe que deberá ser analizado por el responsable de seguridad, quién habrá de comunicarle los resultados al responsable del fichero o ficheros, y, en todo caso, habrá de ponerse a disposición de la Agencia Española de Protección de Datos.

Por lo que se refiere a la exigencia de intensificación de las medidas de seguridad básicas el Reglamento señala, en primer lugar, en lo relativo al sistema de identificación y autenticación de usuarios, la obligatoriedad del establecimiento de un mecanismo que permita bloquear el acceso en caso de varios intentos fallidos y que proceda a grabar la hora y fecha del mismo, de modo tal que quede registrado para proceder a una ulterior comprobación de las circunstancias que dieron lugar a esta incidencia.

[13] Así viene señalado en el Art. 95 in fine del RD 1720/2007 de 21 de diciembre.

[14] En este sentido, y tal y como se señala en MARZO PORTERA, Ana. y MACHO-QUEVEDO PÉREZ-VICTORIA, Alejandro. La Auditoría de Seguridad en la Protección de Datos de Carácter Personal. Segunda edición. Barcelona: Ediciones Experiencia, 2009. 347 p. ISBN: 978-84-96283-78-7. Pp. 46 y 47l: la auditoría interna no puede llevarse a cabo por el responsable de seguridad y de preferencia ha de realizarse por un departamento independiente al encargado de la implementación del sistema de protección de datos.

En cuanto a las medidas de control de acceso a los ficheros, el sistema de protección media exige, además de lo ya citado, que se restrinja la facultad de acceso físico a los elementos en los que estén almacenados los datos (servidores, discos duros, ordenadores…), de tal modo que quede garantizada, además de la indemnidad del software y su contenido, la del hardware en el que éste está instalado a fin de que no se pueda manipular o destruir de forma accidental o intencionada.

Igualmente se establecen medidas adicionales en lo referente a la gestión de soportes y el registro de incidencias. Por lo que atañe a la primera, habrá de crearse un registro de entrada y otro de salida de ficheros, de tal modo que quede claramente perfilado quién, cuándo y cómo se han llevado a cabo. En lo referente al registro de incidencias, a los datos requeridos en el nivel básico, habrán de añadirse los referentes a los procedimientos de recuperación y la persona que los ha llevado a cabo, además de los datos restaurados señalando, en caso de que hubiera sido necesario, aquellos datos que se hubieran grabado manualmente.

En último lugar, dentro del capítulo III, en la última sección se hace referencia a aquellas medidas de seguridad que habrán de tenerse en cuenta en los casos en los que los datos de carácter personal que se recaben se correspondan con los señalados en el apartado tercero del art. 81 del Real Decreto, con las excepciones señaladas en el apartado 5º a las que ya hemos hecho referencia. Entre las medidas de seguridad de nivel alto, podemos destacar de modo muy somero las siguientes:

Se requieren mayores cautelas en lo referente al registro de accesos. Además del sistema de control de entradas fallidas, los datos enmarcados en el nivel de seguridad alto requieren que, en su tratamiento, se establezcan controles exhaustivos de acceso a los mismos, de tal modo que se ha de implementar un registro detallado de entrada en el que consten los datos a los que se accede, la persona que lo hace, así como la fecha y hora en la que se ha llevado a cabo tal operación.

Por lo que se refiere a la gestión de soportes, entre otras cosas, se exige para éstos una mayor diligencia en su denominación y estructura, de modo que resulte claramente identificable por los usuarios autorizados pero no por terceros. Asimismo se exige que la distribución de soportes se verifique cifrando los datos y preferentemente en dispositivos de la propia organización. Por su parte, en el caso de comunicaciones telemáticas de datos, se ha de proceder a una correcta encriptación de los mismos, de modo tal que se garantice el acceso únicamente a aquellos que estén autorizados.

Por último, las copias periódicas de respaldo habrán de ser almacenadas en un lugar distinto a aquel en que se hallaren los equipos de tratamiento y su conservación habrá de cumplir las mismas exigencias previstas para el tratamiento de los ficheros originales.

Por lo que se refiere a las medidas de seguridad aplicables en el caso del tratamiento no automatizado de los datos personales, la regulación de estas medidas está recogida en el Capítulo IV del Reglamento y, además de las medidas previstas en el capítulo anterior para el tratamiento de los datos insertados en ficheros automatizados, cabe reseñar las siguientes medidas específicas para los casos de datos que requieran medidas de seguridad de nivel básico y alto[15].

En lo referente al nivel básico, los ficheros han de estar debidamente archivados y guardados en lugares a los que el acceso esté debidamente restringido físicamente. Por su parte, habrá de garantizarse la custodia responsable de aquellos ficheros o datos que se encuentren fuera del archivo, por causa de su tratamiento o clasificación.

[15] Por lo que se refiere al nivel medio, las medidas de seguridad señaladas en la sección 2 del capítulo IV del Reglamento son las ya analizadas de nombramiento de un responsable de seguridad y la obligatoriedad de auditoría bianual, por lo que no será necesario reproducir sus características en este momento.

Por lo que se refiere al nivel alto, podemos destacar que, entre otras cuestiones, la normativa establece la necesidad de que los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados estén en zonas de acceso restringido. Asimismo, el acceso a los ficheros, en el caso de que existan varias personas autorizadas, habrá de estar debidamente registrado de tal modo que se pueda identificar la persona que accede a ellos en un momento dado.

8.- Infracciones y sanciones

Obvio resulta que tamaña profusión de cautelas y mecanismos de protección debe ir acompañada de mecanismos de corrección que garanticen el cumplimiento de las mismas. En este sentido, es obvio que, independientemente de las ventajas de índole organizativa que una correcta gestión de los datos lleva aparejada, es necesaria la previsión de las consecuencias del incumplimiento de la normativa.

De este modo, la propia Ley de Protección de Datos, en su título VII, establece un catálogo de infracciones y sanciones. De estas últimas, las sanciones, cabe destacar su importancia económica, en todo caso, coherente con el objeto de protección de la normativa de protección de datos, dado que la vulneración de los mismos puede significar un gran menoscabo para los derechos fundamentales de los afectados. De acuerdo con lo dicho, las sanciones actualmente varían entre los 900 y los 600.000 euros en función de la gravedad de la infracción.

La ley establece, como es habitual en la normativa de carácter administrativa, una clasificación tripartita de las infracciones, diferenciando aquellas que son leves, graves o muy graves.

Son infracciones leves, según el apartado segundo del Art. 44 de la LOPD:

a) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.
c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

A estas infracciones leves les corresponde una sanción, de acuerdo con el artículo 45 de la ley, de entre 900 y 40.000 euros.

Por su parte, señala el apartado número 3 del artículo 44 que son infracciones graves, a las que según el 45.2 les serán de aplicación multas de entre 40.001 y 300.000 euros:

a) Crear ficheros de titularidad pública o iniciar la recogida de datos para los mismos sin autorización.
b) Tratar datos sin el consentimiento de las personas afectadas, cuando sea necesario conforme a la ley.
c) Tratar datos o usarlos vulnerando los principios y garantías establecidas en el art. 4 de la LOPD, salvo que constituya infracción muy grave.
d) Vulnerar el deber de guardar secreto acerca del tratamiento de los datos.
e) Impedir u obstaculizar el ejercicio de los derechos ARCO.
f) Incumplir el deber de informar al afectado acerca del tratamiento de sus datos cuando no hayan sido recabados del propio interesado.
g) Incumplir los restantes deberes de notificación o requerimiento al afectado impuestos por la ley.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.
i) No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
j) La obstrucción al ejercicio de la función inspectora.
k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello, salvo que la misma sea constitutiva de infracción muy grave.

Por último, y tal y como señala el art. 44.4 de la Ley, y a las que son de aplicación sanciones entre 300.001 y 600.000 euros, son infracciones muy graves

a) La recogida de datos en forma engañosa o fraudulenta.
b) Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.
c) No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
d) La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

Por lo que se refiere a la determinación de las sanciones dentro de los tramos previstos, la propia LOPD establece un sistema de criterios de graduación[16] basado, entre otras cuestiones, en la perduración en el tiempo de la infracción, el volumen de los tratamientos objeto de infracción y del negocio del infractor, la intencionalidad en la comisión de la infracción y los beneficios obtenidos por esta causa, la reincidencia, la naturaleza del perjuicio e incluso el hecho de que estando implantadas las medidas de seguridad oportunas, la vulneración no haya sido imputable a falta de diligencia por parte del responsable. Esta enumeración no es, ni mucho menos, exhaustiva, dado que el propio artículo 45.4 en su apartado j) hace referencia a *cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora,* de lo que podemos deducir una amplia capacidad de juicio por parte del órgano sancionador.

En esta misma línea, el apartado 5º del mencionado artículo, establece una atenuación de la sanción, estableciéndola en el tramo correspondiente a las infracciones anteriores en gravedad para determinados casos, esta vez, sí, de modo taxativo, en los supuestos en que concurran varias de las circunstancias del apartado anterior; cuando el infractor haya solucionado el problema de modo diligente, cuando se pueda deducir que la infracción se ha cometido por causa de la conducta del o de los afectados o cuando se produzca el reconocimiento espontáneo de su culpabilidad por parte del sancionado. Igualmente, se prevé esta "atenuación en grado" para los casos de fusión por absorción, cuando la entidad absorbente no sea la culpable de la infracción preexistente.

Por último, es necesario señalar que es posible, en caso de que la infracción no sea muy grave, y no se trate de un caso de reincidencia, que el órgano sancionador no acuerde apertura de procedimiento y se limite a apercibir al responsable, señalándole un plazo para que acredite haber introducido las medidas correctoras oportunas, encaminadas a enmendar la situación de ilegalidad.

Como inciso final, nos parece importante hacer referencia a la posibilidad prevista en el artículo 49 de la LOPD, según el cual para los casos de infracciones muy graves, o graves, y ante

[16] Art. 45.4 de la Ley Orgánica 15/1999 de 13 de diciembre. España. Boletín Oficial del Estado, 14 de diciembre de 1999.

la necesidad de protección de los derechos fundamentales de los afectados, puede, además de imponerse la sanción, ordenar la cesación del tratamiento de los ficheros e incluso la inmovilización de los mismos al objeto de reponer en sus derechos a los afectados.

9.- Conclusiones

El actual sistema de protección de datos se configura de un modo muy completo y amplio, en gran medida, como consecuencia de su regulación europea. La incidencia de este sistema de protección en el ámbito de los derechos fundamentales requiere una regulación minuciosa y un tratamiento exquisito tanto por parte de los operadores sociales, como de las Administraciones Públicas, de modo que se garantice la salvaguarda de estos derechos de los afectados. En un mundo como el actual, donde a menudo los datos son moneda de cambio (no olvidemos que la mayoría de los servicios "gratuitos" no lo son tanto) es necesaria una regulación cada vez más tuitiva de las personas y los consumidores.

Es por eso que el grado de internacionalización del mundo ha de traducirse, en cierto modo, en una internacionalización de las normas de protección de datos, de modo tal que no existan lagunas normativas que permitan realizar actos lesivos de esta naturaleza de modo impune. El nuevo Reglamento Europeo supondrá un paso más en este camino que ahora se inicia, y cuya evolución es una incógnita, como lo es el alcance de las nuevas tecnologías en un futuro.

10.- Bibliografía

BOUREAU VERITAS FORMACIÓN. *Ley de protección de datos personales. Manual práctico para la protección de los datos personales de las personas físicas.* Primera edición. Madrid: Fundación Confemetal, 2009. 295p. ISBN-13: 978-84-92735-02-0

MARZO PORTERA, Ana. *Guía práctica para la protección de datos de carácter personal.* Primera edición. Barcelona: Ediciones Experiencia, 2009. 273 p. ISBN: 978-84-96283-76-3.

MARZO PORTERA, Ana. MACHO-QUEVEDO PÉREZ-VICTORIA, Alejandro. *La Auditoría de Seguridad en la Protección de Datos de Carácter Personal.* Segunda edición. Barcelona: Ediciones Experiencia, 2009. 347 p. ISBN: 978-84-96283-78-7.

MONTERO MARTÍN, Silvia. *Ley Orgánica de protección de datos*. Tercera edición. Málaga: Innovación y Cualificación, 2012. 248 p. ISBN: 978-8-15648-94-9

SALVADOR MONTERO, Luis. 20 años de Protección de Datos. *Privacidad legal en España*. 29 de enero de 2013. Disponible en web: <http://www.privacidadlogica.es>

SEMPERE SAMANIEGO, Francisco Javier. Caso "Google" sobre el derecho al olvido:¿Cómo afecta a la propuesta de Reglamento de Protección de Datos?. *Privacidad legal en España*. 25 de junio de 2013. Disponible en web: <http://www.privacidadlogica.es>

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. https://www.agpd.es/