Universitat de Barcelona

89

La ley 15/1999 de protección de datos de carácter personal

Estudio realizado por: Sonia Plaza López

Tesis del Master en Dirección de Entidades Aseguradoras y Financieras

Curso 2003/2004

Esta publicación ha sido posible gracias al patrocinio de
Guy Carpenter & Cia., S.A.

Presentación

El presente estudio sintetiza las normas sobre protección de datos vigentes hoy en el ámbito nacional y comunitario. Recopilando la información que necesitaba para desarrollar el tema he visto la cantidad de grupos de trabajo y debates que suscita el tema de la protección de datos, para ello la página web de la Unión europea me ha sido de un gran interés. Asimismo la Agencia Española de Protección de Datos tiene publicadas en su web, algunas de las consultas realizadas por los consumidores y usuarios así como recomendaciones a los mismos. Evidentemente se trata de una materia de actualidad que afecta a todos y que está presente en multitud de foros.

Resumen

Estructurado en diferentes capítulos el objetivo de este estudio es entrar a analizar la actual ley de Protección de Datos de Carácter Personal en su propio contexto. He querido exponer el porqué de esta ley, su razón de ser, sus antecedentes legales y la normativa que se ha originado a raíz de su aprobación. El desarrollo de la sociedad de la información está introduciendo grandes cambios en las estructuras tradicionales de comunicación y comercio lo que por un lado permite a los consumidores y usuarios disponer de nuevos servicios de comunicación electrónica pero por otro lado introduce nuevos riesgos para sus datos personales y su intimidad. Aquí vamos a ver cual es el contenido del derecho a la libre disponibilidad de nuestros datos y como nos permite la ley disponer y mantener bajo control la información sobre nuestra persona.

Resum

Estructurat en diferents capítols l´objectiu d´aquest estudi ès analitzar l´actual llei de Protecció de Dades de Caràcter Personal dintre del seu propi entorn. He volgut exposar el perquè d´aquesta llei, la raó de la seva existència, els seus antecedents legals y la normativa que s´ha originat arrel de la seva aprobació. El desenvolupament de la societat de la informació està introduint grans canvis a les estructures tradicionals de comunicació i comerç, la qual cosa d´una banda permet als consumidors i usuaris disposar de nous serveis de comunicació electrònica però de l´altre afegeix nous riscos per les seves dades personals i la seva intimitat. Aquí anem a veure quien ès el contingut del dret a la lliure disponibilitat de les nostres dades y de quina manera ens permet la llei disposar i mantenit sota control la informació relativa a la nostra persona.

Summary

Structured in different chapters the objective of this study is to analyse the current law about Data Protection of Personal nature in his own context. I wanted to show the why of this law, his raison d'être, his legal records and the regulations originated as a result of his approval. The development of the information society is introducing big changes in the traditional structures of communication and trade what allows the consumer and users on the one hand to have new services of electronic communication but on the other hand introduces new risks for his own data and privacy. You'll find below the content of the right of free availability of our data and how the law allows us to have and to keep under control the information on our person.

Índice

La Ley 15/1999 de Protección de Datos de Carácter Personal

1. Presentación del problema

La información contenida en los archivos informáticos de las empresas, organismos públicos, centros sanitarios etc., está dotada de un gran valor tanto si la ponemos en relación con la propia actividad de la empresa como respecto a los individuos. Ficheros con datos de personas han existido siempre pero es ahora, con el desarrollo de las nuevas tecnologías y de la informática cuando se hace posible recoger estos datos en ficheros automatizados y en consecuencia, proceder al tratamiento de los mismos.

Un uso indebido de las bases de datos personales puede causar perjuicios a los interesados por ello los Estados y la Unión Europea han desarrollado una amplia normativa que garantice un nivel de protección adecuado. El tratamiento automatizado de datos comporta una serie de riesgos de los que tanto el legislador nacional como comunitario son conscientes.

En nuestro país el derecho a la intimidad quedó consagrado en la Constitución Española de 1978 como una derecho fundamental e incluso hace mención nuestra constitución a la necesidad de proteger dicha intimidad frente al uso de la informática. Sin embargo, el desarrollo de las nuevas tecnologías ha puesto en peligro una nueva vertiente de esta intimidad, más allá de la que comprende el art. 14 de la CE. Ahora entramos en el terreno de las nuevas redes de comunicación y almacenamiento de información, el desarrollo de la sociedad en este sentido llevó a la aprobación en 1992 de la LO 5/1992 de Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), sustituida actualmente por la LO 15/1999 de Protección de Datos de Carácter Personal (LOPD).

En esta exposición vamos a tratar el derecho a la autodeterminación de los datos como derecho fundamental, vamos a ver la normativa vigente sobre el tema y de que manera las personas físicas y jurídicas son protegidas. Asimismo pararé, para entrar con más detalle, en algunos artículos concretos de la Ley que por su incidencia en el mundo asegurador he considerado de interés ya que este sector, como el mundo empresarial en general, debe hacer un gran esfuerzo para adaptar sus estructuras y procedimientos a los requerimientos legales.

El objetivo es conocer y saber de qué medios disponemos para protegernos frente al tratamiento de nuestros datos dotando al presente estudio de una utilidad documental y también práctica.

2. La protección de datos

2.1 El derecho a la protección de los datos personales como derecho fundamental

El continúo desarrollo de la sociedad de la información ha obligado a adoptar la legislación vigente a la nueva realidad que supone el uso de internet y demás medios de comunicación a distancia. El objetivo del legislador es dotar de seguridad jurídica a las relaciones que se muevan dentro de este entorno ya que en definitiva el desarrollo del comercio a distancia dependerá de la confianza del consumidor en el mismo. Y esta confianza pasa por la protección de la intimidad de las personas cuando hacen uso de estos medios y por el respeto del tratamiento de sus datos personales. La finalidad es siempre que tanto la publicidad como las transacciones contractuales realizadas a través de medios electrónicos respeten la legislación vigente en materia de protección de datos.

Esta preocupación por salvaguardar el derecho a la intimidad del individuo frente al tratamiento de su datos ha llevado a que el derecho a la protección de los datos se consagre como un derecho individual, diferente al derecho a la intimidad que recoge en el art. 18 de la Constitución Española

El art. 18 de la Constitución Española establece el derecho a la intimidad personal y familiar como un derecho fundamental y como tal debe ser protegido frente a cualquier tipo de injerencia o intromisión ilegítima.

Art.18.1 CE "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"

No se trata, sin embargo, de un derecho absolutamente ilimitado en el sentido de que los imperativos del interés público pueden hacer que por ley se autoricen determinadas entradas en el ámbito de la intimidad que no podrán ser reputadas ilegítimas. Tampoco tendrán el carácter de ilegítimas aquellas entradas en el ámbito de la intimidad consentidas por el propio individuo, ahora bien la LO 1/1982 de 5 mayo sobre Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, exige que ese consentimiento sea expreso y permite que sea revocado en cualquier momento.

Ahora bien, la Constitución española en su art. 18.1 se está refiriendo a la intimidad como aquella esfera en la que el individuo desarrolla las facetas más reservadas de su vida, sin embargo, el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos suponen una amenaza para la privacidad de las personas en otros terrenos en que el individuo desarrolla otras facetas de su personalidad.

Con la inclusión del art. 18.4 se pone de manifiesto la conciencia por parte del legislador del riesgo que en este sentido puede suponer el uso de la

informática y otorga un ámbito de protección específico y más idóneo que el que podían ofrecer los derechos fundamentales enumerados en el art 18.1

Art. 18.4 "la ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos, y el legítimo ejercicio de sus derechos"

Con este apartado se busca garantizar la protección del individuo dentro de un ámbito más específico que el que recoge el apartado 1.

No podemos obviar las múltiples posibilidades que ofrece el uso de la informática tanto para recoger como para comunicar datos personales, con los consecuentes riesgos que esto puede entrañar. De ahí que se entendiera que el art. 18.1 no era suficiente para proteger a los individuos frente a esta nueva realidad derivada del avance tecnológico y se buscara a través de este otro apartado, proteger el derecho a la intimidad de la amenaza que supone la acelerada evolución del sector de las telecomunicaciones.

Sin embargo, con el art 18.4, seguimos estando dentro del terreno del derecho a la intimidad entendida ésta como intimidad individual, es decir, como el derecho de un individuo a que no se conozcan ciertos datos sobre su persona mientras que con la protección de datos se va más allá y se busca garantizar al individuo un poder de disposición sobre todos sus datos personales con independencia de a que ámbito de la vida del individuo estén referidos los mismos.

Y evidentemente para que la persona pueda ejercer ese derecho y disponer sobre sus datos deberá estar informado sobre:

- Primero, cuál son estos datos.
- Segundo, dónde están, en manos de quién
- Tercero con que finalidad.

Nos encontramos, por tanto, ante un derecho conectado pero diferente al recogido en el art 18 de la CE y que como éste ha sido calificado por el Tribunal Constitucional de fundamental. El contenido de este derecho ha quedado perfectamente retratado en la sentencia 292/2000, 30 de noviembre, del Tribunal Constitucional:

"La función del derecho fundamental a la intimidad del art.18.1 es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros contra su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un 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 derecho del afectado".

Se trata de lo que en esta misma sentencia el Tribunal Constitucional ha denominado *derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal.*

"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 datos personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objetivo no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, si no los datos de carácter fundamental"

Así pues el contenido del derecho fundamental a la protección de datos alude a cualquier tipo de dato referente a la persona y consiste en la facultad de autorizar la recogida, acceso, almacenamiento y tratamiento de los mismos y por consiguiente a la facultad de poder oponerse a todo ello, para lo cual la persona habrá de saber en todo momento, quién posee sus datos, dónde y porqué.

Todas estas facultades componen los principios de la protección de datos y así los recoge la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter Personal.

3. Entorno normativo de la protección de datos

3.1 Actividad de la Unión Europea en materia de protección de datos

El art 8 de la Carta de Derechos fundamentales de la Unión Europea reconoce el derecho de toda persona a la protección de sus datos personales.

Con lo que se ha llamado el "paquete de telecomunicaciones", la Unión Europea ha creado el nuevo conjunto de disposiciones legislativas destinado a regular el sector de las comunicaciones electrónicas y a sustituir la normativa existente en el sector de las telecomunicaciones.

La directiva 2002/58 CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas forma parte de dicho paquete, el cual comprende cuatro directivas más, cinco en total.

- Marco general (Directiva 2002/21/CE relativa a un marco común de las redes y los servicios de comunicación electrónica).
- Directiva relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados a su interconexión (Directiva 2002/19/CE)
- Directiva relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización y licencias 2002/20/CE)
- Directiva relativa al servicio universal (2002/22/CE)
- Directiva relativa al tratamiento de los datos personales (Directiva de intimidad y comunicaciones electrónicas 2002/58/CE).

Con este conjunto de medidas las instancias europeas adoptan una legislación que está en consonancia con el progreso tecnológico y con las exigencias del mercado. Aquí vamos a ocuparnos más concretamente de la Directiva relativa al tratamiento de datos personales y sus antecedentes pero para poder entender la existencia de la misma era imprescindible hacer referencia al entorno legislativo y social en que se ubica.

Sin necesidad de entrar a analizar cada una de estas directivas si voy a resaltar la importancia de la 2002/21/CE (marco general) como piedra angular del paquete de medidas. El objetivo de la Comisión era crear una directiva marco en la que se establezcan los objetivos políticos generales y específicos que deben alcanzar los Estados Miembros y que garantice los derechos específicos de los consumidores.

Asimismo debe asegurar un grado apropiado de interoperabilidad para los servicios y los equipos de comunicaciones y establecer los derechos, responsabilidades, facultades y procedimientos de toma de decisión de las ANR (Autoridad nacional de reglamentación), un nuevo concepto que ha

adquirido un peso significativo en el mercado ya que su función es garantizar una aplicación coherente del marco regulador comunitario en una situación de independencia respecto a los organismos gubernativos de los diferentes estados miembros.

En España es la Comisión del Mercado de las Telecomunicaciones (CMT), creado por Real Decreto-Ley 6/1996, el organismo encargado de llevar a cabo la regulación de las telecomunicaciones.

Por último, en esta directiva se definen y establecen normas de funcionamiento para el nuevo Comité de comunicaciones y para el Grupo de alto nivel sobre las comunicaciones en la elaboración de sus proyectos.

Las definiciones sobre términos relativos a redes y servicios de comunicaciones electrónicas que se contienen en la misma serán de aplicación en la Directiva 2002/58 sobre tratamiento de datos.

Vamos ahora a centrarnos en la directiva 2002/58 CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas que es, como hemos dicho, unas de las cuatro directivas que acompañan a la directiva marco. Empezando por recordar que antes de llegar a esta Directiva existe un largo camino en cuanto al análisis del tratamiento de la protección de datos. El Comité de Ministros del Consejo de Europa ha elaborado varias recomendaciones sobre esta materia (en especial las recomendaciones 4/95, relativa a la protección de datos de carácter personal en el ámbito de los servicios de telecomunicación, y la 5/99 por la que se adoptan determinadas directrices para la protección de datos de carácter personal en las “autopistas de la información”). También el grupo de Trabajo de Protección de datos, creado por el art. 29 de la Directiva 95/46/CE, ha dedicado una gran parte de sus esfuerzos a la protección de datos en el ámbito de las telecomunicaciones y en internet. Por último existe un grupo específico de protección de datos en el ámbito de las telecomunicaciones (el llamado Grupo de Berlín), que también ha hecho varias aportaciones sobre este asunto.

Sin embargo, la adopción de una norma específica en materia de protección de datos con ocasión del uso de las comunicaciones electrónicas llega con la Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Hasta entonces había existido otra directiva, la 95/46/CE , relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos por la que se pretendía proteger el derecho a la intimidad de las personas de forma que sus datos personales pudieran circular libremente en la comunidad, pero esta directiva pretende garantizar la seguridad en la libre circulación de los datos sin preocuparse especialmente por los riesgos que las redes de comunicación electrónicas pueden generar para la intimidad de las personas. Es, como ya hemos dicho, en la Directiva 97/66/CE donde se han querido establecer mecanismos de seguridad en la protección de datos mediante la adopción de una norma específica.

En la actualidad la Directiva 97/66/CE ha sido reemplazada por la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Las razones de esta sucesión normativa vienen recogidas expresamente en la exposición de motivos de la nueva directiva cuyo apartado 4 establece:

"La Directiva 97/66/CE debe ser adaptada al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de comunicaciones electrónicas disponibles al público sea el mismo, con independencia de las tecnologías utilizadas. Procede pues, derogar dicha Directiva y sustituirla por la presente".

Es decir, se pretende con la nueva Directiva dar cumplimiento al principio de neutralidad tecnológica o lo que es lo mismo, que la protección de los derechos de los ciudadanos sea la misma con independencia del tipo de comunicación que motive el tratamiento.

Lo que hace la nueva Directiva es profundizar en cuestiones que no estaban recogidas en la Directiva 97/66/CE ya que la evolución de internet ha ido cambiando las estructuras del mercado y como dice en el apartado 6 de la exposición de motivos:

"Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad".

Introduciendo materias como sería el llamado "spam" es decir, el envío de correo electrónico no solicitado y la exigencia de consentimiento previo al mismo o la regulación del tratamiento de los datos y localización de terminales de telefonía móvil entre otras.

La Directiva 2002/58/CE mantiene aplicable la Directiva 95/46/CE para las cuestiones relativas a la protección de los derechos y libertades fundamentales que en ella no se cubran de forma específica así como para los servicios de comunicaciones electrónicas de carácter público.

En definitiva con las directivas integrantes del "Paquete de telecomunicaciones" se establecen los principios en que las autoridades nacionales deberán basar su análisis de los mercados a fin de garantizar una competencia efectiva y en este entorno la protección del tratamiento de los datos adquiere un papel relevante.

En el ámbito nacional los principios de la protección de datos han quedado recogidos en diferentes normas:

La Ley 34/2002 de 11 de Julio sobre servicios de la sociedad de la información y de comercio electrónico adapta a la legislación española la directiva 2000/31/CE, relativa a determinados aspectos de los servicios de la información. En el preámbulo de esta directiva se indica, en su consideración 14, que le son aplicables a los servicios de la sociedad de la información las directivas 95/46/CE y 97/66/CE (actualmente derogada por la 2002/58/CE) en lo referente a la protección de las personas frente al tratamiento de sus datos.

De modo que la aplicación y ejecución de la directiva 2000/31/CE, y en consecuencia de las normas nacionales que la integran a nuestro ordenamiento, debe respetar los principios relativos a la protección de datos personales.

Asimismo la directiva 2002/58/CE ha quedado parcialmente recogida en otras normas como la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones la cual incorpora al ordenamiento español las directivas comunitarias que integran el paquete de comunicaciones y concretamente en materia de protección de datos la traspone en la medida que afecta a las redes y servicios de comunicaciones electrónicas.

En definitiva, hablar de redes abiertas como internet, de comunicaciones comerciales, de confidencialidad en las comunicaciones, o de cualquier otro aspecto derivado de la sociedad de la información no es posible al margen del respeto a los principios de la protección de datos personales.

3.2. Las Normas estatales en materia de protección de datos

El origen de la protección de datos a nivel estatal se encuentra, como ya hemos comentado, en el art 18 de la CE, dicho artículo autoriza en su punto 4 a limitar el uso de la informática para garantizar el derecho al honor, la intimidad personal y familiar de los ciudadanos y el ejercicio de sus derechos.

El progresivo desarrollo de las técnicas de almacenamiento de datos supone una amenaza para la privacidad de las personas, entendiendo el concepto de privacidad como más amplio que el de intimidad ya que mientras la segunda se limita a las esferas más íntimas de la vida de la persona, la privacidad la constituyen un conjunto más amplio de facetas de su personalidad. Con la idea de instalar mecanismos de protección de las personas frente al tratamiento de su información nace la L.O.R.T.A.D, Ley Orgánica de 29.10.1992 de regulación del tratamiento automatizado de los datos de carácter personal. Esta Ley gira entorno a los denominados “ficheros de datos”, ya que es su existencia y utilización lo que justifica el objetivo de protección derivado de esta Ley. La L.O.R.T.A.D. introduce el concepto de tratamiento de datos, concibiendo los ficheros como algo dinámico, de modo que, si la información contenido en los mismos se cruzara sería posible crear el perfil de una persona.

Esta Ley se estructura en una parte general y una especial. La primera la constituyen los derechos y garantías de las personas y delimita el ámbito de aplicación estableciendo los principios de recogida, registro y uso de los datos. La parte especial define los tipos de ficheros, públicos y privados, estableciendo regímenes diferentes en razón de su titularidad. También se encarga esta Ley de regular la transmisión internacional de datos transponiendo la norma del art. 12 del Convenio 108 del Consejo de Europa.

Para asegurar la eficacia de la Norma se encomienda el control de su aplicación a un órgano independiente, configurando un órgano especializado denominado AGENCIA DE PROTECCIÓN DE DATOS a la cual atribuye el

estatuto de ente público. Asimismo se atribuye a la administración potestad sancionadora como consecuencia de su función de control del uso de los ficheros.

El 20.06.1994 se publica el RD 1332/1994 reglamento de desarrollo que permite la aplicación práctica de la L.O.R.T.A.D., pendiente de un aspecto muy importante como es la seguridad y el 11 de Junio de 1999 aparece el RD 994/1999 que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Ambos reglamentos continúan actualmente en vigor en cuanto no se opongan a lo regulado en la LOPD (LO 15/1999).

La directiva 95/46/CEE de la que ya hemos hablado referente al tratamiento de datos personales y a la libre circulación de estos y la publicación, dos años más tarde, de la directiva 97/66/CE, introducen a nivel comunitario nuevos aspectos en materia de protección de datos. Estas normas más la constante evolución de la sociedad de la información llevan en 1999 a sustituir la L.O.R.T.A.D por la actualmente vigente LO 15/1999 de 13 de diciembre de protección de Datos de Carácter Personal (L.O.P.D.) la cual en su disposición derogatoria única establece:

"Queda derogada la Ley Orgánica 5/1992 de 29 de Octubre, de Regulación del tratamiento automatizado de los datos de carácter personal".

La disposición final primera de la LOPD habilita al gobierno para aprobar o modificar las disposiciones reglamentarias necesarias para la aplicación y desarrollo de esta Ley:

"El gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley".

Como hemos anticipado, las normas reglamentarias de desarrollo de la LORTAD continúan en vigor en cuanto no se opongan a la nueva regulación, así lo establece la Disposición transitoria tercera de la 15/1999 de Protección de datos de carácter personal:

"Hasta tanto no se lleven a efecto las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo (RCL 1993,1393); 1332/1994, de 20 de Junio (RCL 1994, 1707), y 997/1999, de 11 de junio (RCL 1999, 1678), en cuanto no se opongan a la presente Ley".

4. La Ley 15/1999 de Protección de datos de carácter personal

4.1. La Ley 15/1999 de Protección de datos de carácter personal

La intención de este capítulo es entrar a conocer los principios de la protección de datos y los derechos de las personas reconocidos en la Ley 15/1999 no se trata por tanto de ir analizando la Ley artículo tras artículo, sin perjuicio de que más adelante se vayan tratando, por su alcance, algunos de ellos, sino de ver de que mecanismos se sirve para garantizar esa protección de la que ya tanto hemos hablado. Insistiendo en la idea de que esta Ley va más allá de la mera protección del derecho a la intimidad personal y familiar para consagrar el derecho a la libertad informática, protegiendo a las personas físicas frente al tratamiento automatizado de sus datos de carácter personal. Y este objetivo la Ley lo recoge ya en su art. 1 cuando dice:

"La presente Ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"

- Ámbito objetivo;

La LOPD regula el tratamiento de datos de carácter personal, materializado en un fichero. No son datos de carácter personal, a los efectos de la LOPD, los datos que no se pueden asociar a una persona física concreta, es decir, como dice la propia Ley son datos de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables".

Pero además, para ser objeto de esta Ley los datos deben estar en soporte físico y ser susceptibles de tratamiento. Dado que vamos a hablar de estos conceptos a lo largo de todo este capitulo es conveniente ver como quedan definidos por la Ley:

Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y identificable.

Respecto a la definición de fichero hay que destacar que la Agencia Española de Protección de Datos ha manifestado que el concepto que da la Ley de fichero no va unido a la necesidad de que este se encuentre en una misma ubicación, es decir, es posible la existencia de un fichero distribuido en diferentes lugares geográficos siempre que, eso sí, la organización y sistematización de los datos responda a un conjunto organizado e uniformado de datos, sometidos a algún tipo de gestión centralizada. La definición de fichero recogida en la directiva 95/46/CE apoya esta idea cuando dice que, un conjunto de datos tendrá esa consideración: "ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

Por tanto debemos ver, no únicamente en qué servidor está alojado el fichero que contiene los datos, si no de qué modo se lleva a cabo la gestión de los mismos. Esto es importante si pensamos en entidades de un mismo grupo con domicilio social en diferentes países.

Los ficheros que contengan datos de carácter personal deberán ser obligatoriamente inscritos en el RGPD (Registro general de protección de datos). Dicha notificación corresponde a la persona física o jurídica que lo creó.

- Ámbito subjetivo;

Son dos los sujetos que intervienen en todo tratamiento de datos de carácter personal, el responsable del fichero o tratamiento y el afectado o interesado. En cualquier caso, la Ley limita su ámbito de protección a las personas físicas. En consecuencia, las personas jurídicas quedan excluidas de sus garantías.

La agencia de protección de datos se pronunció sobre esta cuestión en su Resolución de 27 de febrero de 2001, indicando en su Fundamento Jurídico II que:

"... la protección conferida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal no es aplicable a las personas jurídicas que no gozarán de ninguna de las garantías establecidas en la Ley, y por extensión lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y con los empresarios individuales que ejercen una actividad comercial y respecto de las cuales sea posible diferenciar su actividad mercantil de su propia actividad privada..... A contrario sensu, tanto los profesionales como los comerciantes individuales quedarían bajo el ámbito de aplicación de la Ley Orgánica 15/1999 y, por tanto, amparados por ella cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando, en consecuencia, la condición de comerciante, y los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada...."

Además ha de tenerse en cuenta que con frecuencia los ficheros que contienen información relativa a empresas incluyen nombres y apellidos de una persona física vinculada con la persona jurídica. En este caso, y con el objetivo de evitar riesgos innecesarios, se ha convenido que todos los registros de entidades jurídicas que contengan el nombre y apellidos de una persona física se entiendan protegidos por la Ley y sean notificados a la Agencia de Protección de Datos mediante la inscripción del correspondiente fichero.

En definitiva la LOPD no es de aplicación a los datos de las personas jurídicas pero sí a los de los empresarios individuales personas físicas (por ejemplo autónomos) y profesionales, así como a los ficheros de empresas que tengan una relación de personas físicas de contacto, como Administradores, Gerentes, Comerciales, etc.

4.2. Principios de la protección de datos

La LOPD concreta a través de estos principios los límites en el tratamiento de los datos de carácter personal. Vamos a seguir en la exposición el orden en el que los recoge la Ley.

1. CALIDAD DE LOS DATOS

Lo que podemos definir como la necesidad de que los datos tratados sean pertinentes con respecto a las finalidades para las que se hayan obtenido.

Los datos de carácter personal solo podrán ser recogidos para su tratamiento, así como someterse a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

A modo de ejemplo podríamos decir que no se cumpliría este principio en el supuesto que una persona se dirija a las oficinas de una entidad aseguradora para contratar una póliza de hogar y para ello se tengan en cuenta datos referentes a su religión o ideología.

Este principio impone una relación de equilibrio o de proporcionalidad entre los datos tratados y las finalidades para las que hayan sido obtenidos. No es posible que el tratamiento comprenda datos que excedan de los necesarios para obtener dichas finalidades.

Como consecuencia lógica de esto, los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, siendo esta cancelación una obligación para el responsable del fichero quien deberá actuar de oficio. En este sentido se pronuncia la sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 9 de marzo de 2001, cuando dice:

"Por lo tanto, si los datos han dejado de ser necesarios para los fines para los cuales fueron recabados o registrados o resulten inexactos, se debe proceder (…) a su cancelación, sin necesidad de solicitud del afectado. Y así se infiere del propio tenor literal de los art. 4.4 y 4.5 de la LO 5/1992, que utiliza la expresión imperativa "serán cancelados" y sin condicionarla a la existencia de una previa solicitud del afectado. En suma, la norma establece la obligación del responsable del fichero de proceder de oficio y con la debida diligencia a cancelar los datos inexactos o que han dejado de ser necesarios para la finalidad del fichero y sin necesidad de solicitud previa del afectado"

Asimismo la calidad de los datos exige la veracidad de los mismos de manera que los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado, por lo que el responsable del fichero está obligado a actualizar los datos que figuran en sus ficheros y almacenarlos de forma que se permita siempre el ejercicio del derecho de acceso (del que hablaremos más adelante) del afectado.

Todos aquellos datos que no puedan ser rectificados o completados, conforme a las prescripciones de la ley deberán ser bloqueados y posteriormente cancelados.

2. DERECHO A INFORMACIÒN EN LA RECOGIDA DE DATOS;

Otro de los principios fundamentales sobre los que se asienta la Ley 15/1999 es el deber de información al afectado, previo al tratamiento de sus datos de carácter personal. Su contenido se encuentra regulado en el art. 5.1 de la Ley:

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a)De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

De modo que cuando los datos personales de una persona vayan a ser recogidos ésta deberá ser informada previamente de todo el contenido del art. 5.1. La ley también establece excepciones a este derecho así cuando del contenido o circunstancias de la recogida de los datos ya se deduzca la información a que se refieren las letras b), c) y d) del art 5.1 no será necesaria suministrarla.

Cuando la recogida de los datos se realice sin el consentimiento del asegurado se le deberá informar en los tres meses siguientes al tratamiento del contenido de los puntos del art. 5.1. Quedan exceptuados de esta información los supuestos en que una ley lo establezca, o cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado, a criterio de la Agencia Española de Protección de Datos o de un organismo autonómico equivalente resulte imposible o exija esfuerzos desproporcionados.

Esta competencia que la LOPD otorga a la Agencia Española de Protección de Datos para que, bajo su criterio, se pronuncie sobre la procedencia de aplicar la excepción del deber de información a los interesados, habrá que someterla a lo establecido en el art.5.5 donde se establece que la exención al deber de informar deberá considerar:

- El número de interesados
- La antigüedad de los datos
- Las posibles medidas compensatorias

La Agencia ha manifestado que dicha exención sólo será posible a través de un acto administrativo suyo en el que se decida sobre la procedencia o improcedencia de la excepción alegada atendiendo a cada caso concreto. Dicho acto implicará la tramitación de un procedimiento administrativo de acuerdo con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Se tratará en todo caso de un procedimiento iniciado por el propio interesado, no de oficio y deberá ser él quien acredite la desproporcionalidad del esfuerzo que conllevaría la práctica de la notificación.

La decisión de la Agencia se limitará a determinar si dadas las circunstancias del caso la notificación implicaría un esfuerzo desproporcionado pero sin que deba ser ella quien se pronuncia sobre las medidas compensatorias que hayan de adoptarse.

Por último indicar que la Resolución deberá ser dictada por el director de la Agencia porque, aunque el art 5.4 no diga nada sobre esta necesidad, así se desprende de la función de Dirección y Representación de la Agencia que le atribuye el art 36.1 de la LOPD, siendo dicha resolución susceptible de recurso contencioso administrativo ante la Audiencia Nacional.

Tampoco será necesario informar, en el sentido del art. 5.1, cuando los datos provengan de fuentes accesibles al publico y se destinen a una actividad de publicidad o prospección comercial en cuyo caso en cada comunicación se informará al afectado del origen de sus datos, del responsable del fichero donde se encuentran y de los derechos que le asisten.

Por fuentes accesibles al público se entienden "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". Unicamente tienen la calificación de fuentes accesibles al público el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos profesionales que contengan los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, los diarios y boletines oficiales y los medios de comunicación.

El incumplimiento del deber de información se encuentra tipificado como falta leve en el art. 44.2.d) de la LO 15/1999:

"proceder a la recogida de los datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley"

3. CONSENTIMIENTO DEL AFECTADO;

El art 6 de la LOPD trata el alcance de la obligación de requerir el consentimiento del afectado, y se impone con carácter general para todos los procesos de recogida de datos personales. Exige que éste se obtenga de forma inequívoca, salvo que la Ley disponga otra cosa. El consentimiento deberá ser emitido de forma libre e inequívoca (por acción u omisión del afectado) pero siempre de manera específica e informada (artículo 3 de la LOPD). Además se ha de tener en cuenta que este consentimiento podrá ser revocado en cualquier momento posterior.

No obstante, sin perjuicio de las normas más rigurosas para los datos especialmente protegidos, existen algunas excepciones al principio general, dado que, siempre que no se vulneren los derechos y libertades fundamentales del interesado, no será preciso el consentimiento en los siguientes supuestos:

- Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.
- Cuando se refieran a las partes en una relación negocial (un contrato de arrendamiento por ejemplo) laboral (un contrato de trabajo) o administrativa, siempre que sea necesario para el cumplimiento de la relación de que se trate (por ejemplo pago de salarios).

- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido.

En los casos en que no es necesario el consentimiento del afectado, se reconoce a éste el derecho a quedar excluido del tratamiento de los datos (derecho de oposición) si con ello no contradice ninguna ley y si partiendo de la situación personal del interesado existe un interés legítimo. Si se da esta situación el responsable del fichero excluirá los datos del afectado del tratamiento:

Art. 6.4: "… 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 …".

El tratamiento de los datos sin haber obtenido consentimiento previo del afectado será causa de infracción grave según la redacción del art. 44.3 c) de la LOPD, a salvo siempre de las excepciones previstas por la Ley.

Para lo que sí será necesario un consentimiento emitido expresamente, además de ser libre, inequívoco (por acción u omisión del afectado, pero siempre de manera informada), específico e informado, es para la recogida y posterior tratamiento de datos de personas calificados como datos especialmente protegidos en el art .7 de la LOPD, que se ocupa del régimen de los datos que, por su especial naturaleza, han de apartarse de la regulación general, y que son los siguientes:

a. Los relativos a ideología, religión o creencia (art.16 CE). En este caso el afectado ha de ser informado sobre su derecho a no prestar los datos correspondientes.
b. En los anteriores y los que revelen la afiliación sindical, para ser objeto de tratamiento, el consentimiento al efecto ha de constar de forma expresa y por escrito, exceptuando únicamente, y sin perjuicio del necesario consentimiento para su cesión, los ficheros mantenidos por algunas organizaciones como los partidos políticos en lo referente a sus asociados.
c. Sobre los datos relativos al origen racial, salud y vida sexual se establece una prohibición general salvo que una ley disponga expresamente, por razones de interés general, o el afectado consienta expresamente tanto su recogida como su tratamiento y cesión.
d. Los ficheros exclusivamente dedicados a datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial o vida sexual quedan expresamente prohibidos.

Sin embargo la Ley establece una importante excepción para el tratamiento de los datos mencionados anteriormente, autorizándolo en determinados supuestos que por motivos médicos queden justificados:

Art. 7.6: "... cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho

tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente al secreto".

En relación con los datos relativos a la salud, ha de mencionarse el art. 8 LOPD el cual autoriza a las instituciones y centros de salud públicos y privados al tratamiento de los datos de carácter personal de las personas que acudan a dichos centros o sean tratados en ellos. Para lo cual habrá que estarse a la legislación estatal o autonómica sobre sanidad.

4. PRINCIPIO DE SEGURIDAD DE LOS DATOS Y REAL DECRETO 994/1999.

El art. 9 de la LOPD establece una obligación para el responsable del fichero y en su caso para el encargado del tratamiento, de adoptar las medidas técnicas y organizativas que sean necesarias para garantizar la seguridad de los datos de carácter personal. El objetivo es evitar que dichos datos puedan perderse, verse alterados o estén expuestos a un tratamiento o acceso no autorizado. Todas estas medidas de seguridad se encuentran desarrolladas reglamentariamente en el RD 994/1999 de 11 de Junio por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Este Reglamento pretende desarrollar el art. 9 LOPD a través de una serie de medidas que son los mínimos que debe cumplir todo fichero automatizado que contenga datos de carácter personal así como todo programa, sistema, locales, equipos, centros de tratamiento, que intervengan en el tratamiento de los datos.

Cuando se trate de ficheros que o bien por la naturaleza de los datos que contienen o bien por sus propias características requieran de un grado de protección mayor podrán establecerse además otras medidas especiales.

Las empresas deberán adecuarse para dar cumplimiento a la LOPD y su normativa de desarrollo. Pensemos que una compañía de seguros por ejemplo tiene en su poder y trata datos relativos a la salud, accidentes, propiedades, entre muchos otros, datos que pueden ser de personal propio, de clientes, proveedores, socios, por ello es de vital importancia la adecuación técnica a las exigencias legales. Algunos especialistas sobre el tema recomiendan, en cualquier entorno empresarial, establecer relaciones estrechas entre los departamentos tecnológicos, jurídicos, de seguridad física y recursos humanos de modo que queden bien definidos cual son los niveles de los datos existentes en sus bases para adoptar las medidas de seguridad adecuadas.

El Reglamento está dividido en cuatro capítulos y clasifica las medidas de seguridad en tres niveles:

- Básico,
- Medio
- Alto.

El art. 2 del Reglamento señala la razón de estos niveles:

"dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información".

Las medidas de seguridad de nivel básico deberá adoptarlas cualquier fichero que contenga datos de carácter personal y a partir de aquí el Reglamento describe las materias que además deben adoptar o bien el nivel medio o bien el nivel alto de seguridad.

Deberán adoptar junto a las medidas de nivel básico las de nivel medio los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los ficheros de acceso al público regulados en el art 28 LOPD, es decir, censo promocional y listas de personas pertenecientes a colegios profesionales. Además de las medidas de nivel básico y medio adoptarán las de nivel alto los ficheros que contengan datos relativos a la ideología, creencias, origen racial, salud o vida sexual así como los que, sin consentimiento de la persona afectada, fueron creados para fines policiales.

Fuera de estos casos, si el fichero contuviera datos personales que puestos en conjunto permitan obtener una evaluación de la personalidad del individuo serán necesarias las medidas de nivel medio.

Toda la normativa de seguridad debe ser implantada por el responsable del fichero mediante el llamado **documento de seguridad**, que contará con diferentes especificaciones en función del nivel y que es de obligado cumplimiento para todo el personal que tenga acceso a los datos personales y a los sistemas de información. Su contenido se establece para el nivel básico y se amplía para los otros dos niveles, por lo tanto, como mínimo deberá contener:

- Su ámbito de aplicación especificando los recursos protegidos.
- Las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- Funciones y obligaciones del personal
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los trata.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Procedimientos de realización de copias de respaldo para la recuperación de los datos.

Si se requieran medidas de seguridad de nivel medio y alto, además de todo lo indicado el documento de seguridad deberá contener:

- La identificación del responsable o responsables de la seguridad
- Los controles periódicos que se deban realizar para verificar lo dispuesto en el documento.
- Las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Además del documento de seguridad, el Reglamento se encarga de garantizar la protección de los datos por otras vías.

En el nivel básico:

- Exige la existencia de un registro de incidencias donde se hará constar el tipo de incidencia, cuando se ha producido, quien la notifica y a quien y que efectos produce.
- El acceso a los datos estará siempre bajo control, de modo que solo los usuarios autorizados en el documento de seguridad podrán acceder a los mismos, para ello el responsable del fichero se encargará de mantener una relación autorizada de los usuarios con acceso cuyas funciones y obligaciones con respecto a los datos de carácter personal están claramente definidas.
- La salida de soportes informáticos fuera de los locales en que está ubicado el fichero será a cargo del responsable del fichero.
- Existe un control de las copias de respaldo y recuperación.

En el nivel medio:

- Los sistemas de información e instalaciones de tratamiento de datos se someterán a auditoría interna o externa almenos cada dos años. El informe de auditoría deberá detectar las deficiencias y proponer las medidas correctoras o complementarias necesarias.
- En el registro de incidencias además de lo indicado para el nivel básico se requerirá consignar los procedimientos realizados de recuperación de datos, la persona que ejecutó el proceso, los datos restaurados y de haber sido necesario los datos grabados para su recuperación.
- Solo el personal autorizado en el documento de seguridad puede tener acceso a los datos.
- Se establece un sistema de entrada de soportes informáticos y de un sistema de registro de salida.

En el nivel alto:

Las medidas de seguridad de nivel alto exigen que el documento contenga lo indicado para los niveles básico y medio y además otras garantías:

- Respecto a la distribución de los soportes, se exige que se realice cifrando los datos o a través de un mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.
- El acceso a datos que están dentro del nivel de seguridad de nivel alto está muy restringido y controlado, de cada acceso se guardarán como mínimo la identificación del usuario, fecha y hora, nombre del fichero, tipo de acceso y si se denegó o aceptó.
- El periodo mínimo de conservación de los datos registrados será de dos años.

El documento de seguridad se irá adecuando a la normativa sobre datos de carácter personal.

Por otro lado, existen sistemas concretos como el HTTPS que son utilizados por entidades bancarias, compañías de seguros y cualquier tipo de servicio que requiera el envío de datos personales. Se trata de un sistema que crea un canal cifrado en el tráfico de información de modo que se consigue la confidencialidad de los datos que se están transmitiendo.

En cuanto a las normas sobre infracciones y sanciones establece el art. 44.3h) de la LOPD que es infracción grave vulnerar las normas de seguridad:

"mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

5. DEBER DE SECRETO.

Es importante hacer especial mención al deber de secreto regulado en el art. 10 de la LOPD ya que, en general, afecta a todas las fases de un tratamiento de datos:

Art. 10 LOPD: " 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 aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

La ley lo contempla como una obligación dirigida al responsable del fichero y a aquellas personas que intervengan en algún momento en el proceso de tratamiento de los datos, de guardar secreto profesional sobre los mismos. La obligación continúa incluso en el caso de que las relaciones con el titular o responsable del fichero dejen de existir ya que una revelación de datos que no se ajuste a la Ley puede llegar a causar graves perjuicios a su titular.

El incumplimiento de este deber puede ser calificado como sancionable de forma leve, grave o muy grave, en función del tipo de dato que se vea afectado. Para determinar el grado de sanción estaremos a lo establecido en los art 44.2, 44. 3g y 44.4g de la LOPD.

El art 44.2 e califica como infracción leve la vulneración del deber de secreto del art 10 de forma genérica, sin especificaciones sobre el tipo de dato. Dicha infracción puede pasar a ser una infracción grave en los supuestos contemplados en el art 44.3 g LOPD:

"la vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo".

Cuando se trate de la vulneración de los datos de carácter personal especialmente protegidos a los que hace referencia el ya mencionado art. 7.2 y 3 así como aquellos que hayan sido recogidos para fines policiales sin

consentimiento de su titular, es considerada como infracción muy grave, atendiendo al texto del art. 44.4g LOPD:

"la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afetadas":

6. COMUNICACIÓN DE DATOS

Hablar de comunicación de datos sólo tiene sentido en el caso de que se prevea realizar cesiones o comunicaciones de los mismos.

Se considerará cesión de datos de acuerdo con el literal del 11 LOPD:

"toda revelación de datos realizada a una persona distinta del interesado o afectado".

La LOPD establece este principio en su art.8 el cual ya en su punto 1 limita la comunicación a un tercero de los datos de carácter personal que sean objeto de tratamiento, a aquellos casos en que en que dicha comunicación sea necesaria para el cumplimiento de los fines directamente relacionados con las funciones del cedente y del cesionario. Por tanto, no se trata de una cesión propiamente dicha la transmisión de datos que se realice entre el encargado del tratamiento y, el responsable del fichero.

El consentimiento del interesado es un requisito necesario para que sea posible la comunicación. En relación al mismo hemos visto la previsión general del art. 6.1 LOPD que dice que:

"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".

Puede ser, por lo tanto, un consentimiento tácito o expreso pero que no deje lugar a dudas sobre su existencia.

Ahora bien, la regla general del consentimiento tiene excepciones en cuanto a la comunicación de los datos. Según el art 11 de la LOPD ésta no precisará de consentimiento cuando:

1. Cuando la cesión está autorizada en una Ley
2. Cuando se trate de datos recogidos de fuentes accesibles al público, y éstas son las mencionadas en el art 3.j. (como el censo promocional, los repertorios telefónicos, listados de personas pertenecientes a un grupo profesional, y los Diarios y Boletines oficiales).
3. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente concesión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
4. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
5. Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
6. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal y autonómica.

Asimismo este artículo establece que el consentimiento será nulo, para la comunicación de datos personales a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

Por otra parte, el consentimiento para la comunicación de los datos tiene un carácter de revocable, de ahí que el responsable del fichero, en el momento en que efectúe la primera cesión de datos, deba informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaliza de los datos que han sido cedidos y el nombre y dirección del cesionario, para que si lo consideran oportuno puedan ejercitar los derechos de acceso, cancelación y/o rectificación.

La comunicación de datos personales, implica a su vez que aquél a quien se comuniquen los datos, se obliga, por el solo hecho de la comunicación, a tratar los datos con el grado de protección exigido por la ley, y a la observancia de todas las disposiciones respecto a la misma.

Habrá que tener en cuenta que si la comunicación se efectúa previo procedimiento de "disociación", lo antes dicho, no le será aplicable. La expresión PROCEDIMIENTO DE DISOCIACIÓN está definida por la propia LOPD como:

"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable".

La cesión o comunicación de datos personales de un asegurado, por tanto, solo puede hacerse cuando haya sido consentida por el interesado, especialmente cuando se trate de información relativa a su salud y, en general, cualquier dato que sea considerado como "especialmente protegido.

En el caso del reaseguro, la cesión de dichos datos a las empresas reaseguradoras queda justificada cuando la misma es una información sobre la persona o personas objeto de cobertura necesaria para la formalización del contrato de reaseguro. De manera que sin dicha información el reasegurador no podría cotizar correctamente el riesgo.

En cuanto al régimen de sanciones el art. 44.4 b) de la LOPD califica como muy grave la infracción cometida al realizar una cesión de datos de carácter personal sin consentimiento del interesado, fuera de los casos en que esté permitido por la Ley.

7. ACCESO A LOS DATOS POR CUENTA DE TERCERO

El art. 12 LOPD se ocupa específicamente del acceso a los datos por parte de un tercero indicando que, cuando dicho acceso sea requisito necesario para la prestación de un servicio al responsable del tratamiento de los datos, no se considerará comunicación.

Por responsable del tratamiento se entiende:

"toda 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"

Al ser éste un tema delicado la Ley exige que quede regulado en un contrato el cual deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

Debe establecerse expresamente que el encargado del tratamiento únicamente trabajará los datos conforme a las instrucciones del responsable del fichero en cuestión, y que no los aplicará o utilizará con un fin distinto al que figure en el contrato, asimismo tampoco los comunicará a otras personas, ni siquiera para su conservación.

En el contrato se estipularán las medidas de seguridad a que se refiere el art 9 LOPD y que el encargado del tratamiento está obligado a implementar. Dicho contrato deberá incluir, entre otras, las siguientes menciones:

1. Indicación de que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del fichero.
2. El fin del contrato y que los datos no serán utilizados o aplicados con un fin distinto al indicado
3. Las medidas de seguridad que el encargado del tratamiento está obligado a implementar. De ello se deduce que el encargado del tratamiento es responsable de las medidas de seguridad.

La Ley responsabiliza al encargado del tratamiento y lo considera, también, responsable del mismo, en caso de que destine los datos a otra finalidad o los comunique o utilice incumpliendo lo establecido en el contrato. En estos casos deberá responder de las infracciones en que hubiera incurrido personalmente.
Cuando la prestación contractual ha sido cumplida, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, igual que los soportes o documentos en que consten cualquiera de los datos objeto del tratamiento.

4.3 El movimiento Internacional de Datos

Aunque la LOPD lo regula en su Titulo V art 33 y 34, he considerado oportuno tratar a continuación de la comunicación de datos y del acceso por cuenta de terceros, el tema del MOVIMIENTO INTERNACIONAL DE DATOS, también regulado en la Instrucción 1/2000 de 1 de diciembre de la APD y donde queda definido como:

"toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero".

En definitiva podemos definir transferencia internacional de datos como aquel transporte de datos entre sistemas informáticos por cualquier medio de

transmisión, así como el transporte de soportes de datos por correo o cualquier otro medio convencional. En virtud de la competencia que le otorga la LO 15/99, la Agencia de Protección de Datos, elaboró la Instrucción 1/2000 por la que se rigen los movimientos internacionales de datos.

Hasta la LOPD 15/1999 el movimiento internacional de datos era una materia que no venía recogida en un texto específico y su aplicación e interpretación debía adaptarse a las normas incluidas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de personas.

Existen dos Órdenes, una de 2 de Febrero de 1995 y otra de 31 de Julio del Ministerio del Interior, que establecen la relación entre países que disponen de un nivel de seguridad equiparable al de España en lo que atañe al tratamiento de estos datos.

La **regla general** que recoge el art 33 LOPD es que no podrán hacerse transferencias temporales, ni definitivas, de datos de carácter personal o que hayan sido objeto de un tratamiento concreto, o que hayan sido recogidos para someterlos a dicho tratamiento (finalidad) con destino a países que no proporcionen un nivel de protección equiparable al que presta la LOPD, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, quién solo podrá otorgarla si se obtiene las garantías adecuadas.

La transferencia temporal o definitiva de datos de carácter personal con destino a países que no proporcionen un nivel adecuado de protección equiparable al español, sin autorización del Director de la Agencia Española de Protección de Datos, está calificado en el art 44.e de la LOPD como infracción muy grave.

Será la Agencia de Protección de Datos quien deberá evaluar el carácter adecuado del nivel de protección que ofrece el país de destino, para lo cual deberá tener en cuenta todas las circunstancias que concurran en la transferencia o categoría de transferencias de datos. En particular tomará en consideración:

- La naturaleza de los datos
- La finalidad y la duración del tratamiento o tratamientos previstos.
- El país de origen y el país de destino final
- Las normas de Derecho, generales o sectoriales, vigentes en el país tercero que se trate.
- El contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Solo si, una vez analizado todo eso, se puede garantizar un grado de protección equivalente al de la LOPD en el país de destino se concederá la autorización de movimiento internacional de datos.

Los supuestos en que lo dicho no será de aplicación, los recoge la Ley en el art. 34, bajo el título "**excepciones**":

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia se a necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
d) Cuando se refiera a transferencia dinerarias, conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
g) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
h) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
i) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado

La no aplicación del régimen de autorización previa del art. 33 (norma general) no excluye que la transferencia deba sujetarse al régimen general de comunicación de datos a que se refiere el art. 11 LOPD. Es decir, si por ejemplo la transmisión internacional de datos se realizara a un país de la Unión de Europea (los cuales deben haber adaptado las directivas comunitarias en materia de protección de datos y por tanto garantizar un nivel adecuado de protección) no será necesario el pronunciamiento del director de la Agencia de Protección de Datos a que se refiere el art 33 LOPD pero esto no quita que la transmisión deba acogerse al régimen general de comunicación, es decir, que dicha cesión se efectúe a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario, así como el previo consentimiento del interesado, suficientemente informado, de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretendan comunicar.

En cualquier caso, las transferencias deben seguir el régimen general previsto en el art. 11 LOPD, donde se exige que dicha cesión se efectúe para el cumplimiento de fines "directamente relacionados con las funciones legítimas del cedente y cesionario", y siendo necesario el consentimiento informado y previo del afectado.

Resaltar que todo lo anterior será de aplicación cuando la cesión se efectúe entre sociedades pertenecientes a un mismo grupo empresarial, ya que, desde el momento en que estamos ante una entidad diferente a aquella a la que los interesados cedieron su datos, el cesionario tiene la condición de tercero a que se refiere el art. 3.i de la Ley Orgánica: "toda persona distinta del interesado" y podemos hablar, por tanto, de cesión o comunicación de datos. Pensemos en el caso

A esto hay que añadir la previsión del RD 1332/1994, de 20 de Junio, que desarrolla determinados aspectos de la Ley 5/1992 del tratamiento automatizado de los datos de carácter personal, la cual en su art 6 señala:

"la persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de datos, mediante escrito o soporte informático en modelo normalizado que al efecto elabore la agencia".

Entre los datos que deberán constar en dicho escrito o soporte informático se encuentran las cesiones de datos previstas así como las trasferencias temporales o definitivas que se prevean realizar a otros países, con expresión de los mismos.

El art. 8 del mismo Real Decreto establece que:

"cualquier modificación posterior en el contenido de los extremos a que se refiere el art 6 del presente Real Decreto se comunicará, a efectos de inscripción, en su caso, a la Agencia Española de Protección de Datos, dentro del mes siguiente a la fecha en que aquella se hubiera producido".

Por tanto, aunque la cesión o transferencia de datos no se hubiera comunicado inicialmente a la Agencia Española de Protección de Datos, deberá hacerse cuando posteriormente se prevea.

La circulación de información dentro de la Unión Europea es una necesidad inherente al funcionamiento del mercado interior y a libre circulación de personas y servicios. Cualquier comunicación de datos personales entre países comunitarios deberá respetar los principios de los que venimos hablando. Por poner un ejemplo de la importancia de que las comunicaciones internacionales se realicen con plena garantía del respeto a la privacidad de las personas, hablaremos de uno de los servicios transfronterizos que la Unión Europea ha creado en el marco del desarrollo del mercado interior.

Concretamente en el ámbito de los servicios financieros la Comisión Europea ha creado una red de reclamación de los consumidores para los servicios financieros, por la que se propone facilitar una acceso sencillo a procedimientos extrajudiciales de reclamación en asuntos transfronterizos. Dicha red es conocida como **FIN- NET.** Fin-Net se basa en la cooperación entre organismos nacionales de solución de litigios y funciona plenamente dentro de la Unión Europea. Su papel es fundamental en el desarrollo de un auténtico mercado interior de servicios financieros. Lo que pretende es ayudar a los consumidores y empresas a resolver los litigios con rapidez y eficacia sin acciones legales largas y costosas. Al tratarse de un procedimiento de denuncia extrajudicial no sustituye al procedimiento judicial y puede tener resultados diferentes, con este mecanismo lo que se busca es constituir una manera rápida, económica y sencilla de resolver conflictos. Ahora bien, la aspiración a un verdadero mercado interior nunca podría cumplirse sin la confianza del consumidor en el mismo, es decir, el ciudadano deber sentirse cómodo y seguro comprando servicios financieros en otro Estado Miembro si allí encuentra mayores ventajas o, si posteriormente es necesario, haciendo uso de la red de reclamación. Dicha confianza depende de varios factores y entre ellos, obviamente, la protección de sus datos personales.

El marco de Fin-net garantiza que el intercambio de información entre los distintos sistemas europeos sea eficaz y rápido tanto cuando se trata de información general como de información concreta para casos específicos.

Además para conseguir que los consumidores confíen es estos sistemas se exige a los distintos países participantes que cumplan una serie de garantías (como un procedimiento imparcial, justo y eficiente).

El procedimiento extrajudicial es siempre alternativo y en cada país puede adoptar una forma distinta. En el caso de los servicios financieros el modelo más frecuente es el llamado sistema del defensor del cliente (Ombudsman) pero existen otros como las comisiones sobre denuncias de consumo, las comisiones de arbitraje en materia de consumo y los sistemas de denuncia propios de las autoridades de supervisión. Concretamente en el estado español debemos mencionar la reciente Orden ECO 734/2004, de 11 de Marzo por la que se obliga a las siguientes entidades a disponer de un departamento o servicio de atención al cliente, separado de los distintos departamentos comerciales u operativos:

Entidades aseguradoras
Entidades gestoras de Fondos de Pensiones
Sociedades de Corredurías de Seguros
Sucursales en España de las entidades anteriores

La orden entró en vigor el 24 de Julio de este año y se aplicará a todas las personas físicas o jurídicas que tengan la condición de usuario.

No nos alargaremos más sobre este tema ya que no es el objetivo de este estudio pero sirva como ejemplo de la cantidad de datos personales que puede llegar a gestionar una empresa, solamente en uno de estos departamentos serían miles y miles.

La Unión Europea no se preocupa únicamente de las relaciones entre sus Estados Miembros, donde el nivel de protección queda en principio garantizado ya que son países que deben haber adoptado su legislación a las directivas comunitarias, también se ha preocupado por las transferencias de datos a terceros países no miembros. Por ejemplo, en el caso de Canadá tenemos que referirnos a la decisión de la Comisión de 20 de Diciembre de 2001 con arreglo a la Directiva 95/46/CE, sobre la adecuación de la protección de los datos personales conferida por la Ley Canadiense Personal Information and Electronic Documents Act. Mediante la citada decisión la Comisión manifiesta que la Ley Canadiense ofrece el nivel de protección adecuado autorizando las transferencias de datos personales entre Canadá y los Estados Miembros (es competencia de la Comisión manifestar si un Estado no miembro posee el nivel de protección necesario para que sea posible la transmisión de datos desde un estado sí miembro). Dicha decisión la adopta la Comisión a raíz de los estudios llevados a cabo por el Grupo de Trabajo de protección de las personas en cuanto al tratamiento de sus datos personales, creado en virtud del art 29 de la Directiva 95/46/CE. Lo que hace el grupo de trabajo es estudiar la legislación aplicable en materia de protección de datos en todo el territorio del estado en cuestión.

En el caso de Estados Unidos las negociaciones se inician en 1999, dado que su legislación sobre protección de datos no es uniforme si no que existen normas dispersas que regulan materias concretas, la decisión de la Comisión en cuanto a declarar la adecuación del nivel de protección de datos personales fue algo costosa. Finalmente el Departamento de Comercio de Estados Unidos presentó un borrador de "principios de puerto seguro" para garantizar que los operadores que se adhirieran a estos principios ofrecerían el nivel adecuado de protección exigido por la Directiva. El Acuerdo de Puerto Seguro consta de siete principios sobre:

- información a los afectados
- posibilidad de oposición
- principios de finalidad
- proporcionalidad
- procedimientos para la satisfacción de los derechos de los afectados
- seguridad
- integridad de los datos

Finalmente la Comisión Europea, mediante su Decisión de 26 de Julio de 2000, y con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, se pronunció sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada.

Igual pronunciamiento se hizo respecto a la Bahía de Guernsey, perteneciente a la Corona británica aunque no forma parte del Reino Unido, a través de la decisión de la Comisión de Noviembre 2003 relativa al carácter adecuado de la protección de datos personales en Guernsey.

En el marco de las relaciones de la Unión Europea con Latinoamérica, en materia de protección de datos, pondremos en primer lugar el ejemplo de Argentina. El Gobierno de la República Argentina solicitó a la Comisión Europea que determinara si dicho país garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el artículo 25 de la Directiva 95/46 , de Protección de Datos. Para poder considerar esta petición la Comisión Europea solicitó el pronunciamiento del Grupo Europeo de Autoridades de Protección de Datos (Grupo de Trabajo 29) el cual se pronunció favorablemente sobre el nivel de protección que ofrecía la Ley sobre protección de Datos Personales de Argentina, del año 2000. Por la Decisión de 30 de Junio de 2003, Comisión declaró públicamente dicha adecuación.

Las relaciones con Iberoamérica son objetivo prioritario de la Agencia Española de Protección de Datos quien anualmente promueve un Encuentro Iberoamericano de Protección de Datos. En el encuentro del 2003 en La Antigua (Guatemala) se creó la **Red Iberoamericana de Protección de Datos** como un foro permanente que pretende potenciar las relaciones entre los estados Iberoamericanos. Los objetivos fundamentales de la red se encuadran en la Declaración de la Antigua.

4.4 Derechos de las personas

1. DERECHO DE IMPUGNACIÓN DE VALORACIONES

Los datos personales de una persona, al ser tratados y cruzados entre sí pueden llevar a formar un perfil de su personalidad. El derecho a la impugnación de valoraciones trata de proteger a las personas frente a decisiones con efectos jurídicos que estén basadas únicamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad.

De modo que, cuando existe un acto administrativo o una decisión privada que impliquen una valoración del comportamiento del individuo y dicha valoración sólo se fundamente en el tratamiento de datos personales el afectado, podrá impugnar el acto o decisión. Se trata del caso en que a través del tratamiento de los datos se ha llegado a una definición de las características o personalidad del individuo y ésta ha sido utilizada para fundamentar una decisión con efectos jurídicos.

Con esta finalidad el afectado tiene derecho a que se le informe sobre quién es el responsable del fichero y que criterios de valoración y programas ha utilizado para adoptar la decisión.

Únicamente cuando el afectado lo solicite, la valoración sobre su comportamiento, basada en el tratamiento de datos, podrá tener valor probatorio, es decir, solo el titular de los datos podrá consentir que se utilice como prueba el perfil de su personalidad derivado de los datos que sobre él mismo constan en un fichero.

2. DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

En un breve artículo, el 14, la LOPD regula este derecho cuyo contenido queda redactado de la siguiente manera:

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

En cuanto al procedimiento el Registro General será de consulta pública y gratuita.

3. DERECHO DE ACCESO

Uno de los extremos sobre los que el responsable del fichero ha de informar de modo expreso, preciso e inequívoco, a los interesados, con ocasión de solicitar sus datos personales, es sobre la posibilidad de ejercer su derecho de acceso, junto con los de rectificación, cancelación y oposición. Este derecho se encuentra definido en el art. 15 LOPD:

"el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".

El ejercicio de este derecho es personalísimo y debe ser ejercido directamente por los interesados ante cada uno de los responsables /titulares de los ficheros. Por tanto, cualquier persona puede dirigirse ante la empresa u organismo público de los que sabe que tienen sus datos, solicitando información sobre qué datos tienen y cómo los han obtenido (derecho de acceso). Deberá dirigirse directamente al responsable del fichero utilizando cualquier medio que permita acreditar el envío y la recogida de su solicitud, acompañando copia de su DNI e indicando el fichero o ficheros a consultar. El responsable de fichero tiene la obligación de atender la solicitud del interesado.

La información pretendida podrá obtenerse mediante la consulta de sus datos a través de diferentes medios: su visualización, escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. No será posible le acceso por estos medios a la información de terceros.

Si el interesado que envía su consulta no es contestado en un plazo de un mes desde que su solicitud fue recibida, podrá dirigirse a la AEPD para que ésta se encargue de hacer efectivo el ejercicio de este derecho.

Tal y como dice el art. 15 LOPD, este derecho no puede ejercitarse por intervalos inferiores a doce meses "salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes".

La Agencia Española de Protección de Datos tiene en su página web, a disposición de todos, los modelos de formulario para el ejercicio de este derecho, de los cuales anexamos copia.

4. DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

El ejercicio del derecho de cancelación o rectificación es también personalísimo, lo que significa que el titular de los datos deberá dirigirse directamente al responsable del fichero de la entidad que se trate, utilizando cualquier medio que permita acreditar el envío y la recogida de su solicitud, para el ejercicio de sus derechos, acompañando copia de su D.N.I. Si el interesado desconoce la dirección del responsable del fichero podrá solicitarla a la Agencia Española de Protección de Datos.

Estamos tratando aquí de dos derechos diferentes aunque la Ley los recoge conjuntamente en el art. 16:

- Por un lado, el derecho de rectificación posibilita al afectado o interesado para solicitar al responsable del fichero la rectificación de sus datos cuando estos son erróneos o incorrectos. Será el interesado quién deberá indicar que dato es erróneo o incompleto así como la corrección que debe realizarse, la cual deberá acreditar.

- Por otro lado, el derecho de cancelación se refiere al derecho del afectado para revocar el consentimiento que otorgó en otro momento para el tratamiento de sus datos, de modo que revocado éste, los datos personales deberán ser excluidos de tratamiento. El responsable del fichero podrá solicitar al interesado que justifique la solicitud realizada.

Ejercitado el derecho de rectificación o cancelación, el responsable del fichero deberá atender la solicitud formulada por el interesado en un plazo de diez días de no recibir respuesta en este plazo, podrá reclamar ante la Agencia Española de Protección de Datos.

Hay que tener en cuenta que la cancelación de los datos obliga a su bloqueo hasta que prescriban todas las acciones que, como consecuencia del tratamiento, puedan producirse en el futuro y a fin de que puedan ser atendidas. Por tanto, hasta que llegue dicha fecha de prescripción los datos permanecerán a disposición de la Administración, Jueces y Tribunales para la atención de dichas posibles responsabilidades. Posteriormente deberá procederse a la supresión de los mismos.

La ley también establece que en el caso de que los datos hubieran sido comunicados con anterioridad a su rectificación o cancelación una vez se haya producido cualquiera de las dos, deberá informarse de este hecho a quien se comunicaron.

5. DERECHO A INDEMNIZACIÓN

Con su art 19 la LOPD otorga a los interesados que, como consecuencia del tratamiento de sus datos sufran daños o lesiones en sus bienes o derechos, el derecho a ser indemnizados. El daño o lesión deberá producirse como consecuencia del incumplimiento de la LOPD. A los efectos de imputar responsabilidades el art 19 distingue entre ficheros de titularidad pública y privada, señalando que en el caso de lo primeros la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidades de las Administraciones Públicas mientras que en el caso de los segundos la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

6. TUTELA DE LOS DERECHOS

Ya hemos mencionado en relación a los derechos de oposición, acceso, rectificación o cancelación, que el interesado que ejercite cualquiera de estos derechos y se le denieguen, podrá dirigirse a la Agencia Española de Protección de Datos la cual se pronunciará sobre la procedencia o improcedencia de la denegación en un plazo de seis meses.

Así pues la Ley otorga a la Agencia Española de Protección de datos el papel de garante de los derechos referidos a la protección de los datos personales. La relevancia de este ente es evidente y es por ello que vamos a tratarlo con más detalle en otro capítulo.

7. PROCEDIMIENTO DE OPOSICIÓN, ACCESO, RECTIFICACIÓN O CANCELACIÓN;

Este es el título que recibe el art. 17 LOPD. De los procedimientos de acceso, rectificación o cancelación hemos estado hablando en los puntos anteriores, sobre todos ellos el art 17 dice que su ejercicio no conllevará contraprestación alguna.

En cuanto al derecho de oposición debemos decir que se trata de la negativa del afectado a la continuación del tratamiento de sus datos y hace referencia, por tanto, a la cancelación genérica. En lo referente a su procedimiento, debemos necesariamente remitirnos al art 6.4 de la Ley 15/1999, que establece:

"…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..".

Asimismo, en el caso del tratamiento de datos obtenidos de fuentes accesibles al público con fines de publicidad y prospección comercial, el interesado tiene derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja para el tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

4.5. La inconstitucionalidad de los art. 21.1 y 24 de la LOPD. Comentario a la Sentencia 292/2000 del Tribunal Constitucional

La LOPD otorga a los ciudadanos seguridad jurídica en cuanto al tratamiento de sus datos ya que permite a sus titulares el control sobre los mismos. Para ello establece mecanismos de salvaguarda en todas las fases del tratamiento, desde que son recogidos hasta cualquier uso posterior que pueda hacerse de ellos. Los derechos reconocidos a los titulares de los datos se cruzan con las obligaciones impuestas a los responsables y titulares de los ficheros frente cualquier infracción que puedan cometer.

De este modo la Ley crea un entorno de confianza para las personas físicas con respecto a sus datos personales impidiendo un uso arbitrario de los mismos. Sin embargo, en el momento de su aprobación la LOPD en dos de sus artículos, parecía contradecir su propia finalidad poniendo en peligro la seguridad en el tratamiento de los datos personales, este hecho motivó que el Defensor del Pueblo impusiera un Recurso de Constitucionalidad, al que dedicamos el presente capítulo.

Justo en este punto de la exposición y una vez hemos visto los principios de la protección de datos y los derechos que la LOPD 15/1999 otorga a las personas, será fácil entender la resolución del Tribunal Constitucional de 292/2000 de 30 de Noviembre por la que declaró inconstitucionales algunos incisos del art. 21.1 y art. 24.1 y 2 de la LOPD.

El recurso fue interpuesto por el Defensor del Pueblo quien entendía que dichos preceptos de la LOPD lesionaban los derechos a la libertad informática de los ciudadanos.

A continuación se anexa la versión inicial de ambos artículos, los incisos remarcados en negrita son los únicos impugnados por el Defensor del Pueblo y declarados posteriormente inconstitucionales por el Tribunal Constitucional:

Art 21 Comunicación de datos entre Administraciones Públicas

1.Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo **cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso**, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

7. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3 .No obstante lo establecido en el artículo 11.2 b, la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley**.**

Artículo 24.Otras excepciones a los derechos de los afectados.

1.Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos 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, a la seguridad pública o a la persecución de infracciones penales o administrativas.

2.. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

Recordemos que, los apartados 1 y 2 del art. 5 LOPD al que remite el art. 24.1 establecen los requisitos y garantías del derecho a la información en la recogida de datos y el art. 15 y el 16.1 LOPD, a los que remite el art. 24.2 hacen referencia, respectivamente, al derecho de acceso a los datos personales así como al deber del responsable del tratamiento de hacer efectivo el derecho de rectificación o cancelación de los datos en el plazo de diez días.

A través del art. 21.1 la LOPD estaba permitiendo que una norma reglamentaria autorizara la cesión de datos entre Administraciones Públicas y además, con el fin de que dichos datos fueran empleados en materias distintas de las que motivaron su recogida y sin consentimiento previo del interesado. Hecho éste que se contradice con el contenido del derecho a la protección de datos ya que deja fuera del alcance del propio individuo el control de la información que circula sobre él.

Sobre este punto el Tribunal Constitucional manifestó que la limitación de un derecho fundamental, de acuerdo con el art. 53.1 CE, como es el derecho a la libre disponibilidad de los datos de carácter personal, se reserva en exclusiva a la Ley. En palabras del Tribunal Constitucional:

"el motivo de la inconstitucionalidad del art. 21.1 LOPD resulta, pues, claro. La LOPD en este punto no ha fijado por sí misma, como le impone la Constitución (art. 53.1 CE) los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art 11 LOPD en relación con lo dispuesto en los art 4, 6 y 34 e) LOPD) sino que se ha limitado a identificar la norma que puede hacerlo en su lugar. Norma que bien puede ser reglamentaria (…) lo que resulta ser, desde luego, contrario a la Constitución".

Para una correcta protección de los datos personales es necesario que la persona conozca y consienta el almacenamiento y el uso que se hace de su información, en torno ha esto giran los principios de la protección de datos y los derechos de las personas sobre los mismos que hemos visto en el capítulo anterior por lo que ciertamente la LOPD vulneraba sus propios principios otorgando a la Administración unas facultades que no le corresponden. También así en el art. 24 LOPD, apartados 1 y 2.

De un lado, en el apartado 1, la LOPD habilita a la Administración para que restrinja derechos fundamentales (concretamente el derecho a ser informado del art 5 LOPD) en cumplimiento de sus "funciones de control y verificación" lo que el Tribunal entendió que era lo mismo que decir, prácticamente en todo caso, ya que, la Administración en sus relaciones con los administrados, cuando necesita de sus datos personales hará uso de estas potestades:

"en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración".

Esta facultad de la Administración provoca, sin duda, inseguridad jurídica a las personas en cuanto al tratamiento de sus datos ya que deja a la voluntad de la Administración la posible restricción de sus derechos.

Y en el mismo sentido se pronuncia el Constitucional sobre la expresión "interés público" del art. 24.2 LOPD ya que, como fundamento de la limitación de derechos fundamentales "encierra un grado de incertidumbre aún mayor".

El concepto "interés público" es tan impreciso y tan amplio que prácticamente elimina el contenido del derecho porque en todas las actuaciones de la Administración podríamos decir que está presente. Si al menos se definieran por ejemplo a través de un listado cerrado las circunstancias en las que existe interés público el nivel de incertidumbre sería algo menor pero es que el art 24.2 ni siquiera establece cuales pueden ser estos intereses ni las circunstancias en que pueden hacerse valer para restringir los derechos. Veamos los comentarios al respecto recogidos en la sentencia 292/2000 TC:

"los motivos de limitación adolecen de tal grado de indeterminación que deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco del `poder normativo que defrauda la reserva de ley".

A razón de estos argumentos la STC TC 292/2000 declaró inconstitucionales y nulos los incisos comentados de los art. 21.1 y 24.1 y 2 de la LOPD.

5. El art. 29 de la Ley 15/1999. Prestación de servicios de la información sobre solvencia patrimonial y crédito

Art 29 LOPD:

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2.Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de las obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés ...."

De este modo el art. 29 LOPD regula lo que se ha llamado las "listas de morosos", es decir, listados autorizados en los que se incluyen los datos de las personas que han incumplido el pago de sus deudas en un plazo establecido. Normalmente son administrados por sociedades mercantiles con ánimo de lucro en su explotación. Se trata en definitiva de registros de solvencia ya que su finalidad es ofrecer información sobre el riesgo comercial que supone la contratación con personas que tienen algún precedente de incumplimiento.

Estos registros de almacenamiento de datos relativos al incumplimiento de obligaciones dinerarias solo pueden obtener sus datos de un acreedor, o de quien actúe de su cuenta o interés. Según el art. 29 LOPD tal y tal y como se explica en la página web de la Agencia de Protección de Datos, para formar parte de los ficheros de deudores hay una serie de requisitos que son imprescindibles y que deben darse siempre:

- La existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada.
- El requerimiento previo de pago a quien corresponda, en su caso, del incumplimiento de la obligación
- Que el acreedor o quien actúe por su cuenta e interés, se asegure de que concurren todos los requisitos exigidos en los apartados anteriores, en el momento de notificar los datos adversos al responsable del fichero común.
- Cuando el dato cedido por el acreedor resulte inexacto o no esté actualizado, deberá ser éste, o quien actúe por su cuenta e interés, quien comunique al responsable del fichero común en el mínimo tiempo posible la modificación del dato, sin perjuicio de los establecido en el artículo 16 de la Ley Orgánica sobre el derecho de rectificación y cancelación.
- El responsable del fichero común deberá proceder a la cancelación cautelar del dato cuando el deudor aporte un principio de prueba documental suficiente, que desvirtúe alguno de los requisitos necesarios que se describen en los apartados anteriores.

Los ficheros más conocidos en los que se incluyen morosos son Asnef Equifax; Equifax Ibérica, S.L; Información Técnica de Crédito S.L (INCRESA); el RAI, dependiente del centro de cooperación Interbancaria; el Experian Bureau de

Crédito S.A (BADEX) y el servicio de Ficheros Mecanizados S.A, antiguamente conocido como intérpretes S.L. Cuando han transcurrido noventa días desde que se produce el impago, las entidades financieras acuden a alguno de estos ficheros para notificar los datos del supuesto moroso.

Un dato a resaltar es que para que el acreedor pueda facilitar el dato del impago al registro de morosos no es preciso el consentimiento del deudor, ni siquiera su conocimiento, pero sí se le deberá informar. La obligación de comunicar al interesado la inclusión de sus datos en un fichero de este tipo viene determinada por el art. 29.2 de la Ley Orgánica y es una obligación que debe cumplir el responsable del fichero en el plazo máximo de treinta días desde dicha inclusión. El afectado, deudor, debe ser informado de qué datos han sido incluidos así como de su derecho a recabar información sobre la totalidad de ellos. Esta notificación debe efectuarse para cada una de las deudas con independencia de que se tengan con el mismo acreedor o coincida alguno de ellos.

Si el afectado solicita información sobre sus datos, el titular del registro de morosos deberá facilitarle la totalidad de la información disponible así como el uso que se ha hecho de dicha información y las personas a las que se ha facilitado, el **derecho de acceso** del afectado, por tanto, debe quedar garantizado en todo momento como se desprende de la obligación que el artículo 29.3 de la LOPD impone al responsable del fichero de facilitar las evaluaciones y apreciaciones que se hayan comunicado sobre el afectado en los últimos seis meses, así como el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

Es importante destacar que sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados ya que es este el objeto del fichero y además estos datos, cuando sean adversos, no podrán referirse a más de seis años y siempre que respondan con veracidad a la situación actual de los afectado, es decir:

- No pueden facilitarse datos sin relevancia económica
- El dato registrado (por ejemplo un impago) no puede tener más de seis años de antigüedad, contados desde la fecha de inclusión del dato en el Registro.
- No puede incluirse ningún impago o cumplimiento irregular, sino desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico.
- Los datos de carácter personal registrado deberán responder a la situación actual del afectado.

Si el afectado que ha accedido a la información sobre sus datos y considera que estos son incorrectos podrá solicitar la modificación de los mismos a través del ejercicio del **derecho de rectificación.** Como ya vimos este derecho está regulado en el art. 16 LOPD, se trata de un derecho personalísimo que solo el afectado podrá ejercitar y que lo posibilita para solicitar la rectificación de sus

datos cuando estos son erróneos o incorrectos. Del mismo modo podrá el interesado o afectado ejercer su **derecho de cancelación**, también regulado en el art 16 LOPD, mediante el cual el afectado podrá revocar el consentimiento que otorgó en otro momento para el tratamiento de sus datos, de modo que revocado éste, los datos personales deberán ser excluidos de tratamiento.

Para el ejercicio de estos derechos podrá dirigirse el interesado o afectado tanto al acreedor como directamente a la persona responsable del registro, veamos a continuación los diferentes supuestos:

- Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del registro de morosos, éste comunicará dicha solicitud a la entidad que haya facilitado los datos (acreedor), para que ésta la resuelva. En el caso de que el responsable del registro no haya recibido contestación por parte de la entidad en el plazo de diez días, procederá a la rectificación o cancelación cautelar de los mismos.

- El interesado dirige su solicitud a cualquier entidad de las participantes en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, deberá proceder a la rectificación o cancelación de los datos en sus ficheros y notificarlo al responsable común en un plazo de diez días.

- Si el interesado dirige la solicitud al acreedor, sobre datos que la entidad no hubiera facilitado al registro de morosos, el acreedor informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

Los trámites de rectificación serán siempre gratuitos y la comunicación deberá enviarse por escrito y por cualquier medio que permita acreditar el envío y la recepción acreditando:

- Copia del DNI
- Datos a cancelar o rectificar en el fichero o ficheros
- Domicilio a efectos de notificaciones
- Fecha y Firma del solicitante.

Cuando el responsable del fichero de morosos reciba una solicitud deberá contestarla con independencia de que en sus ficheros existan o no datos personales del solicitante. Además si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación a aquellas entidades que hubieran conocido los datos.

La cancelación supone que los datos sean bloqueados y que sólo se conserven para atender posibles reclamaciones que puedan derivarse del tratamiento de los datos, durante el plazo de prescripción de éstas, en este periodo únicamente estarán a disposición de las Administraciones Públicas, Jueces y

Tribunales. Una vez cumplido dicho plazo de prescripción, podrá procederse a la supresión de los datos.

La rectificación podrá negarse en un plazo de diez días pero siempre mediante resolución motivada. El afectado, en estos casos, podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos, que se asegurará de la procedencia o improcedencia de la denegación.

Los ficheros autorizados por el art. 29, relacionados con la solvencia patrimonial y crédito de las personas físicas, a los que nos estamos refiriendo se encuadran dentro de los ficheros sujetos a medidas de seguridad de nivel medio (vimos en su momento el desarrollo del Reglamento de Medidas de Seguridad) por lo tanto, de acuerdo con dicho Reglamento y concretamente con su art. 17.2 existe la obligación de someterlos a auditoria externa o interna de modo que se verifique el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad de datos. Las auditorías deberán llevarse a cabo al menos cada dos años.

Por otro lado la Agencia Española de Protección de datos ofrece un servicio de atención al ciudadano en el que facilita los requisitos para el ejercicio de los derechos del usuario. Si se detecta una infracción en la Ley, la Agencia puede abrir expedientes sancionadores o bien a las empresas acreedoras o bien a las sociedades que administran los registros de morosidad. Hay que destacar aquí que la actividad sancionadora y de control de la agencia ha contribuido a reducir notablemente el número de quejas y reclamaciones con respecto a los registros de morosos.

Asimismo la Agencia, consciente del perjuicio que puede suponer para una persona el estar incluido en uno de estos listados, ha recomendado a los gestores de listados de morosos que cuando exista al menos “un principio de duda” en relación a la supuesta deuda, no se incluya en los archivos a ninguna persona.

Otra cuestión que ha suscitado un gran debate es el llamado “saldo cero”, es decir, algunas entidades mantienen dentro de sus listados de morosos los datos de personas que ya han saldado completamente su deuda. Aunque la AEPD sostiene que toda persona que ha cumplido con su deuda no debe permanecer en el fichero, la Dirección General de Defensa de la Competencia defiende una permanencia de tres meses.

Lo que sí es evidente es que la morosidad supone un inconveniente para el desarrollo del mercado y por eso se buscan mecanismos para reducirla y controlarla lo que debe hacerse dentro de un marco de respeto a los derechos de las personas, aunque en este estudio nos centramos en ella en la medida en que puede afectar a los datos personales de los individuos que como morosos quedan incluidos en un listado, y alejándome de mi objetivo, no quería pasar por alto que tanto a nivel comunitario como nacional se está trabajando con el objetivo de reducir la morosidad y los efectos negativos que produce en las transacciones comerciales. En este entorno el Gobierno aprobó el 24 de

Junio de 2004 un Proyecto de Ley por la que se establecen medidas de lucha contra la morosidad en las operaciones comerciales y por el que queda transpuesta al ordenamiento jurídico español la directiva comunitaria 2000/35/CE, aunque, dicho sea de paso, esta transposición llega con dos años de retraso en el plazo que la comisión concedió a los Estados Miembros. El ámbito de aplicación de esta ley se limita a los pagos efectuados como contraprestación en operaciones comerciales entre empresas y entre estas y la administración, se trata de proteger, a las pequeñas y medianas empresas excluyéndose expresamente a las operaciones en que intervengan consumidores, los intereses relacionados con otros pagos (letras de cambio o cheques), los pagos realizados por compañías de seguros, así como las deudas sometidas a procesos concursales.

6. El art 30 de la LOPD. Tratamientos con fines de publicidad y de prospección comercial

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.
2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.
3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.
4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán datos de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Con este artículo la LOPD regula las comunicaciones comerciales y es importante destacar que el tratamiento que se da a las mismas es diferente al que se contemplaba en la LSSI (Ley de servicios de la sociedad de la información), en especial en lo relativo a las comunicaciones comerciales no solicitadas realizadas por vía electrónica. En la LSSI y, concretamente en sus art. 19 y ss, se establecía un régimen especial respecto al recogido en la LOPD para los envíos publicitarios.

Es decir, con el artículo 19.1 se permite la utilización de datos provenientes de fuentes accesibles al público sin que para ello sea necesario el consentimiento del afectado, siempre y cuando se le dé la información que esta ley marca en su art. 15 y se le garantice el derecho de oposición libre de gastos. Ahora bien, todo esto sería aplicable cuando se tratase de medios de comunicación que podríamos llamar tradicionales.

En el caso de utilizarse medios electrónicos entraría en juego la regulación de la LSSI la cual, en su art 21, prohibía el envío de comunicaciones publicitarias a través de medios electrónicos si previamente no habían sido solicitadas o expresamente autorizadas por los destinatarios, lo que es lo mismo que decir que la LSSI exige el consentimiento expreso del afectado en las comunicaciones realizadas por vía electrónica cosa que no hace la LOPD para el resto de comunicaciones.

En todo lo demás cabe decir que la LOPD es plenamente aplicable a los tratamientos de datos personales que tengan lugar en internet, lo que permite a la Agencia Española de Protección de Datos supervisar y defender aquellas actividades cubiertas por la LSSI, los servicios de la sociedad de la información.

A nivel comunitario se ha trabajado en este sentido y la ultima directiva comunitaria relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónica, la 2002/58/CE, aborda una serie de temas entre los que se encuentra el envío de mensajes electrónicos no solicitados, el llamado spam.

Como curiosidad diremos que el término SPAM (práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados), se utilizaba para aludir a la carne enlatada que se proporcionada a los soldados americanos y que debido a su pobre calidad, ganó una fama bastante negativa. Originariamente se trataba de un jamón con especias (spiced Ham) producido por Hormel en 1926 como el primer producto de carne enlatada que no requería refrigeración, esta característica es lo que hacía que estuviera en todas partes y que fuera ideal para los soldados.

La directiva comunitaria establece que los usuarios han de dar su consentimiento previo antes de recibir mensajes del tipo SMS y demás mensajes electrónicos recibidos en cualquier equipo terminal, fijo o móvil. Ahora bien, permite el envío de publicidad electrónica no solicitada a aquellas personas que hubieran facilitado su dirección electrónica en el curso de una relación comercial previa con quien remite la publicidad, para la promoción de productos o servicios similares, siempre y cuando se le informe en cada envío de la posibilidad de oponerse a continuarla recibiendo de forma clara, oposición que debe poder realizar gratuitamente y de manera sencilla. Al mismo tiempo la directiva deja libertad a los Estados Miembros para que regulen si quieren el consentimiento previo o consideran suficiente el derecho de oposición para aquellos con los que no existe dicha relación comercial previa.

Como hemos anticipado la LSSI, Ley 34/2002, tomó partido en cuanto a la disyuntiva de permitir o no el envío masivo e indiscriminado de correspondencia comercial a través de internet (spam) y, aunque no lo prohibió, la supeditó siempre a que el destinatario solicitara o autorizara expresamente la misma, de este modo pretendía evitar que el usuario se viera invadido por una publicidad no querida. Así, en el terreno de las comunicaciones electrónicas se separó la LSSI de la regulación que la LOPD en su art. 30 había acogido y que continúa vigente actualmente para las comunicaciones tradicionales. Sin embargo esta regulación de la LSSI generó una serie de problemas en el sentido que los requisitos de consentimiento que exige provocaron que muchas empresas se dirigieran a los usuarios solicitando su autorización para remitirles informaciones lo que causó un efecto contrario al perseguido por la Ley al generar el envío de miles de correos.

La nueva Ley General de Telecomunicaciones 32/2003 de 3 de Noviembre, más acorde con las directrices de la última directiva comunitaria en materia de protección de datos, en su disposición final primera salva el problema generado por la LSSI, al permitir la utilización del correo electrónico para remitir mensajes a aquellas personas o empresas con las que se haya mantenido una relación contractual sin necesidad de una autorización previa por parte de éstas y siempre que el cliente no hubiera manifestado expresamente su oposición a recibir este tipo de mensajes. La Ley General de Comunicaciones da un nuevo redactado a los art. 21 y 22 de la LSSI que quedan de la siguiente manera:

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. **Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente**. **En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija**».

«Artículo 22. Derechos de los destinatarios de servicios.
1. **El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente**.
A tal efecto, los prestadores de servicios deberán habilitar **procedimientos sencillos y gratuitos** para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.
Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.
2. Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.
Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario».

Recordemos que la Ley de Telecomunicaciones transpone a la legislación española la directiva 2002/58/CE en la medida que afecta a las redes y servicios de telecomunicaciones y en esa función autoriza las comunicaciones con el cliente siempre que este no haya manifestado expresamente su oposición a recibir mensajes electrónicos.

El 80% de spam europeo es en inglés y el 80% del mismo se origina en Estados Unidos donde el criterio que se sigue es diferente al europeo ya que si a nivel comunitario no se permite el envío comercial si el receptor no lo autoriza expresamente al remitente (la llamada cláusula opt-in), en Estados Unidos el criterio es autorizar de entrada el envío y que sea el receptor quien tome la iniciativa de comunicar que no quiere recibirlo (cláusula opt-out), en esta dirección ha tomado algunas medidas como la de etiquetar el correo pornográfico para que se advierta explícitamente su contenido.

El problema del Spam se ha puesto de manifiesto en diferentes foros a nivel mundial, según Brightmail el 50% de los mensajes que circulan por Internet son spam y en el mismo sentido la UE ha resaltado que los e-mail publicitarios no deseados suponen ya más de la mitad de los correos electrónicos que circulan por la Red. A raíz de este problema han empezado a surgir propuestas de las propias empresas asociadas a sellos digitales u otros medios de pago como requisito previo al envío de correos comerciales. Por ejemplo la compañía Goodmail propone un sistema de pago que consiste en que la empresa que quiere remitir masivamente un correo comercial lo hace a través de Goodmail, los clientes de Goodmail (la empresa) deben garantizar que cumplirán con las peticiones de baja de quienes reciban su correo. El proveedor del servicio de acceso recibe el paquete de correos de correos de sus cuentas, con sello cifrado y garantizando la limpieza de los archivos, y cobra al remitente por el envío a sus abonados. También Hotmail ha conseguido rebajar su tráfico de spam mediante medidas tecnológicas y AOL intenta evitar la llegada de correo basura desde servidores que no estén identificados como de la empresa emisora, eso por ejemplo, bloquearía todo el spam que circula gracias a la instalación de virus en máquinas particulares ya que muchos virus abren una puerta trasera del ordenador infectado para

permitir su control al autor del mismo y ese control puede utilizarlo para que la máquina envíe spam sin que el propietario de la mismo se dé ni cuenta.

En definitiva, se pone de manifiesto con todas estas medidas que el spam es un problema real contra el que se intenta luchar tanto desde las propias compañías como desde los estados y la UE, con la aprobación de normativas que abren una batalla legal contra el envío masivo de correo electrónico no autorizado.

En el ámbito nacional, los principales proveedores de e-mail han constituido un Consejo con el objetivo de buscar soluciones efectivas contra el spam de ahí surge el llamado proyecto PePi-II, que pretende mejorar la calidad del correo electrónico. Se trata de un proyecto compartido en el que intervienen todos aquellos que hacen posible un e-mail: proveedores, creadores de páginas web, usuarios y administración. PePi-II se propone dotar a todos ellos de medios para mejorar la calidad y las prestaciones del e-mail.

El nombre lo debe al faraón PePi-II, del año 2002 AC, y a la calidad de los materiales y de la gestión de sus servicios de comunicación que han hecho que muchas de sus comunicaciones se hayan conservado hasta nuestros tiempos.

6.1. Las Listas Robinson

Actualmente cualquier ciudadano que no quiera recibir publicidad en su domicilio debe inscribirse en un registro, esto son las llamadas **Listas Robinson,** es decir, un fichero precisamente para quienes no quieren figurar en ninguno. El fichero Robinson de España fue creado en 1992 promovido por la Federación de Comercio Electrónico y Marketing Directo (Fecemd) y con el fin no lucrativo de reforzar las buenas relaciones entre los profesionales del sector del Marketing Directo y el público en general. El servicio de Listas Robinson (SLR) se enmarca dentro del ámbito de la publicidad personalizada, es decir, aquella publicidad que recibe un usuario a su nombre y dirección y está dirigido a consumidores particulares y empresas.

Estas listas pueden ser elaboradas en el ámbito interno de una entidad o a través de una asociación o de un grupo de empresas. La más numerosa, creada en 1992, es la lista de Fecemd, donde se agrupan más del 90% de las empresas del sector.

Las empresas que se dedican al marketing directo y al comercio electrónico en realidad son las primeras interesadas en promover este tipo de lista ya que no les interesa que sus mensajes promocionales lleguen a personas poco receptivas y así evitan que su publicidad se pierda con consumidores que no tienen el más mínimo interés en ella.

Aunque se trate de una relación de personas que no quieren recibir publicidad, es un fichero y, por tanto, está sometido a la Ley Orgánica de Protección de Datos, los datos deben recabarse con el consentimiento de los interesados y no deben utilizarse para ningún otro fin.

Las empresas de publicidad directa deben asegurarse de que los listados de direcciones que emplean han sido enfrentados con las listas Robinson. No obstante, si una persona después de darse de alta y transcurridos de tres a seis meses, continúa recibiendo publicidad, puede dirigirse a la Agencia Española de Protección de Datos denunciando este hecho. En este caso la Agencia podrá abrir una investigación para averiguar lo que ha pasado y una vez conocidos los hechos iniciar un expediente o si esto no fuera oportuno archivar el caso.

Si la Agencia constata que existen indicios de que se ha producido una infracción deberá resolver el asunto en seis meses. La sanción económica depende de la infracción y las multas oscilan de 600 a 600.000 euros, según la gravedad.

El sistema de listas Robinson es eficaz tanto para las empresas como para los consumidores y consta de dos ficheros informáticos:

- Lista Robinson que recoge los nombres y direcciones de todas aquellas personas que no desean recibir publicidad por correo. Estos datos, tratados confidencialmente, serán excluidos de los envíos directos que realicen las empresas adheridas al servicio.

- Lista de Preferencia que tiene la misión de potenciar los envíos publicitarios, dando prioridad a aquellos temas que el usuario designe de mayor interés. De este modo las empresas conocen los nombres y direcciones de las personas interesadas en recibir su publicidad ya que estas han manifestado los temas concretos sobre los que están interesados (moda, deporte, turismo, hogar, etc.)

Para la empresa el coste de este servicio depende. Si están asociados a FECEMD el hecho de ser miembro de esta federación supone la adhesión automática y gratuita, en cambio, si no están asociadas deberán pagar una cuota anual (de unos 453,71 euros) en concepto de contribución a los gastos de mantenimiento.

Para el consumidor la inscripción es totalmente gratuita, recordemos el redactado del art 22 de la LSSI, modificado tras la aprobación de la nueva Ley general de Telecomunicaciones:

"El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente. A tal efecto, **los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado".**

Cualquier persona que quiera borrar definitivamente sus datos publicitarios tan sólo deberá marcar un número de teléfono, el 93 240 27 07 y a los diez días recibirá gratuitamente en su casa un cupón que deberá cumplimentar con su nombre y direcciones en las que no desea recibir publicidad. También es

posible rellenar el cupón de la página de web de la Federación de Empresas de Comercio Electrónico y Mrketing Directo (www.fecemd.org).

Cada tres meses se borran los datos de estas personas de los listados y en un plazo de seis meses quienes lo han solicitado deben dejar de recibir envíos publicitarios.

Ahora bien, las listas Robinson no eliminan el buzoneo de impresos sin dirección, revistas gratuitas y, en general, la publicidad de empresas no adheridas a estos servicios.

7. El fichero Histórico de Seguros de Automóviles

La Ley 30/1995 de Ordenación y Supervisión de los Seguros Privados establece en su art. 24 que:

"las entidades aseguradoras podrán establecer ficheros comunes que contengan de datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y la selección de riesgos y la elaboración de estudios de técnica aseguradora …"

Este artículo es el fundamento del Fichero histórico de vehículos, también llamado SINCO, el contenido del cual está de acuerdo con la Ley Orgánica 15/1999 de Protección de Datos de carácter Personal, especialmente en todo lo previsto en cuanto a garantizar los derechos de las personas cuyos datos son tratados por dicho fichero.

La finalidad del SINCO es precisamente la descrita en la Ley 30/1995 de ahí que los datos de las pólizas y de los siniestros vinculados a ésta, se encuentren en un fichero común. El objetivo es facilitar a las compañías el acceso a esta información, que en todo caso será fidedigna, en el momento de suscribir un nuevo seguro para el automóvil. Estos datos no pueden utilizarse en ningún caso con otros fines, como publicidad o acciones de marketing y quedan siempre bajo la protección de los principios y derechos que reconoce la LOPD.

El responsable de este fichero es UNESPA (Unión Española de Entidades Aseguradoras) como Asociación de empresas de seguros que operan en el mercado español y TIREA (Tecnologías de la Información y Redes para las Entidades Aseguradoras), la responsable de su tratamiento. (TIREA es una empresa que ofrece servicios informáticos a las compañías aseguradoras). En esta calidad, TIREA se encarga del tratamiento de los datos aportados por las Aseguradoras al SINCO, así como de atender a las personas que quieran ejercer sus derechos de acceso, rectificación, cancelación u oposición.

Podrán adherirse al Fichero todas las entidades aseguradoras autorizadas para operar en España en el ramo de la responsabilidad civil de automóviles, teniendo como único requisito el estar inscritas en el Registro Especial de la Dirección General de Seguros. Asimismo las entidades podrán darse de baja en el Convenio mediante notificación por escrito de su voluntad con un mínimo de dos meses de antelación respecto a la fecha en que se desea causar la baja. En este caso se eliminaran del fichero todos los datos que hubiera aportado y se comunicará a la Agencia Española de Protección de Datos.
El funcionamiento del Fichero Histórico de Seguros de Automóviles se inició en noviembre del año 2000, después de un largo proceso de diseño y desarrollo en el que ha tenido un papel fundamental la Comisión Técnica de seguros de Automóviles.

La adscripción de las entidades aseguradoras al Fichero no se ha realizado en un mismo momento, si no que van adhiriéndose al fichero de forma

escalonada, esto es porque para una compañía aseguradora la adaptación de su sistema informático para hacer posibles las consultas al fichero y el conocimiento de los resultados, así como la descarga de sus datos en el mismo, suponen un gran esfuerzo a nivel humano y de medios y también un elevado coste económico, hay que remarcar que cada entidad debe satisfacer a Tirea en retribución de los servicios de puesta en funcionamiento, gestión y mantenimiento del fichero, una cuota de adhesión al servicio, cuotas periódicas de mantenimiento y de cartera y una cuota variable para las consultas al fichero que excedan del número a que da derecho la cuota de cartera.

La operativa de adhesión establecida señala que cada entidad comenzará a cargar en el fichero cada mes los datos relativos a su cartera renovada o realizada en el curso del mes anterior. Lo que supone que aún partiendo de una cartera de pólizas de automóvil más o menos homogénea (dicho de otro modo, sin estacionalidad) en la contratación o en la renovación, es fácil entender que una compañía necesitará como mínimo doce meses desde el inicio de su carga hasta que termine de descargar toda la cartera. De ahí que desde la adhesión hasta que una compañía pueda trabajar con el fichero deba mediar un plazo que puede estimarse entre doce y dieciocho meses ya que hasta que no tengan terminado el proceso de descarga de sus datos el fichero no será plenamente operativo.

Todo el funcionamiento del Fichero Histórico de Seguros de Automóviles se rige por el código tipo que ha sido aprobado por la Agencia Española de Protección de datos y que es de obligado cumplimiento para las entidades adheridas al fichero. Se ha aprobado con duración indefinida aunque por el propio desarrollo del Fichero o por necesidades legales podrá ser modificado. Todos los cambios deberán ser elaborados y propuestos por la comisión de control, para su aprobación por la Agencia y posteriormente será comunicado a todos los intervinientes.

La cesión de los datos al fichero no requiere autorización de los interesados pero sí deben ser informados como indica el art. 24 de la Ley de Ordenación y Supervisión de los Seguros Privados:

"…la cesión de datos a los citados ficheros no requerirá el consentimiento previo de afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley"

En el código- tipo se da cumplimiento a lo mencionado en el citado artículo cuando, en su punto 7.3, exige a las compañías que cumplan con la Ley 30/1995 y previamente a ceder los datos a los ficheros comunes informen a los afectados de la intención de ceder sus datos, de la existencia del fichero y de su finalidad. Asimismo para que puedan ejercer sus derechos de oposición, acceso, rectificación y cancelación deberá indicárseles quién es el responsable del fichero y el procedimiento a seguir en el ejercicio de dichos derechos. En los anexos se encuentra la cláusula modelo de información que se incluye en el Código-Tipo.

Pero veamos ahora que datos pueden ser cedidos al SINCO. Como hemos adelantado su objetivo es permitir a las compañías personalizar la prima en función de cada riesgo asegurado y la aplicación de criterios tarifarios equitativos, para que esto pueda llevarse a cabo es necesario contar con información, es decir, contar con el historial de siniestralidad de quienes contratan los seguros de modo que sea posible deducir su comportamiento. El fichero lo que permite es complementar la información que facilita el Tomador en el momento de contratar. Para ello, se cederán los datos relativos a los contratos así como el historial de siniestros de cada tomador de seguro de automóviles durante los últimos cinco años. Evidentemente la información debe ser veraz y por eso el código tipo responsabiliza a cada entidad cedente sobre la veracidad de los datos e informaciones que facilita al fichero, igualmente será responsable de la confidencialidad y del buen uso que realice de dicha información, es importante destacar que a la información que describiremos a continuación únicamente podrán tener acceso personas vinculadas laboralmente con la entidad, es decir, no se podrá autorizar a agentes o corredores a que accedan directamente al SINCO sino que cualquier consulta deberán realizarla a través de la entidad aseguradora. El fichero contendrá los siguientes datos:

- Vehículo asegurado

- Datos del Tomador: nombre y apellidos o razón social, DNI, NIF, Pasaporte o Tarjeta de residencia del tomador del seguro.

- Datos del contrato: coberturas que se incluyen dentro del grupo de ramos denominado “seguro del automóvil” así como las coberturas recogidas en los ramos “Asistencia” y “Defensa Jurídica”. Periodo de vigencia del contrato.

- Datos del Siniestro: Cobertura afectada por cada siniestro, fecha, existencia de daños materiales o corporales, importe del siniestro (en los supuestos en que el siniestro esté pendiente de liquidación o pago el campo relativo a importe quedaré en blanco). A estos efectos se entienden por siniestros computables todos aquellos que registren un concepto de cargo a la garantía de Responsabilidad Civil de Automóviles de tipo indemnizatorio. En los siniestros tramitados por el sistema de Convenios de Indemnización Directa, no serán computables todos aquellos que la entidad aseguradora haya terminado desde una posición acreedora.

Evidentemente la información debe estar siempre actualizada o de poco serviría por lo que las entidades deberán comunicar al SINCO cualquier tipo de modificación posterior a la cesión de la misma.

Para poder acceder a esta información, la entidad que recibe una solicitud de aseguramiento, deberá identificarse correctamente informando al sistema mediante las claves necesarias que serán: los últimos cinco dígitos de la póliza en vigor y al menos uno de los siguientes datos: nombre y apellidos del Tomador, número de documento identificativo, matrícula del vehículo.

Se trata de datos que sería difícil reunir sin la connivencia del asegurado. La regulación de la confidencialidad de los datos es muy importante y, aunque figure en el fichero, el Tomador es el único propietario de la información de ahí que para realizar una consulta se obligue a la entidad a seguir estas normas de seguridad y autentificación.

Por otro lado como responsables del uso del fichero, las entidades aseguradoras están obligadas a establecer sistemas internos de control que eviten un uso indebido, además para garantizar la confidencialidad de los datos de los afectados la información que contiene el fichero no podrá ser grabada, imprimida o copiada y únicamente podrá guardarse cuando el contrato quede formalizado ya que en ese caso formará parte de la proposición de seguro.

Como hemos dicho, el Tomador del seguro es el único propietario de la información incluida en el fichero por eso al ser el derecho de acceso a la información un derecho personalísimo sólo puede ser ejercido por él, esto es, por el titular de los datos o en su caso por su representante legal.

Para poder ejercer dicho derecho de acceso y conocer los datos que sobre su persona están registrados en el fichero, el titular deberá dirigirse por escrito a TIREA, responsable del tratamiento. En el escrito deberá figurar su nombre y apellidos o razón social en caso de ser una empresa, DNI, CIF O NIF, domicilio al que remitir la consulta y fotocopia de algún documento acreditativo de la personalidad.

Por teléfono no podrá facilitarse ninguna información sobre los datos del fichero ya que este medio no permite comprobar ni asegurar que la persona que está hablando o solicitando la información es el titular de los datos por eso para garantizar la seguridad e intimidad respecto a los mismos solo se aceptarán las solicitudes dirigidas a TIREA realizadas por escrito o personalmente. Tirea comunicará su resolución en un plazo máximo de treinta días naturales contados desde la recepción de la solicitud y lo hará siempre por correo certificado para garantizar la confidencialidad y seguridad de los datos.

Ejercido el derecho de acceso el interesado podrá ejercitar los derechos de rectificación, cancelación u oposición, indicando en su solicitud los datos que considera incorrectos o inexactos y que por tanto desea que sean modificados o cancelados. En el caso que ejercite el derecho de oposición deberá argumentar porqué considera que sus datos no deben ser objeto de tratamiento automatizado.

De todo lo dicho anteriormente se desprende que el Fichero Histórico de Seguros de Automóviles no es una lista de conductores con alta siniestralidad, ya que en él figuran todos los Tomadores de pólizas de auto de una entidad con independencia del número de siniestros y no es, tampoco, un fichero contra el fraude, aunque en este punto debemos indicar que la LOSSP en su art 24 sí autoriza a las entidades aseguradoras para establecer ficheros comunes cuya finalidad sea prevenir el fraude, pero la finalidad del SINCO no

es localizar casos de este tipo si no que su función es construir unos precios que distribuyan los costes de acuerdo con los riesgos a que cada asegurado está expuesto y que estos sean suficientes y no valoren el riesgo por debajo de su nivel esperable, en realidad se trata de dos obligaciones legales que las entidades aseguradoras deben cumplir, de acuerdo con el art. 24.3 de la Ley de Ordenación y Supervisión de Seguros Privados cuando dice que:

"las tarifas de primas deberán ser suficientes, según hipótesis actuariales razonables, para permitir a la entidad aseguradora satisfacer el conjunto de las obligaciones derivadas de los contratos de seguro y, en particular, constituir las provisiones técnicas adecuadas …".

La utilidad del SINCO ha quedado sobradamente demostrada a lo largo de la exposición sin embargo, bajo mi punto de vista, el fichero no está exento de críticas. El seguro de responsabilidad civil de automóvil trata de proteger a los ciudadanos frente a los daños causados como consecuencia de hechos derivados de la circulación de vehículos a motor, esto es, según el art. 3 del RD 7/2001, de 12 de enero por el que se aprueba el Reglamento sobre la responsabilidad civil y seguro en la circulación de vehículos a motor:

"los derivados del riesgo creado por la conducción de los vehículos a motor…"

Es decir, es de la conducción de un vehículo a motor de lo que deriva el riesgo y son los conductores los que producen los siniestros. El SINCO, sin embargo, no tiene en cuenta el historial de siniestralidad del conductor sino el de los últimos cinco años del Tomador, de modo que la información que se recibe de la consulta al fichero bien podría ser la de una persona, el Tomador, que ha contratado un seguro de auto pero que en realidad nunca ha conducido el vehículo o en el caso contrario, una persona que nunca contrató una póliza (por tanto nunca ha sido Tomador) pero que constaba en la misma como conductor habitual o como primer conductor. Al realizarse a SINCO la consulta por Tomador en su expediente de siniestralidad podrían aparecer cero siniestros cuando pudiera ser que esta persona sea un conductor desastroso con una alta siniestralidad. La prima de su nuevo seguro se calcularía partiendo de una información inexacta.

Este hecho no ha pasado inadvertido para las entidades aseguradoras, concretamente en el caso de Zurich la Dirección Técnica de Automóvil se ha encargado de realizar un estudio sobre su cartera concluyendo que, en el caso de las personas físicas, de cada diez pólizas analizadas en ocho de ellas la figura del tomador y del conductor coincide, lo que prácticamente eliminaría el problema planteado. Sin embargo, es algo diferente en el caso de las Personas Jurídicas donde como Tomador de la póliza aparece la empresa con su número de CIF, lo que hace que sea imposible que coincida con el nombre del conductor que debe ser necesariamente una persona física, pensemos como ejemplo en el caso de una empresa de renting.

8. La Agencia Española de Protección de Datos

La Agencia Española de Protección 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.

A partir del art 79 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la Agencia de Protección de Datos pasa a denominarse **Agencia Española de Protección de Datos** (en lo sucesivo AEPD) quedando modificada la Ley 15/1999 de Protección de Datos de Carácter Personal en el sentido que las referencias a la Agencia de Protección de Datos tanto en esta Ley como en las normas a las que se refiere su disposición transitoria tercera (normas reglamentarias y reales decretos) y cualquiera otras que se encuentren en vigor deberán entenderse realizadas a la Agencia Española de Protección de Datos.

Los órganos de la Agencia son el director, el consejo consultivo, el registro general de protección de datos, la inspección de datos y la secretaría general de la agencia:

- El Director; es nombrado por Real Decreto entre los miembros del consejo consultivo para un mandato de cuatro años y a propuesta del Ministro de Justicia, ostenta la representación de la AEPD por lo que sus actos se entienden como propios de ésta. Las resoluciones del director ponen fin a la vía administrativa y son recurribles ante la sala de lo contencioso de la Audiencia Nacional. En cuanto a sus funciones, hemos ido detallándolas a lo largo de la exposición. Actualmente este cargo lo ostenta D. José Luis Piñar Mañas.
- El consejo consultivo; es un órgano colegiado de asesoramiento del director y emite informes en los temas que el director se lo solicite, Se reúne al menos una vez cada seis meses. También se encarga de formular las propuestas en materia de protección de datos.
- La inspección de datos; Se encarga de comprobar la legalidad de los tratamientos de datos. Tiene funciones instructoras y de tutela de los derechos.
- El registro general de protección de datos; Vela por la publicidad de los tratamientos de datos.
- La secretaria general de la agencia; se encarga de dar apoyo al desarrollo de la actividad de la agencia.

En cuanto a las funciones de las AEPD, he considerado muy adecuado reproducir aquí la clasificación que de las mismas ha hecho la propia agencia, la cual distribuye las funciones en función de la materia o personas a quienes afecta. A lo largo de la exposición ya hemos hecho referencia en varias ocasiones a estas funciones, que ahora quedan agrupadas de la siguiente manera:

1. General: velará por el cumplimiento de la legislación sobre protección de datos y controlará su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
2. En relación a los afectados: Atenderá sus peticiones y reclamaciones, informará sobre los derechos reconocidos en la Ley y promoverá las campañas de difusión a través de los medios.
3. En relación a quienes tratan los datos: Emite las autorizaciones previstas en la Ley, requiere medidas de corrección y ordena, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos. Asimismo le corresponde ejercer la potestad sancionadora, recabar la ayuda e información que precise y autorizar las transferencias internacionales de datos.
4. En la elaboración de normas: Informa los proyectos de normas de desarrollo de la LOPD así como de aquellas normas que incidan en materias de protección de datos. Dicta instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD y recomendaciones en caso de materias de seguridad y control de acceso a los ficheros.
5. En materia de Telecomunicaciones: Se encarga de la tutela de los derechos y garantías de los abonados y usuarios en el ámbito de las telecomunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas cuando se realizan a través de correo electrónico o medios de comunicación electrónica equivalentes.
6. Otras funciones: Vela por la publicidad de las tratamientos, publicando anualmente una lista de los mismos. Se encarga de representar a España en los foros internacionales sobre protección de datos y de la cooperación internacional (participa, con carácter de autoridad independiente, en todos los grupos de trabajo, comités y autoridades centrales de control en materia de protección de datos de la Unión Europea, tanto en los aspectos relativos al desarrollo efectivo del mercado único europeo, como en lo que afecta a la cooperación policial y judicial. También participa en los comités ad hoc del Consejo de Europa, en las Conferencias Internacionales y sus grupos de trabajo y, finalmente, de forma bilateral mediante la cooperación con otras autoridades de control extranjeras.).También controla lo dispuesto en la Ley reguladora de la Función estadística pública y elabora una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.

La Ley 62/2003, que entró en vigor el 1 de enero de 2004, también modificó el art 37, añade su párrafo segundo, de la LOPD estableciendo que las resoluciones de la AEPD se harán públicas una vez se hayan notificado a los interesados:

"Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos. Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones. Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta Ley Orgánica".

A raíz de este precepto la AEPD habrá de publicar todas sus resoluciones que correspondan a procedimientos iniciados a partir del 1 de enero de 2004. A la

vez, la AEPD ha manifestado que también serán publicadas las resoluciones que consideren de especial relevancia en materia de protección de datos de carácter personal.

9. Conclusiones

El derecho a la libre disposición de los datos de carácter personal es un derecho fundamental y como tal cuenta con un grado de protección específica y superior al de otros derechos no fundamentales. Es muy importante en la sociedad en la que vivimos conocer el contenido de dicho derecho y ser consciente de los mecanismos de defensa de que disponemos frente a cualquier vulneración del mismo. A través de este estudio hemos visto cual son esos principios y derechos y de que manera podemos ejercerlos.

Hablar de protección de datos centrándonos exclusivamente en la LO 15/1999 era insuficiente por ello se ha hecho un repaso a la normativa comunitaria sobre el tema así como a otras normas nacionales que adaptan las directivas comunitarias en materia de protección de datos y que tienen una gran incidencia en la regulación de la sociedad de la información como son la Ley General de Telecomunicaciones y la Ley de servicios de la Sociedad de la Información y de comercio electrónico.

En materia de seguridad se ha desarrollado el RD 994/1999 de 11 de Junio por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, viendo los niveles de seguridad que deben adoptar las entidades con respecto a los datos que almacenan.

Se ha hecho referencia de manera más concreta a ficheros como el Sinco o las listas de morosos, estos son solo un ejemplo de los miles de ficheros existentes en los que pueden estar registrados datos sobre nuestra personalidad o nuestras características físicas. La capacidad de almacenamiento de datos de los soportes informáticos es inmensa pero afortunadamente los instrumentos para poder defendernos frente a los usos fraudulentos que puedan hacerse de los mismos están creados.

Las empresas juegan un papel relevante en todo este contexto en cuanto responsables de muchos de estos ficheros por lo que es imprescindible que adopten sus estructuras a las exigencias de la Ley. Hemos visto las medidas técnicas y organizativas que están obligadas a adoptar así como el régimen de sanciones al que se somete el incumplimiento de la normativa.

Por último, y aunque era inevitable ir nombrándola a lo largo de toda la exposición, se dedica un capítulo a la Agencia Española de Protección de Datos por las importantes funciones que asume en materia de Protección de Datos.

En definitiva se ha intentado repasar el marco normativo aplicable al tratamiento de los datos personales buscando su enfoque práctico, su incidencia en el desarrollo de la sociedad en general y en la privacidad de los individuos en particular.

10. Bibliografía

Páginas web consultadas:

www.agdp.es
www.europa.eu.int
www.tirea.es
www.mir.es

- Manual Práctico. Protección de Datos de Carácter Personal. 2003. Editorial Derecho.com

- Legislación sobre datos de carácter personal. 2003. Editorial Tecnos.

- Derecho Comunitario y de la Unión Europea. 2002. Paolo Mengozzi. Editorial Tecnos.

ANEXOS

Como complemento a la exposición se indican los siguientes documentos:

A - Derecho de acceso:

https://www.agpd.es/upload/mod_a_derecho_acceso.pdf

A.1 Hoja de solicitud para ejercicio del derecho de acceso.
A.2 Hoja de solicitud de reclamación de tutela por denegación del derecho de acceso.
A.3 Instrucciones para la cumplimentación de los documentos anteriores.

B - Derecho de rectificación

https://www.agpd.es/upload/mod_b_derecho_rectificacion.pdf

B.1 Hoja de solicitud para ejercicio del derecho de rectificación.
B.2 Hoja de solicitud de reclamación de tutela por denegación del derecho de rectificación.
B.3 Instrucciones para la cumplimentación de los documentos anteriores.

C - Derecho de cancelación

https://www.agpd.es/upload/mod_c_derecho_cancelacion.pdf

C.1 Hoja de solicitud para ejercicio del derecho de cancelación.
C.2 Hoja de solicitud de reclamación de tutela por denegación del derecho de cancelación.
C.3 Instrucciones para la cumplimentación de los documentos anteriores.

D - Derecho de Exclusión

https://www.agpd.es/upload/mod_d_derecho_exclusion.pdf

D.1 Hoja de solicitud para ejercicio del derecho de exclusión.
D.2 Hoja de solicitud de reclamación de tutela por denegación del derecho de exclusión.
D.3 Instrucciones para la cumplimentación de los documentos anteriores.

E - Denuncia ante la Agencia de Protección de Datos

https://www.agpd.es/upload/mod_e_denuncia.pdf

F - Modelo de comunicación de la entidad Aseguradora al Tomador respecto a la cesión de datos al SINCO:

En virtud de la autorización que concede la ley 30/1995, Unión Española de Entidades Aseguradoras y reaseguradoras (UNESPA) ha creado el Fichero Histórico de Seguros de

Automóviles para la tarificación y selección de riesgos, constituido con la información aportada por las Entidades Aseguradoras.

Le comunicamos que los datos sobre su contrato de seguro del automóvil y los siniestros vinculados a éste, de los últimos cinco años, si los hubiere, serán cedidos al citado fichero común.

Si desea ejercitar los derechos de acceso, rectificación, cancelación y oposición puede dirigirse a TIREA, c/García de Paredes, nº 55, 28010 Madrid, debiéndose identificar mediante DNI., Pasaporte o Tarjeta de Residencia.

Sonia Plaza López

Licenciada en Derecho en el año 2000 por la Universidad de Barcelona ha desarrollado la gran parte de su carrera profesional en ZURICH ESPAÑA.

Actualmente forma parte del equipo de la Asesoría Jurídica de dicha entidad.

COLECCIÓN "CUADERNOS DE DIRECCIÓN ASEGURADORA"

Master en Dirección de Entidades Aseguradoras y Financieras
Facultad de Economía y Empresa. Universidad de Barcelona

PUBLICACIONES

1.- Francisco Abián Rodríguez: "Modelo Global de un Servicio de Prestaciones Vida y su interrelación con Suscripción" 2005/2006

2.- Erika Johanna Aguilar Olaya: "Gobierno Corporativo en las Mutualidades de Seguros" 2005/2006

3.- Alex Aguyé Casademunt: "La Entidad Multicanal. Elementos clave para la implantación de la Estrategia Multicanal en una entidad aseguradora" 2009/2010

4.- José María Alonso-Rodríguez Piedra: "Creación de una plataforma de servicios de siniestros orientada al cliente" 2007/2008

5.- Jorge Alvez Jiménez: "innovación y excelencia en retención de clientes" 2009/2010

6.- Anna Aragonés Palom: "El Cuadro de Mando Integral en el Entorno de los seguros Multirriesgo" 2008/2009

7.- Maribel Avila Ostos: "La tele-suscripción de Riesgos en los Seguros de Vida" 2009/20010

8.- Mercé Bascompte Riquelme: "El Seguro de Hogar en España. Análisis y tendencias" 2005/2006

9.- Aurelio Beltrán Cortés: "Bancaseguros. Canal Estratégico de crecimiento del sector asegurador" 2010/2011

10.- Manuel Blanco Alpuente:"Delimitación temporal de cobertura en el seguro de responsabilidad civil. Las cláusulas claims made" 2008/2009

11.- Eduard Blanxart Raventós: "El Gobierno Corporativo y el Seguro D & O" 2004/2005

12.- Rubén Bouso López: "El Sector Industrial en España y su respuesta aseguradora: el Multirriesgo Industrial. Protección de la empresa frente a las grandes pérdidas patrimoniales"2006/2007

13.- Kevin van den Boom:"El Mercado Reasegurador (Cedentes, Brokers y Reaseguradores). Nuevas Tendencias y Retos Futuros" 2008/2009

14.- Laia Bruno Sazatornil: "L'ètica i la rentabilitat en les companyies asseguradores. Proposta de codi deontològic" 2004/2005

15.- María Dolores Caldés LLopis: "Centro Integral de Operaciones Vida" 2007/2008

16.- Adolfo Calvo Llorca: "Instrumentos legales para el recobro en el marco del seguro de crédito" 2010/2011

17.- Ferran Camprubí Baiges: "La gestión de las inversiones en las entidades aseguradoras. Selección de inversiones" 2010/2011

18.- Joan Antoni Carbonell Aregall: "La Gestió Internacional de Sinistres d'Automòbil amb Resultat de Danys Materials" 2003-2004

19.- Susana Carmona Llevadot: "Viabilidad de la creación de un sistema de Obra Social en una entidad aseguradora" 2007/2008

20.- Sergi Casas del Alcazar: "El PLan de Contingencias en la Empresa de Seguros" 2010/2011

21.- Francisco Javier Cortés Martínez: "Análisis Global del Seguro de Decesos" 2003-2004

22.- María Carmen Ceña Nogué:"El Seguro de Comunidades y su Gestión" 2009/2010

23.- Jordi Cots Paltor: "Control Interno. El auto-control en los Centros de Siniestros de Automóviles" 2007/2008

24.- Montserrat Cunillé Salgado: “Los riesgos operacionales en las Entidades Aseguradoras” 2003-2004

25.- Ricard Doménech Pagés: “La realidad 2.0. La percepción del cliente, más importante que nunca” 2010/2011

26.- Luis Domínguez Martínez: “Formas alternativas para la Cobertura de Riesgos” 2003-2004

27.- Marta Escudero Cutal: “Solvencia II. Aplicación práctica en una entidad de Vida” 2007/2008

28.- Salvador Esteve Casablancas: “La Dirección de Reaseguro. Manual de Reaseguro” 2005/2006

29.- Alvaro de Falguera Gaminde: “Plan Estratégico de una Correduría de Seguros Náuticos” 2004/2005

30.- Isabel Mª Fernández García: “Nuevos aires para las Rentas Vitalicias” 2006/2007

31.- Eduard Fillet Catarina: “Contratación y Gestión de un Programa Internacional de Seguros” 2009/2010

32.- Pablo Follana Murcia: “Métodos de Valoración de una Compañía de Seguros. Modelos Financieros de Proyección y Valoración consistentes” 2004/2005

33.- Juan Fuentes Jassé: “El fraude en el seguro del Automóvil” 2007/2008

34.- Xavier Gabarró Navarro: “"El Seguro de Protección Jurídica. Una oportunidad de Negocio"” 2009/2010

35.- Josep María Galcerá Gombau: “La Responsabilidad Civil del Automóvil y el Daño Corporal. La gestión de siniestros. Adaptación a los cambios legislativos y propuestas de futuro” 2003-2004

36.- Luisa García Martínez: “El Carácter tuitivo de la LCS y los sistemas de Defensa del Asegurado. Perspectiva de un Operador de Banca Seguros” 2006/2007

37.- Fernando García Giralt: “Control de Gestión en las Entidades Aseguradoras” 2006/2007

38.- Jordi García-Muret Ubis: “Dirección de la Sucursal. D. A. F. O.” 2006/2007

39.- David Giménez Rodríguez: “El seguro de Crédito: Evolución y sus Canales de Distribución” 2008/2009

40.- Juan Antonio González Arriete: “Línea de Descuento Asegurada” 2007/2008

41.- Miquel Gotés Grau: “Assegurances Agràries a BancaSeguros. Potencial i Sistema de Comercialització” 2010/2011

42.- Jesús Gracia León: “Los Centros de Siniestros de Seguros Generales. De Centros Operativos a Centros Resolutivos. De la optimización de recursos a la calidad de servicio” 2006/2007

43.- José Antonio Guerra Díez: “Creación de unas Tablas de Mortalidad Dinámicas” 2007/2008

44.- Santiago Guerrero Caballero: “La politización de las pensiones en España” 2010/2011

45.- Francisco J. Herencia Conde: “El Seguro de Dependencia. Estudio comparativo a nivel internacional y posibilidades de desarrollo en España” 2006/2007

46.- Francisco Javier Herrera Ruiz:“Selección de riesgos en el seguro de Salud” 2009/2010

47.- Alicia Hoya Hernández:“Impacto del cambio climático en el reaseguro” 2008/2009

48.- Jordi Jiménez Baena: “Creación de una Red de Agentes Exclusivos” 2007/2008

49.- Oriol Jorba Cartoixà:“La oportunidad aseguradora en el sector de las energías renovables” 2008/2009

50.- Anna Juncá Puig: “Una nueva metodología de fidelización en el sector asegurador” 2003/2004

51.- Ignacio Lacalle Goría: “El artículo 38 Ley Contrato de Seguro en la Gestión de Siniestros. El procedimiento de peritos” 2004/2005

52.- Mª Carmen Lara Ortíz: “Solvencia II. Riesgo de ALM en Vida” 2003/2004

53.- Haydée Noemí Lara Téllez: “El nuevo sistema de Pensiones en México” 2004/2005

54.- Marta Leiva Costa: “La reforma de pensiones públicas y el impacto que esta modificación supone en la previsión social” 2010/2011

55.- Victoria León Rodríguez: “Problemàtica del aseguramiento de los Jóvenes en la política comercial de las aseguradoras” 2010/2011

56.- Pilar Lindín Soriano: “Gestión eficiente de pólizas colectivas de vida” 2003/2004

57.- Victor Lombardero Guarner: “La Dirección Económico Financiera en el Sector Asegurador” 2010/2011

58.- Maite López Aladros: “Análisis de los Comercios en España. Composición, Evolución y Oportunidades de negocio para el mercado asegurador” 2008/2009

59.- Josep March Arranz: “Los Riesgos Personales de Autónomos y Trabajadores por cuenta propia. Una visión de la oferta aseguradora” 2005/2006

60.- Miquel Maresch Camprubí: “Necesidades de organización en las estructuras de distribución por mediadores” 2010/2011

61.- José Luis Marín de Alcaraz: “El seguro de impago de alquiler de viviendas” 2007/2008

62.- Miguel Ángel Martínez Boix: “Creatividad, innovación y tecnología en la empresa de seguros” 2005/2006

63.- Susana Martínez Corveira: “Propuesta de Reforma del Baremo de Autos” 2009/2010

64.- Inmaculada Martínez Lozano: “La Tributación en el mundo del seguro” 2008/2009

65.- Dolors Melero Montero: “Distribución en bancaseguros: Actuación en productos de empresas y gerencia de riesgos" 2008/2009

66.- Josep Mena Font: “La Internalización de la Empresa Española” 2009/2010

67.- Angela Milla Molina: “La Gestión de la Previsión Social Complementaria en las Compañías de Seguros. Hacia un nuevo modelo de Gestión” 2004/2005

68.- Montserrat Montull Rossón: “Control de entidades aseguradoras” 2004/2005

69.- Eugenio Morales González: “Oferta de licuación de patrimonio inmobiliario en España” 2007/2008

70.- Lluis Morales Navarro: “Plan de Marketing. División de Bancaseguros” 2003/2004

71.- Sonia Moya Fernández: “Creación de un seguro de vida. El éxito de su diseño” 2006/2007

72.- Rocio Moya Morón: “Creación y desarrollo de nuevos Modelos de Facturación Electrónica en el Seguro de Salud y ampliación de los modelos existentes” 2008/2009

73.- María Eugenia Muguerza Goya: “Bancaseguros. La comercialización de Productos de Seguros No Vida a través de redes bancarias” 2005/2006

74.- Ana Isabel Mullor Cabo: “Impacto del Envejecimiento en el Seguro” 2003/2004

75.- Estefanía Nicolás Ramos: “Programas Multinacionales de Seguros” 2003/2004

76.- Santiago de la Nogal Mesa: “Control interno en las Entidades Aseguradoras” 2005/2006

77.- Antonio Nolasco Gutiérrez: “Venta Cruzada. Mediación de Seguros de Riesgo en la Entidad Financiera” 2006/2007

78.- Francesc Ocaña Herrera: “Bonus-Malus en seguros de asistencia sanitaria” 2006/2007

79.- Antonio Olmos Francino: “El Cuadro de Mando Integral: Perspectiva Presente y Futura” 2004/2005

80.- Luis Palacios García: “El Contrato de Prestación de Servicios Logísticos y la Gerencia de Riesgos en Operadores Logísticos” 2004/2005

81.- Jaume Paris Martínez: “Segmento Discapacitados. Una oportunidad de Negocio” 2009/2010

82.- Martín Pascual San Martín: “El incremento de la Longevidad y sus efectos colaterales” 2004/2005

83.- Montserrat Pascual Villacampa: “Proceso de Tarificación en el Seguro del Automóvil. Una perspectiva técnica” 2005/2006

84.- Marco Antonio Payo Aguirre: “La Gerencia de Riesgos. Las Compañías Cautivas como alternativa y tendencia en el Risk Management” 2006/2007

85.- Patricia Pérez Julián: “Impacto de las nuevas tecnologías en el sector asegurador” 2008/2009

86.- María Felicidad Pérez Soro: “La atención telefónica como transmisora de imagen” 2009/2010

87.- Marco José Piccirillo: “Ley de Ordenación de la Edificación y Seguro. Garantía Decenal de Daños” 2006/2007

88.- Irene Plana Güell: “Sistemas d’Informació Geogràfica en el Sector Assegurador” 2010/2011

89.- Sonia Plaza López: “La Ley 15/1999 de Protección de Datos de carácter personal” 2003/2004

90.- Pere Pons Pena: “Identificación de Oportunidades comerciales en la Provincia de Tarragona” 2007/2008

91.- María Luisa Postigo Díaz: “La Responsabilidad Civil Empresarial por accidentes del trabajo. La Prevención de Riesgos Laborales, una asignatura pendiente” 2006/2007

92.- Jordi Pozo Tamarit: “Gerencia de Riesgos de Terminales Marítimas” 2003/2004

93.- Francesc Pujol Niñerola: “La Gerencia de Riesgos en los grupos multisectoriales” 2003-2004

94.- Mª del Carmen Puyol Rodríguez: “Recursos Humanos. Breve mirada en el sector de Seguros” 2003/2004

95.- Antonio Miguel Reina Vidal: “Sistema de Control Interno, Compañía de Vida. Bancaseguros” 2006/2007

96.- Marta Rodríguez Carreiras: “Internet en el Sector Asegurador” 2003/2004

97.- Juan Carlos Rodríguez García: “Seguro de Asistencia Sanitaria. Análisis del proceso de tramitación de Actos Médicos” 2004/2005

98.- Mónica Rodríguez Nogueiras: “La Cobertura de Riesgos Catastróficos en el Mundo y soluciones alternativas en el sector asegurador” 2005/2006

99.- Susana Roquet Palma: “Fusiones y Adquisiciones. La integración y su impacto cultural” 2008/2009

100.- Santiago Rovira Obradors: “El Servei d’Assegurances. Identificació de les variables clau” 2007/2008

101.- Carlos Ruano Espí: “Microseguro. Una oportunidad para todos” 2008/2009

102.- Mireia Rubio Cantisano: “El Comercio Electrónico en el sector asegurador” 2009/2010

103.- María Elena Ruíz Rodríguez: “Análisis del sistema español de Pensiones. Evolución hacia un modelo europeo de Pensiones único y viabilidad del mismo” 2005/2006

104.- Eduardo Ruiz-Cuevas García: “Fases y etapas en el desarrollo de un nuevo producto. El Taller de Productos” 2006/2007

105.- Pablo Martín Sáenz de la Pascua: “Solvencia II y Modelos de Solvencia en Latinoamérica. Sistemas de Seguros de Chile, México y Perú” 2005/2006

106.- Carlos Sala Farré: “Distribución de seguros. Pasado, presente y tendencias de futuro” 2008/2009

107.- Ana Isabel Salguero Matarín: “Quién es quién en el mundo del Plan de Pensiones de Empleo en España” 2006/2007

108.- Jorge Sánchez García: “El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras” 2006/2007

109.- María Angels Serral Floreta: “El lucro cesante derivado de los daños personales en un accidente de circulación” 2010/2011

110.- David Serrano Solano: “Metodología para planificar acciones comerciales mediante el análisis de su impacto en los resultados de una compañía aseguradora de No Vida” 2003/2004

111.- Jaume Siberta Durán: “Calidad. Obtención de la Normativa ISO 9000 en un centro de Atención Telefónica” 2003/2004

112.- María Jesús Suárez González: “Los Poolings Multinacionales” 2005/2006

113.- Miguel Torres Juan: “Los siniestros IBNR y el Seguro de Responsabilidad Civil” 2004/2005

114.- Carlos Travé Babiano: “Provisiones Técnicas en Solvencia II. Valoración de las provisiones de siniestros” 2010/2011

115.- Rosa Viciana García: “Banca-Seguros. Evolución, regulación y nuevos retos” 2007/2008

116.- Ramón Vidal Escobosa: “El baremo de Daños Personales en el Seguro de Automóviles” 2009/2010

117.- Tomás Wong-Kit Ching: “Análisis del Reaseguro como mitigador del capital de riesgo” 2008/2009

118.- Yibo Xiong: “Estudio del mercado chino de Seguros: La actualidad y la tendencia” 2005/2006

119.- Beatriz Bernal Callizo: “Póliza de Servicios Asistenciales” 2003/2004

120.- Marta Bové Badell: “Estudio comparativo de evaluación del Riesgo de Incendio en la Industria Química” 2003/2004

121.- Ernest Castellón Texidó: “La edificación. Fases del proceso, riesgos y seguros” 2004/2005

122.- Sandra Clusella Giménez: “Gestió d’Actius i Passius. Inmunització Financera” 2004/2005

123.- Miquel Crespí Argemí: “El Seguro de Todo Riesgo Construcción” 2005/2006

124.- Yolanda Dengra Martínez: “Modelos para la oferta de seguros de Hogar en una Caja de Ahorros” 2007/2008

125.- Marta Fernández Ayala: “El futuro del Seguro. Bancaseguros” 2003/2004

126.- Antonio Galí Isus: “Inclusión de las Energías Renovables en el sistema Eléctrico Español” 2009/2010

127.- Gloria Gorbea Bretones: “El control interno en una entidad aseguradora” 2006/2007

128.- Marta Jiménez Rubio: “El procedimiento de tramitación de siniestros de daños materiales de automóvil: análisis, ventajas y desventajas” 2008/2009

129.- Lorena Alejandra Libson: “Protección de las víctimas de los accidentes de circulación. Comparación entre el sistema español y el argentino” 2003/2004

130.- Mario Manzano Gómez: “La responsabilidad civil por productos defectuosos. Solución aseguradora” 2005/2006

131.- Àlvar Martín Botí: “El Ahorro Previsión en España y Europa. Retos y Oportunidades de Futuro” 2006/2007

132.- Sergio Martínez Olivé: “Construcción de un modelo de previsión de resultados en una Entidad Aseguradora de Seguros No Vida” 2003/2004

133.- Pilar Miracle Vázquez: “Alternativas de implementación de un Departamento de Gestión Global del Riesgo. Aplicado a empresas industriales de mediana dimensión” 2003/2004

134.- María José Morales Muñoz: “La Gestión de los Servicios de Asistencia en los Multirriesgo de Hogar” 2007/2008

135.- Juan Luis Moreno Pedroso: "El Seguro de Caución. Situación actual y perspectivas" 2003/2004

136.- Rosario Isabel Pastrana Gutiérrez: “Creació d'una empresa de serveis socials d'atenció a la dependència de les persones grans enfocada a productes d'assegurances” 2007/2008

137.- Joan Prat Rifá: "La Previsió Social Complementaria a l'Empresa" 2003/2004

138.- Alberto Sanz Moreno: “Beneficios del Seguro de Protección de Pagos” 2004/2005

139.- Judith Safont González: “Efectes de la contaminació i del estils de vida sobre les assegurances de salut i vida” 2009/2010

140.- Carles Soldevila Mejías: “Models de gestió en companyies d’assegurances. Outsourcing / Insourcing” 2005/2006

141.- Olga Torrente Pascual: “IFRS-19 Retribuciones post-empleo” 2003/2004

142.- Annabel Roig Navarro: “La importancia de las mutualidades de previsión social como complementarias al sistema publico” 2009/2010

143.- José Angel Ansón Tortosa: “Gerencia de Riesgos en la Empresa española” 2011/2012

144.- María Mecedes Bernués Burillo: “El permiso por puntos y su solución aseguradora” 2011/2012

145.- Sònia Beulas Boix: “Prevención del blanqueo de capitales en el seguro de vida” 2011/2012

146.- Ana Borràs Pons: “Teletrabajo y Recursos Humanos en el sector Asegurador” 2011/2012

147.- María Asunción Cabezas Bono: “La gestión del cliente en el sector de bancaseguros” 2011/2012

148.- María Carrasco Mora: “Matching Premium. New approach to calculate technical provisions Life insurance companies” 2011/2012

149.- Eduard Huguet Palouzie: “Las redes sociales en el Sector Asegurador. Plan social-media. El Community Manager” 2011/2012

150.- Laura Monedero Ramírez: “Tratamiento del Riesgo Operacional en los 3 pilares de Solvencia II” 2011/2012

151.- Salvador Obregón Gomá: “La Gestión de Intangibles en la Empresa de Seguros” 2011/2012

152.- Elisabet Ordóñez Somolinos: “El sistema de control Interno de la Información Financiera en las Entidades Cotizadas” 2011/2012

153.- Gemma Ortega Vidal: “La Mediación. Técnica de resolución de conflictos aplicada al Sector Asegurador” 2011/2012

154.- Miguel Ángel Pino García: “Seguro de Crédito: Implantación en una aseguradora multirramo” 2011/2012

155.- Genevieve Thibault: “The Costumer Experience as a Sorce of Competitive Advantage” 2011/2012

156.- Francesc Vidal Bueno: “La Mediación como método alternativo de gestión de conflictos y su aplicación en el ámbito asegurador” 2011/2012

157.- Mireia Arenas López: “El Fraude en los Seguros de Asistencia. Asistencia en Carretera, Viaje y Multirriesgo” 2012/2013

158.- Lluis Fernández Rabat: “El proyecto de contratos de Seguro-IFRS4. Expectativas y realidades” 2012/2013

159.- Josep Ferrer Arilla: “El seguro de decesos. Presente y tendencias de futuro” 2012/2013

160.- Alicia García Rodríguez: “El Cuadro de Mando Integral en el Ramo de Defensa Jurídica” 2012/2013

161.- David Jarque Solsona: “Nuevos sistemas de suscripción en el negocio de vida. Aplicación en el canal bancaseguros” 2012/2013

162.- Kamal Mustafá Gondolbeu: “Estrategias de Expansión en el Sector Asegurador. Matriz de Madurez del Mercado de Seguros Mundial” 2012/2013

163.- Jordi Núñez García: “Redes Periciales. Eficacia de la Red y Calidad en el Servicio” 2012/2013

164.- Paula Núñez García: “Benchmarking de Autoevaluación del Control en un Centro de Siniestros Diversos” 2012/2013

165.- Cristina Riera Asensio: “Agregadores. Nuevo modelo de negocio en el Sector Asegurador” 2012/2013

166.- Joan Carles Simón Robles: “Responsabilidad Social Empresarial. Propuesta para el canal de agentes y agencias de una compañía de seguros generalista” 2012/2013

167.- Marc Vilardebó Miró: “La política de inversión de las compañías aseguradoras ¿Influirá Solvencia II en la toma de decisiones?” 2012/2013

168.- Josep María Bertrán Aranés: “Segmentación de la oferta aseguradora para el sector agrícola en la provincia de Lleida” 2013/2014

169.- María Buendía Pérez: “Estrategia: Formulación, implementación, valoración y control” 2013/2014

170.- Gabriella Fernández Andrade: “Oportunidades de mejora en el mercado de seguros de Panamá” 2013/2014

171.- Alejandro Galcerán Rosal: “El Plan Estratégico de la Mediación: cómo una Entidad Aseguradora puede ayudar a un Mediador a implementar el PEM” 2013/2014

172.- Raquel Gómez Fernández: “La Previsión Social Complementaria: una apuesta de futuro” 2013/2014

173.- Xoan Jovaní Guiral: “Combinaciones de negocios en entidades aseguradoras: una aproximación práctica” 2013/2014

174.- Àlex Lansac Font: “Visión 360 de cliente: desarrollo, gestión y fidelización” 2013/2014

175.- Albert Llambrich Moreno: “Distribución: Evolución y retos de futuro: la evolución tecnológica” 2013/2014

176.- Montserrat Pastor Ventura: “Gestión de la Red de Mediadores en una Entidad Aseguradora. Presente y futuro de los agentes exclusivos” 2013/2014

177.- Javier Portalés Pau: “El impacto de Solvencia II en el área de TI” 2013/2014

178.- Jesús Rey Pulido: “El Seguro de Impago de Alquileres: Nuevas Tendencias” 2013/2014

179.- Anna Solé Serra: “Del cliente satisfecho al cliente entusiasmado. La experiencia cliente en los seguros de vida” 2013/2014

180.- Eva Tejedor Escorihuela: “Implantación de un Programa Internacional de Seguro por una compañía española sin sucursales o filiales propias en el extranjero. Caso práctico: Seguro de Daños Materiales y RC” 2013/2014