Instituto de Ciencias del Seguro

LA SEGURIDAD JURÍDICA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SECTOR ASEGURADOR

Isabel Álvarez-Rico

Carretera de Pozuelo 52
28220 Majadahonda. Madrid

www.fundacionmapfre.com/cienciasdelseguro
publicaciones.ics@mapfre.com

ISBN: 978-84-9844-102-4
Depósito Legal: SE-4712-2008

PRESENTACIÓN

Desde 1992 FUNDACIÓN MAPFRE realiza anualmente una convocatoria de becas destinadas a promover estudios monográficos en materia de Riesgo y Seguro, incluyendo áreas temáticas relacionadas específicamente con el seguro iberoamericano.

Su objetivo es facilitar apoyo económico para la realización de trabajos de investigación en las áreas antes mencionadas y están dirigidas a titulados universitarios y profesionales del mundo del seguro, de cualquier nacionalidad, que deseen desarrollar programas de investigación.

Para la realización de este trabajo, FUNDACIÓN MAPFRE concedió a su autora una Beca de Investigación Riesgo y Seguro en la convocatoria 2006/2007.

Isabel Álvarez-Rico es Doctora en Derecho y especialista en Derecho de Nuevas Tecnologías. Trabaja desde 1996 como profesora asociada en la Universidad Pontificia de Salamanca (Campus de Madrid) donde imparte la Asignatura de Derecho Informático en la Facultad y Escuela de Informática. Asimismo es profesora del Master de Ciencias de la Salud y del de Ingeniería del Software de la misma Universidad y colabora con MAPFRE en la Facultad de Ciencias del Seguro, Jurídicas y de la Empresa.

En la actualidad dirige también el área legal de la consultora EURADIA INTERNACIONAL, centrando su actividad en la formación y adaptación de las empresas a la normativa legal vigente en materia de protección de datos y comercio electrónico.

Dedicatoria

A mi padre, eterno profesor.
A mi marido, eterno sufridor de mis desvelos e incondicional soporte y
a mis hijos: Pablo, Rebeca y Sofía, mis eternas pasiones.

PRÓLOGO

Constituye un honor para nosotros haber participado de algún modo en este trabajo, aún desde la faceta de tutorizar el mismo. Como también es un honor que se nos haya dado la posibilidad de prologarlo. Cuestiones por las que damos las gracias a la autora, la Doctora Dª Isabel Álvarez-Rico y a FUNDACIÓN MAPFRE que lo acogió en el seno de sus proyectos de investigación.

Y decimos que es un honor para nosotros haber participado en este trabajo de investigación, porque se trata de un magnífico trabajo, sumamente interesante, que ha sido elaborado desde una perspectiva jurídica relevante, no exento de una notable aportación técnica y enfocado todo a la vertiente práctica.

La Doctora Isabel Álvarez-Rico inicia su trabajo desgranando la evolución de las tecnologías de la información en el sector asegurador, esbozando su uso creciente en el mismo y poniendo de manifiesto la extraordinaria perspectiva de crecimiento que redundará a su vez en una mejora del propio negocio. Y nos ha llamado la atención, la aún incipiente participación directa en el proceso de contratación y gestión del seguro de las nuevas tecnologías.

Como uno de los puntos fuertes del trabajo, ilustra al lector con un análisis pormenorizado y de elevado nivel técnico jurídico, de toda la normativa aplicable a las tecnologías de la información, centrándose como no podía ser de otra forma, en el sector asegurador. De especial interés para los lectores profesionales de estas materias que, además de por cualquier otro motivo, se acerquen a esta obra buscando soluciones a problemas concretos del día a día, será la inclusión de numerosas sentencias y resoluciones de la Agencia de Protección de Datos que aportan una vertiente práctica de primer orden.

Además de sus elevados conocimientos jurídicos, la autora, pone de relieve su experiencia profesional en la materia, aportando soluciones a problemas concretos y complejos, actitud que sin duda agradecerá el lector. Todo ello sin dejar de señalar las dificultades que entraña la aplicación práctica de esta normativa, sobre todo en lo concerniente al tratamiento de datos de carácter personal; dificultad que en el sector asegurador se acrecienta por la propia naturaleza del negocio, en el que los datos personales, incluso del más alto nivel, constituyen una parte esencial del mismo.

Destacar la atención prestada a los medios de prueba electrónica, esto es a la firma electrónica y al DNI electrónico. Verdadera especialista en esta materia concreta, no en vano a ello dedicó su tesis doctoral, la autora nos explica no sólo el funcionamiento técnico con detalle, sino que pone de relieve su decisiva aplicación como instrumento jurídico en cuanto a la prueba. Y, aún avanzando más y en línea con todo el trabajo, se adentra en el análisis de cómo están siendo utilizados estos medios por el sector asegurador, llamándonos la atención sobre la revolución que va a suponer en este ámbito su previsible utilización masiva.

Finalmente a modo de guía práctica y como colofón final, nos deja lo que a su juicio son los retos del sector asegurador en el campo de las nuevas tecnologías y en el de INTERNET en particular.

Desde la perspectiva del profesional de la seguridad, en la que nos encontramos, con la obligación de gestionar de forma integral los riesgos de nuestra empresa, no es nada fácil encontrar respuestas a problemas técnicos propios de la seguridad de la información en su vertiente tecnológica, teniendo claro a su vez, el aspecto jurídico. Porque, no se puede perder de vista, que si el análisis de la regulación normativa es vital no sólo en cualquier materia que pueda afectar a cualquier campo profesional, sino en toda relación humana envuelta por el velo jurídico, en el campo de la seguridad en general y en particular en el de la seguridad de la documentación, el análisis jurídico, cobra una importancia desmedida incrementada por la problemática del tratamiento de los datos personales; tanta que es este aspecto jurídico el que está concentrando la atención de los profesionales. Y resulta que la faceta jurídica a veces está alejada de la técnica y viceversa, lo que supone una dificultad añadida para el profesional de la seguridad. Pues bien, este trabajo de investigación contribuye a estrechar la relación de la técnica con el mundo jurídico, analizando la problemática de la aplicación de las tecnologías en el sector asegurador, desde ambas perspectivas. Cuestión por la que a nuestro juicio supone una buena herramienta para el profesional de la seguridad que gestiona seguridad de la información.

Desde el otro lado del problema, el jurista que se enfrenta a la seguridad de la información y concretamente al análisis jurídico de las nuevas tecnologías, se encuentra con la problemática técnica. Para el profesional jurídico, este trabajo realizado por una jurista con un elevado conocimiento técnico, puede arrojarle luz a muchos de sus problemas derivados de las nuevas tecnologías.

Por último, en el conjunto de los sectores profesionales potencialmente favorecidos por este trabajo de investigación, no se puede dejar de mencionar al sector profesional que lo ha motivado, el asegurador. Para los profesionales del seguro, más que o además de aportar soluciones a problemas concretos, se trata de una verdadera guía de actuación para el tratamiento de los datos personales en general y en cuanto a su aplicación a las tecnologías de la información en particular. Nos atrevemos a decir que se trata de una obra muy recomendable para el profesional del sector del seguro, en cualquiera de sus facetas. Con el valor añadido de afectar a todos los ámbitos del seguro y, como consecuencia de sus ejemplos que a veces ponen de manifiesto graves consecuencias para la aseguradora, operar como factor de mentalización y formación.

José María Cortés Saavedra
Subdirección General de Seguridad y Medio Ambiente de MAPFRE

ÍNDICE

ABREVIATURAS

LOPD	Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos Personales
RD	Real Decreto
SI	Sociedad de la Información
TIC	Tecnologías de la Información y del Conocimiento
St.	Sentencia
art.	Artículo
AEDP	Agencia Estatal de Protección de Datos
Núm.	Número
Rec.	Recurso
Res.	Resolución
LORTAD	Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LSSI-CE	Ley 34/2002, de 11 de julio de Servicios de la sociedad de la Información y de Comercio electrónico

INTRODUCCIÓN

El llamado síndrome del pez rojo es sin duda el que mejor refleja la situación ante la que se encuentra cualquier usuario que navega por la Red. Esta expresión hace referencia al riesgo al que queda expuesto cualquier persona que se conecta a la Internet. En efecto, desde del momento en que solicitamos que nuestro terminal se conecte a la Red pasamos a formar parte del escaparate en el que todos nuestros datos se muestran con o sin nuestro consentimiento de manera que pasamos a ser observados como si de una gran pecera se tratara y en la que los peces navegan a su antojo ajenos a la curiosidad que su "aspecto" suscita.

Este símbolo puede trasladarse al entorno asegurador para demostrar como su plena incorporación al entorno de las nuevas tecnologías ha abierto un espacio que bajo el manto protector de la Red de Redes va dibujando un escenario dinámico, cambiante y regido muchas veces por la incertidumbre o, cuanto menos, por la duda sobre la seguridad jurídica del usuario de la Red.

Partiendo de esta idea, la primera cuestión a dilucidar es el objeto y el sujeto sobre el que se va a centrar este estudio. El objeto es el sector asegurador y dentro de él se acota el trabajo centrándolo en la problemática que plantea la prestación de servicios on-line. Incluso con esta delimitación, que lleva a excluir un gran debate como es el de la prestación de servicios off-line, el objeto del trabajo resulta bastante amplio lo que permite hacer un planteamiento de origen global, en el que se creará la plataforma jurídica común que hasta el momento sirve de anclaje para garantizar la actuación del sector asegurador en el marco de las nuevas tecnologías.

El segundo paso será focalizar el interés en las cuestiones concretas que preocupan al sector asegurador en sus relaciones y comunicaciones por Internet.

Por lo que se refiere al sujeto de este estudio, hay que destacar el carácter bifronte del mismo. En efecto, interesa analizar no sólo al usuario de Internet en tanto que "cliente" o "potencial cliente" sino también la seguridad jurídica de las compañías aseguradoras que ofrecen sus servicios en la Red.

Mucho se escribe sobre la necesidad de proteger al usuario en su navegación por Internet, pero la protección de las empresas parece ser un tema más técnico que jurídico, una cuestión que el sector empresarial debe resolver por

sus propios medios a través de inversiones económicas que lógicamente estarán en función de la capacidad financiera de la empresa, de su tamaño y de sus prioridades, pero nunca, salvo contadas y honrosas excepciones, de ayudas públicas.

Una de las cuestiones que más preocupa a las empresas que desarrollan toda o parte de su actividad comercial por Internet es la de la identidad de la otra parte de la conexión.

No es está, por supuesto, la única inquietud: la alteración de datos, el desvío y utilización no deseados de los mismos, entre otras, figuran como principales preocupaciones.

En el sector asegurador a lo anterior hay que añadir el importante cambio que ha sufrido el mercado bajo el influjo de los propios acontecimientos sociales que vive nuestra sociedad donde las estructuras tradicionales están cambiando y las preocupaciones y prioridades también. Ello ha producido una importante transformación en el modelo de negocio que responde a las necesidades del mercado.

Al mismo tiempo, el espectro legal también ha sido modelado lentamente por el cincel del estado del arte dando como resultado el nuevo perfil del mercado asegurador y marcando las pautas para su plena integración en el entorno digital.

Un ligero vistazo a la Red nos permite afirmar que quien no está presente en su arquitectura simplemente no existe en ni para el mercado.

El documento publicado por la revista *Actualidad Aseguradora* en marzo de 2007 sobre el *Informe de la situación del sector asegurador en Internet en España y en el mundo* muestra la presencia de las principales compañías en la Red y cómo su oferta de servicios crece exponencialmente. Con todo, también se han alzado voces que denuncian la excesiva euforia con la que se anunció el advenimiento de las compañías aseguradoras al entorno digital y la situación real en estos momentos, muy por debajo de las expectativas.

En este contexto, los cambios se asientan sobre cuatro pilares: sociales, jurídicos, económicos y tecnológicos. De todos ellos, este trabajo centra la atención en el segundo de ellos lo que no obsta para que, a lo largo del desarrollo, se utilicen aspectos de los otros tres pilares con el fin de ofrecer al lector una visión panorámica completa de la seguridad jurídica de las tecnologías de la información en el sector asegurador.

El pilar jurídico constituye sin duda el rodamiento de partida que pone en marcha la compleja maquinaria que hace posible ir perfeccionando la protección jurídica que demandan usuarios y empresas.

El Dorado para muchos está más cerca pero si bien esto resulta incuestionable, la premisa contraria debe mantenerse férreamente instalada en la mente de todos los que participan en la Red de modo que nunca se abandone la perspectiva utópica de la seguridad absoluta. En otras palabras, quien no quiera correr riesgos simplemente debe optar por no correr, pero esto, de nuevo, resulta utópico en la sociedad actual.

Por tanto ante la disyuntiva de estar o no estar el riesgo se asume como parte del negocio, en el caso de las empresas y como resignación mal llevada por parte del usuario de a pie.

Para entender cómo funciona el sector asegurador en Internet y qué protección existe en la actualidad, se ha dividido el trabajo en dos partes.

En la primera se justifica el nuevo entorno en que actúa: aspectos sociales y tecnológicos, así como la panorámica jurídica en que se desenvuelve.

En la segunda parte, se profundiza en los problemas que para el sector asegurador implica el uso de las nuevas tecnologías desde el punto de vista de la seguridad jurídica de las relaciones on-line. Para ello se ha delimitado el campo de análisis a aquellas materias que plantean mayores interrogantes: la identidad de las partes, la contratación de seguros on-line, el valor de la prueba y el cumplimiento de la normativa sobre protección de datos.

En esta parte, la metodología que se va a utilizar será descriptiva partiendo del planteamiento de la cuestión con cuadros y ejemplos reales y fundamentando la solución en las herramientas con que cuenta todo jurista: la Ley, la interpretación judicial de problemas puntuales, los Informes de la Agencia Española de Protección de Datos y la posición doctrinal, cuando proceda.

Las nuevas tecnologías no agotan su espectro de influencia en el entorno digital en el que se desenvuelven sino que, muy al contrario, lanzan puentes de retorno al mundo material. Por paradójico que parezca el desbordante desarrollo de las TIC lejos de producir una brecha insoslayable entre el mundo digital y el físico, como algunos autores vaticinaban[1] está coadyuvando a reforzar la seguridad jurídica del interesado hasta el punto que el proyecto de Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre y publicado en el BOE de 19 de enero de 2008, incluye un Título dedicado a la protección de los ficheros *no automatizados*.

Esto es, se corrige ahora algo por donde debería haberse empezado allá por 1992, cuando se aprueba la primera LPD, y se hablaba de un término nuevo para la mayoría de nosotros como eran “los ficheros automatizados”

[1] LESSIG, El Código y las Leyes, 2001.

concediendo una moratoria que expiró en octubre de 2007, para adaptar los ficheros no automatizados a la LPD.

El principal problema es que el Reglamento se ha aprobado acabada la moratoria lo que obliga a modificar las medidas de seguridad de esos ficheros y varía el catálogo de ficheros a los que se exigen medidas de niveles alto/medio o bajo.

Dada la importancia que los ficheros no automatizados tienen para el sector asegurador, se dedica un apartado, en la Primera Parte de este trabajo, al análisis del Reglamento de Seguridad, con la intención de dejar constancia de los interrogantes que abre toda vez que la impresión en papel de cualquier documento convierte a éste en objeto de protección por la LOPD.

En la última parte del trabajo se describen los retos del nuevo mercado asegurador contemplando cuestiones como las nuevas funciones atribuidas a los mediadores de seguros.

Con ello se pretende dar una panorámica de la situación jurídica del mercado asegurador a la luz de las tecnologías de la información y las comunicaciones y suscitar en el lector nuevos interrogantes a los que pueda dar respuesta con apoyo de las páginas de este trabajo o al menos utilizarlas en la búsqueda de las mismas.

1ª Parte
PANORÁMICA JURÍDICA DEL ENTORNO ON-LINE DEL SECTOR ASEGURADOR

Capítulo I
UTILIZACIÓN DE LAS TIC EN EL SECTOR ASEGURADOR

SUMARIO. 1. EL SECTOR ASEGURADOR Y SUS RETOS. 1.1.- La transformación del sector asegurador. 1.2.- El cliente como eje central del negocio. 1.3.- Tecnologías más humanas. 2. INFLUENCIA DE LAS TIC EN EL SECTOR ASEGURADOR. 2.1- Evolución y tendencias de las tecnologías de la información y las comunicaciones en el mercado asegurador. 2.2.- Previsiones de crecimiento del sector asegurador en Internet. 2.3. Modelos de negocio en Internet.

1. EL SECTOR ASEGURADOR Y SUS RETOS

1.1 La transformación del sector asegurador

El sector asegurador interactúa por naturaleza con el entorno en que se mueve por lo que debe tener muy presente ese medio a la hora de diseñar sus decisiones. De este modo, la realidad empresarial coloca en primer término a los aspectos sociales, económicos, culturales, políticos, tecnológicos y jurídicos.

El conocimiento de todos ellos permite identificar un número variable de factores que son tenidos en cuenta a la hora de diseñar las estrategias de trabajo en el entorno asegurador. El interés por su estudio se apoya en los profundos cambios que se han producido en las dos últimas décadas.

La década de los setenta marca el inicio del cambio en el sector asegurador, pasando de una situación estática y fuertemente regulada a otra más dinámica, liberalizada y marcada por la competitividad.

Este precipitado puede analizarse desde dos puntos de vista. Desde la óptica de la desregulación que sufre el mercado asegurador y desde la perspectiva de los cambios de tipo institucional que se traducen en una variación en el comportamiento de las aseguradoras.

De este modo, el cuadro siguiente muestra los componentes que han favorecido el cambio y el modo en que éstos han influido en el mismo:

FACTORES	VARIABLES	INCIDENCIA
Socioculturales	Demografía Envejecimiento de la población Nueva percepción de los seguros Cambio estilos de vida Multiplicación de formas unidad familiar Inmigración *Singles*	Cambios en la demanda Cambios en la oferta
Económicos	Crecimiento económico. Aumento Renta per cápita Incremento relaciones comerciales Tasa de ahorro de las economías domésticas Tipos de interés Tasa de inflación	Potencial crecimiento Riesgos asociados Nuevos riesgos
Sectoriales	Mercado Único de Seguros	Expansión del mercado Incremento competencia Nuevos productos Nuevos canales distribución
Legislativos	Regulación del sector Adaptación acervo comunitario Mediadores	Concentración Competencia de distribución Especialización
Tecnológicos	Redes Informáticas Internet Tecnologías de Información y Comunicaciones	Mediación del seguro Producción del seguro Accesibilidad

Fuente: elaboración propia

Todos los cambios manifiestan una estrecha correlación entre el crecimiento económico y la actividad aseguradora. Cambios sociales tales como el nivel cultural de la población, los cambios demográficos, la inmigración o las nuevas formas de unidades familiares influyen igualmente en los productos que se ofrecen y en la demanda de seguros. Además el desarrollo de las nuevas tecnologías de la información y las comunicaciones presenta implicaciones directas en la oferta y la demanda.

La desregulación del sector supone no sólo la eliminación de las normas más restrictivas que se aplicaban a determinadas operaciones sino la liberalización del sector con la creación del Mercado Único del Seguro.

Para entender la transformación que ha sufrido el sector asegurador y con ello localizar las necesidades del mercado, se analizan los factores enumerados en el cuadro anterior y su incidencia en el seguro.

El objetivo en este momento es exponer todos los factores que intervienen en la configuración de la actual industria aseguradora, si bien los dos últimos son los que específicamente centran este trabajo y de ahí que se trate de ellos con más profundidad en los siguientes apartados de este Capítulo.

La delimitación de las necesidades se sitúa, por un lado, en la base para la creación de productos dentro del sector y, por otra, sirven de referencia para configurar una protección jurídica lo suficientemente fuerte para garantizar, en último extremo, la seguridad del sector asegurador en Internet.

Los *cambios socioculturales* sitúan al cliente como principal elemento de referencia. Los comportamientos de la población, su estilo de vida, el nivel de educación o la demografía han cambiado provocando una preocupación por la previsión aseguradora. Tradicionalmente los consumidores excluían los productos aseguradores de su cultura financiera por no ser considerados como fórmula de ahorro; sin embargo, en los noventa la percepción cambia y comienza a verse en los seguros una garantía para mantener en el futuro el nivel de vida deseado. Así, la decisión de contratar un seguro de vida comienza a suscribirse con independencia de la edad del asegurado y de su adscripción al sistema de la Seguridad Social.

En España, a lo anterior se añade la difícil situación que atravesaba el sistema público de pensiones para garantizar las jubilaciones futuras, lo que favoreció la aparición de productos de vida (en su modalidad de ahorro y de planes de jubilación/pensiones).

Por tanto, los cambios socioculturales modificaron cambios en la demanda de seguros pasando a ser considerados como forma de ahorro y de previsión en paralelo a la expansión del gasto per cápita de las economías domésticas en seguros. La actitud del consumidor también se ha transformado, ahora es él quien toma la decisión de asegurarse.

Los cambios demográficos afectan positivamente a la industria aseguradora. El segmento de población que muestra una mayor necesidad por adquirir un seguro para cubrir una situación patrimonial o personal se extiende desde los treinta hasta los cincuenta años.

Sin duda, la conceptuación del seguro como producto financiero con rentabilidad aparejada supuso el impulso que el sector buscaba. Las rentas más altas, comenzaron a suscribir seguros no sólo como previsión sino por las ventajas fiscales de los mismos y las rentas medias y bajas se subieron al carro con objeto de obtener cierta rentabilidad.

A finales de los noventa los estudios elaborados por el Instituto de Cooperación entre Entidades Aseguradora (ICEA) confirman al seguro como el sistema de previsión preferido por el cliente y en 1999, por primera vez, el gasto en vida supera al gasto por habitante y año realizado en los ramos no vida, lo que reafirma un cambio de actitud en el consumidor ante el seguro como fórmula de ahorro y previsión.

El *proceso de desregulación* se suele contemplar desde la óptica bancaria pero tiene una gran repercusión en el sector asegurador. En España, el carácter universal de la banca permite a ésta realizar cualquier tipo de operaciones bancarias y parabancarias, sobre la base de la Segunda Directiva de Coordinación Bancaria de la Unión Europea. De este modo, se permite que la banca intervenga, a través de filiales especializadas, en actividades que antes tenía vedadas como era el caso de los seguros[2].

Esta participación, sin embargo, está limitada a la distribución de productos de seguros por parte de las instituciones financieras y no a la producción del servicio asegurador en sí que únicamente puede prestarse por las empresas que han recibido la expresa habilitación para actuar en la actividad aseguradora. Esta circunstancia ha propiciado la interrelación y cooperación entre la actividad de la banca y de seguros articulándose la mayoría de las veces a través de una entidad bancaria matriz de aseguradoras filiales especializadas.

Con ello la desregulación, al eliminar barreras legales, ha fomentado el aumento de opciones estratégicas creando nuevas oportunidades de negocio, diversificando los productos y facilitando nuevas formas para acceder a los mercados, lo que, a su vez se ha visto catapultado por el uso de las nuevas tecnologías de la información y las comunicaciones.

La *evolución de la economía*, por su parte, orienta la actividad aseguradora hasta el punto de llegar a afirmarse que la evolución del seguro explica la evolución de la economía y viceversa. El desarrollo del seguro está íntimamente ligado a las magnitudes económicas, si bien se manifiesta con retraso por el carácter prepagable de las primas. El incremento del PIB de un país aumenta las primas emitidas por el sector asegurador.

El aumento de la actividad aseguradora se justifica por el incremento de la riqueza, que, a su vez, genera una mayor demanda de propiedades y bienes duraderos susceptibles de ser asegurados. Se produce un fenómeno paralelo

[2] Ley 3/1994, de Adaptación de la Segunda Directiva de Coordinación Bancaria.

en los seguros de daños dado que a mayor desarrollo económico aumentan los riesgos de manera proporcional lo que supone una demanda en ese mismo sentido de cobertura de seguro.

Otras variables económicas que inciden directamente en la contratación de seguros de vida es la tasa de ahorro de las economías domésticas, la fluctuación de los tipos de interés y la tasa de inflación.

Los tipos de interés varían en función de las políticas monetarias y fiscales condicionando la intermediación financiera de las compañías aseguradoras. Así, una reducción de tipos resulta perniciosa sobre la demanda del seguro de vida y sustituye la opción del cliente por activos a largo plazo por otros a corto.

Otro dato fundamental para los intermediarios financieros y para las entidades aseguradoras, en particular, es la tasa de inflación. La subida de los precios perjudica al seguro, provoca inestabilidad y desincentiva el ahorro. La capacidad adquisitiva de los capitales asegurados se reduce, el gasto aumenta y el ahorro disminuye, elevándose los gastos de gestión del seguro de vida y no vida.

Con esta perspectiva, y dada la situación de bonanza económica de nuestro país en los últimos años el mercado asegurador continúa consolidándose, situándose muy cerca de los países de nuestro entorno.

El *Mercado Único de Seguros* fue consecuencia de la liberalización de los movimientos de capital y de la liberalización de la oferta como consecuencia de la puesta en marcha de la libre prestación de servicios y de la libertad de establecimiento propugnada por la Unión Europea.

La puesta en marcha del Espacio Económico Europeo y sus principios dirigidos a la liberalización del mercado han llevado a una desregulación caracterizada por la caída de barreras legales, fronterizas y comerciales, entre las que destacan la liberalización de los sistemas de distribución.

La implantación de las cuatro libertades básicas: personas, servicios, capitales y establecimiento, esenciales para la creación del gran mercado comunitario único, culminó con estas dos últimas. El proceso se dividió en dos fases que fueron configurando el marco legal asegurador.

Todos estos esfuerzos supusieron la eliminación de restricciones y discriminaciones en la actividad de las compañías de seguros procedentes de diferentes países de la Unión Europea con respecto a aquéllas cuya actividad se localizaba en el país de residencia del cliente.

1.2. El cliente como eje central del negocio

Los factores que se vienen identificando como elementos del cambio del sector asegurador sitúan al cliente en un lugar de privilegio. El cliente demanda servicios de calidad y compara los productos que ofrece el mercado.

En todo este proceso las nuevas tecnologías han venido a facilitar el acceso a los productos aseguradores y a elevar el nivel de información sobre los mismos, a lo que se añade la mayor formación de los clientes. Por otro lado, Internet se sitúa en el canal más utilizado por los españoles para conseguir información sobre servicios o productos.

Los datos evidencian que el usuario está demandando información y la tendencia apunta a que esa información sea cada vez más completa y continuada de manera que quede reflejado todo el proceso así como el detalle de la cartera de servicios disponible.

El cliente está demandando también nuevos canales de comunicación con el sector asegurador, tanto de distribución como de relación. Estos canales son fundamentalmente el teléfono e Internet.

Las nuevas tecnologías de la información y las comunicaciones ofrecen una amplia gama de posibilidades para que el acceso a la información sea cada vez más especializado y dirigido a las necesidades del cliente en particular. Lo que demanda no es sólo acceder a la web de la aseguradora sino una continuidad en la relación; esto es, que una vez adquirido el producto pueda seguir en contacto con la aseguradora de manera que pueda resolver on-line los problemas o dudas que le puedan surgir.

1.3. Tecnologías más humanas

En este punto del trabajo resulta más que evidente que la llamada Sociedad de la Información está cambiando nuestros hábitos de conducta y cada vez más nuestra cotidianeidad está siendo ocupada por las diferentes tecnologías que nos ayudan a una vida más cómoda.

Dentro de los numerosos aspectos que pueden analizarse en relación al impacto de las TIC en el sector asegurador se va a centrar la atención en este momento en la humanización de los servicios prestados. Esta humanización hace referencia a un estilo en la oferta de productos y servicios. Lejos del trato aséptico que durante algún tiempo la profesionalidad de las empresas ha llevado aparejado, el cliente demanda un trato más humano, más próximo, mas, si se me permite, “de barrio”, en el que perciba que sus preocupaciones y necesidades realmente interesan a la otra parte de la relación.

En la práctica, las nuevas tecnologías ayudan a reducir esta brecha al permitir obtener respuestas con una simple llamada o un clic sobre el ratón; si bien se debe continuar trabajando en esta línea. Todas las grandes compañías aseguradoras cuentan con números gratuitos a disposición del cliente para la resolución de cuestiones generales si bien se cuida menos el trato al cliente una vez establecida la conexión, la atención suele ser fría y poco satisfactoria para el cliente.

El uso de Internet viene a paliar un poco está situación, al menos para la horquilla de población que maneja este recurso. El trato sigue siendo lejano e impersonal pero da respuesta a las cuestiones planteadas por el interesado.

De ahí que el siguiente paso sea acercar el sector seguros al cliente a través de las tecnologías en el sentido de personalizar el trato a través, por ejemplo de asistentes personales con los que poder comunicarse a través de mails, sms, páginas webs, etc.

Todo ello se engloba dentro del término calidad del servicio. La calidad vista desde la óptica del cliente debe cimentarse en tres pilares: la atención directa, la información y la participación del ciudadano. La conjugación de estos principios permite alcanzar la auténtica calidad en la prestación de los servicios aseguradores con un elevado grado de satisfacción para el cliente.

Se viene incidiendo en este trabajo en el cambio sufrido por la sociedad en las últimas décadas tanto en lo que se refiere a formación como a la información que llega a los clientes. Ello se ha traducido en un aumento de las exigencias del ciudadano a la hora de interesarse por los productos aseguradores lo que ha impulsado un cambio de la oferta y un incremento en la calidad de los mismos.

El aparente binomio calidad-satisfacción se presentan como términos independientes en la práctica. Puede disponerse de una cartera de productos de muy buena calidad y, a la vez, obtener un grado de satisfacción variable que estará íntimamente ligado a las expectativas creadas.

2. INFLUENCIA DE LAS TIC EN EL SECTOR ASEGURADOR

2.1. Introducción

El constante avance de las tecnologías de la información y las comunicaciones ha favorecido el procesamiento y almacenamiento de datos y ha logrado conectar los mercados a nivel mundial. Paralelamente al desarrollo de la informática el avance de las comunicaciones, y en particular, la popularización de Internet unido a la generalización de la banda ancha han

conformado el nicho idóneo para el desarrollo de nuevas aplicaciones centradas en las comunicaciones.

Por otro lado, los protocolos para la comunicación de los sistemas informáticos han adquirido la madurez necesaria para producir una revolución en la creación de sistemas informáticos en red. Si a esto se añade la mejora en las técnicas de tratamiento masivo de información (*datamining* o *datawarehouse)* así como el uso generalizado de herramientas de gestión del negocio (CRM, ERP) o las tecnologías que permiten el intercambio seguro de datos, completan el mapa de la actividad aseguradora en el entorno digital. Con todo, el impacto ha sido limitado.

El sector seguros se encuentra en un momento adecuado para aprovechar todos estos progresos a un coste lo suficientemente bajo. La aportación tecnológica al negocio consiste en proporcionar un sistema de información desde, por y para el negocio que permita adaptar ágilmente los procesos de gestión actuales y futuros. Este sistema ha de responder a la gestión de nuevos clientes y a la gestión de soluciones (producto-canal-modelo relacional). Las ventajas del uso de las nuevas tecnologías para la industria aseguradora pueden enumerarse de la siguiente manera:

1. Favorece la eliminación de barreras de acceso al mercado lo que incrementa la competencia.

2. Eleva la eficacia del proceso de transacciones en el ámbito de la distribución.

3. Modifica la cadena de actividades de las aseguradoras tanto en la distribución como en la producción de seguros.

4. Incrementa el número de aseguradores con diferentes modelos de negocio, por lo que aquéllas que parten con una marca de reconocido prestigio captan con mayor rapidez la confianza del cliente.

5. Internet se postula como un nuevo canal de distribución que modula la concepción de los productos y eleva la eficacia de la intermediación.

6. Internet es considerado como un canal de venta pasivo, por que se considera la vía ideal para la comercialización de productos estandarizados como los de automóviles, multirriesgo y hogar.

7. El uso de Internet supone un potencial ahorro de costes, dado que parte del trabajo administrativo recae en el propio cliente que realiza parte del proceso, por ejemplo, a través del registro de sus datos personales.

8. Lo anterior implica la optimización de los procesos de producción, al mejorar la administración, la gestión de siniestro y la obtención, análisis y suministro de información.

9. También supone nuevos retos como son la eliminación de barreras de entrada, una mayor competencia y un cumplimiento escrupuloso de la legislación relacionada con las nuevas tecnologías.

Las tecnologías de la información y las comunicaciones amplían el abanico de posibilidades de la industria aseguradora en diversos campos. De este modo, destaca la innovación de la oferta aseguradora y los cambios en la distribución y comercialización del seguro. La eliminación de barreras físicas facilita el acceso de nuevos participantes e introduce cambios en la competencia, en los productos y favorece nuevas posibilidades de distribución; si bien, esto último depende de la actitud del consumidor, que es quien decide asegurarse en línea. De ahí la importancia clave que para el sector asegurador tiene el diseño de sus plataformas en la Red, no sólo desde el punto de vista de sus contenidos, diseño, accesibilidad o facilidad de uso, sino también de la seguridad jurídica de las operaciones que se realicen por el consumidor-cliente.

2.2. Evolución y tendencias de las tecnologías de la información y las comunicaciones en el mercado asegurador

En este apartado se analiza el papel de tienen las Tecnologías de la Información y las Comunicaciones en el sector asegurador. Para ello, se utilizan ejemplos significativos de soluciones basadas en el uso de las TIC que pueden contribuir a alcanzar los retos que se plantean a la industria aseguradora. No se busca en este momento identificar con carácter exhaustivo todas las soluciones disponibles en el mercado sino exponer las más generalizadas que ilustran el entorno digital asegurador y que se sitúan en la base de este estudio para, a partir de ahí, construir, en la tercera parte de este trabajo y, sobre planteamientos prácticos, el marco jurídico regulador de la actividad aseguradora en la SI.

Las TIC constituyen la herramienta esencial para la implantación de la Sociedad de la Información y están presentes en todos los ámbitos de la actividad aseguradora. La presencia de las TIC ha cambiado la manera en que se producen las relaciones entre ciudadanos, empresas y administraciones y hoy en día sería muy difícil ya entender éstas sin aquéllas.

Los puntos más destacables en este proceso son:

- En relación al cliente, la penetración de la tecnología fija y móvil ha permitido la comunicación y el acceso a información desde cualquier lugar, lo que incide, como ya se ha apuntado más arriba en la calidad de vida y

en la comodidad de servicios como: mails, mensajería, acceso a información vía web, contratación de servicios on-line..., contribuyendo a modificar los hábitos de los ciudadanos.

- En cuanto a las empresas aseguradoras, han percibido con rapidez las ventajas asociadas al uso de las TIC potenciando cambios en los procesos para mejorar la eficiencia en el uso de Internet para realizar transacciones comerciales o para informar sobre productos y servicios.

- Las Administraciones, por su parte, también se han incorporado al uso de las TIC y en muchos casos son punteras en su utilización. Utilizan Internet para mostrar información, permiten rellenar formularios o cumplir con obligaciones vía electrónica.

En la última década el sector asegurador ha sufrido una transformación significativa tanto en su estructura como en su marco regulador impulsado por la competitividad del mercado que las tecnologías de la información y las comunicaciones han acelerado.

El ritmo de evolución de las tecnologías ha sido muy intenso y lejos de reducirse tiende a incrementarse como consecuencia del elevado grado de innovación tecnológica y la competencia del mercado. Así, se lanzan a diario cientos de dispositivos electrónicos y servicios relacionados con las TIC y, aunque en muchos casos se trata de nuevas versiones de productos ya existentes, incluyen mejoras y se consideran conceptualmente como distintos a los anteriores.

La tecnología que se aplica en el sector asegurador se resume en:

1. Sistemas informáticos y bases de datos centralizadas.
2. Aplicaciones de gestión en entorno web.
3. Aplicaciones web de gestión para clientes (mediadores).

El incremento constante del *ancho de banda* para la conexión de terminales a Internet ha permitido un nuevo escenario en el que la provisión de servicios ha aumentado enormemente. El ancho de banda determina la velocidad a la que el usuario puede enviar y recibir información y de ahí que un mayor ancho de banda permite una respuesta más rápida en los accesos a Internet y en la descarga de páginas web, correos electrónicos, etc. Además determinados servicios no pueden funcionar sino cuentan con un mínimo de ancho como ocurre con la voz o el video.

La *tecnología de movilidad* o tecnología inalámbrica favorece las posibilidades con que cuenta el usuario a la hora de acceder a los servicios y productos aseguradores con independencia del lugar en que se encuentre. A ello se añade la alta capacidad de comunicación que se puede obtener con

tecnologías como el HSDPA[3] del UMTS[4] que previsiblemente aumentará cuando se completen los desarrollos actuales de LTE[5]. Estas tecnologías resultan muy útiles en el ámbito de la sanidad cuando se trata de trasladar actividades a lugares distintos de los habituales[6].

Un segundo grupo de tecnologías inalámbricas está formado por aquéllas de menor alcance cuyo uso se circunscribe a edificios. Entre ellas destacan las tecnologías Wi-Fi (Wireless Fidelity) que posibilita la transmisión de datos en un radio de 100 metros.

Los terminales equipados con un acceso Wi-Fi como los PC, PDA, portátiles, etc., acceden a la red inalámbrica que a su vez está conectada a la Intranet de la aseguradora o a Internet. En el futuro los equipos Wi-Fi basados en el estándar IEEE 802.1 1n o en el grupo de tecnologías Wimax auguran mayores ventajas tanto en velocidad como en alcance de las redes.

Un tercer grupo de tecnologías sin cable es el *Bluetooth* que permiten la transmisión de datos y voz entre equipos a través de un enlace por radiofrecuencia, facilitando las comunicaciones de corto alcance entre equipos móviles y fijos, eliminado cables.

Por último las tecnologías *RFID* (Radio Frequency Identification, identificación por radiofrecuencia) es un método de almacenamiento y recuperación de datos remoto que utiliza etiquetas o *tags*. Estas pegatinas se pegan al producto lo que les permite recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID.

La *digitalización de contenidos* consiste en el proceso de conversión de la información a un formato digital de manera que pueda procesarse fácilmente por un ordenador. La digitalización de la información constituye un elemento clave para la convergencia tecnológica permitiendo manejar de forma única toda clase de fuentes de información, con el consiguiente ahorro de costes y ofreciendo una mayor flexibilidad y libertad a la hora de implantar nuevos productos.

Además resulta más efectivo almacenar, manejar y procesar la información en formato digital. En este sentido, las nuevas tecnologías facilitan la catalogación, búsqueda y distribución no sólo de la información contenida en formatos digitales sino también la no digitalizada, siendo un excelente ejemplo en este sentido el efectivo y eficiente trabajo que realiza el Servicio de Documentación de MAPFRE.

[3] High-Speed Downlink Packet Access.

[4] Universal Mobile Telecommunications System

[5] LonfgTerm Evolution

[6] Informe sobre las TIC en la sanidad del futuro, p. 146. Telefónica, 2006.

El sector asegurador debe contar con un sistema de desarrollo e implantación que permita registrar de manera digital toda la actividad que se realiza en el sector, transmitiendo por redes telemáticas los datos actualizados del cliente de manera inmediata y concurrente. De esta manera se evita la duplicidad de datos o la utilización de datos no actualizados, que constituye uno de los caballos de batalla del sector y por lo que recibe el mayor número de denuncias y sanciones (Ej.: Procedimiento PS 377/2005, que dio lugar a la resolución de 23 de mayo de 2006 en relación a la contratación de un seguro sin autorización del cliente; Sentencia de la Audiencia Nacional de 20 de junio de 2005 o Sentencia de 28 de septiembre de 2005, ambas por cesiones inconsentidas de datos por aseguradoras).

El *equipamiento* (PC, portátiles, PDA, móviles,etc.) evoluciona continuamente demostrando así la conocida Ley de Moore según la cual cada 18 meses se duplica la densidad de los transistores integrados en un chip lo que implica que *las prestaciones de los chips se vienen duplicando cada año y medio*.

Además la capacidad de memoria y de los discos duros aumenta al tiempo que los nuevos diseños incorporan en ordenadores más pequeños y ligeros mayor número de prestaciones. Nuevas tecnologías como las memorias flash, utilizadas en cámara digitales, PDA, pen-drives,etc., se han extendido rápidamente y su alta calidad unido a su bajo precio, los ha convertido en los más demandados del mercado llegando a sustituir a los discos duros en las aplicaciones que requieren menor capacidad.

Por otro lado, la existencia de redes de comunicaciones de alta velocidad permite separar el lugar donde reside la información de aquel en que se utiliza lo que ha favorecido la creación de centros de almacenamiento de datos de gran seguridad donde se guarda la información.

El desarrollo de sistemas ha permitido la aparición de nuevas *arquitecturas tecnológicas*, fundamentalmente de aquéllas relacionadas con Internet que permiten aplicaciones interoperables, flexibles, auditables y escalables.

Como ejemplo de este tipo de arquitectura: *SOA* (Service-Oriented Architecture). Se trata de una arquitectura *software* dirigida a los servicios. Esta arquitectura permite desarrollar servicios[7] que pueden ser utilizados por otras aplicaciones *software*. SOA implementa los servicios de una forma determinada para cada componente *software*, si bien los usuarios de los servicios (personas o aplicaciones informáticas) pueden utilizarlo a través de un interfaz estándar con independiencia de su implementación interna; esto es, los componentes son independientes pero se estandariza el interfaz de

[7] Entendiendo por servicio la unidad de trabajo necesaria para llevar a cabo una tarea particular.

servicios y por tanto la forma en que los componentes se comunican entre si. Esta arquitectura se implementa normalmente a través de *web services*[8].

El sector seguros está evolucionando hacia formas más proactivas y personales, integrando de manera masiva las tecnologías de la información y de las comunicaciones. Se trabaja en fórmulas más efectivas y eficientes para los clientes, personalizando la oferta, confirmando, de este modo, a las TIC como uno de los agentes del cambio del sector.

2.3. Previsiones de crecimiento del sector asegurador en Internet

El informe realizado por la consultora Tatum, en marzo de 2007, refleja el gran avance que se ha producido en el uso de las TIC pero también pone de manifiesto otra evidencia y es que no se han cumplido las expectativas generadas. A pesar de ello, el documento resulta de gran interés por los datos que ofrece y que permiten elaborar un perfil del tipo de usuarios que accede a la gran red, sus prioridades, el índice de contratación a través de la red, sus prevenciones y, en definitiva, dibujar el escenario sobre el que el sector asegurador proyecta una parte importante de su actividad.

Los costes informáticos del sector asegurador crecieron un 10% en 2006 respecto al año anterior, lo que supone un 2,04% de las primas periódicas y alrededor de 8,63 euros por póliza. El coste en informática se repartió de la siguiente manera: un 39% para el personal (interno y externo), un 20% en servicios; el 16% en software, un 15% en equipos y el 11% en telecomunicaciones. La preocupación por la seguridad se refleja en el incremento en un 6% del presupuesto destinado a la misma (Informe nº 1034 de ICEA, septiembre 2007).

Las comunicaciones a través de Internet se perciben como algo habitual y el grado de dependencia es muy alto. Todas las entidades usan el correo electrónico. Aparte de Internet las aseguradoras disponen de gran variedad de tecnologías relacionadas con la informática. Las más utilizadas y por este orden son: los *call centrer* (77%), data warehouse (74%), gestión documental (63%), videocoferencias (56%), wireless (51,5%), B2B (42%), worflow (42%) y B2C (37%).

El uso de Internet por el cliente se encuentra por debajo de lo esperado. En nuestro país, la radiografía muestra que el perfil que accede a la red es el de un varón de entre 25 y 44 años, de clase social media-media, que reside en Madrid, País Vasco o Cataluña, con tiempo para acceder todos los días desde

[8] Conjunto de estándares que definen un protocolo de innovación remota de servicios, generalmente basado en el lenguaje XML Los *servicios web* permiten que aplicaciones de *software* desarrolladas en lenguajes de programación diferentes y que se ejecutan sobre cualquier plataforma puedan interactuar e intercambiar datos en redes de ordenadores como Internet.

su propia casa y que consulta páginas de la World Wide Web o el correo electrónico. Curiosamente si se analizan estos datos con detenimiento se observa que el número de usuarios ha aumentado del 1% en 1996 hasta casi el 38% en 2007 y los usuarios que se conectan diariamente han aumentado en un 70%.

Un cambio importante ha sido el lugar desde el que nos conectamos a Internet. La incorporación del ordenador al hogar es una constante hasta el punto de que el 97,4% de las conexiones se hacen desde allí, reduciéndose aquéllas que se realizan desde el trabajo o desde los centros de estudio.

Otra de las cuestiones que se intentan resolver es para qué accede a la red el usuario. En este sentido, el mayor crecimiento se ha localizado en las tradicionales descargas de música o documentos (P2P), con un avance desde el año 2004 de un 33,7%. Otros usos por este orden son el correo electrónico, el Messenger y la consulta de dominios. Por el contrario disminuye el uso de chat y la transferencia de ficheros.

Por sexos sigue dominando la presencia del masculino, aunque ha descendido un 24,5%, incrementándose, por el contrario, la presencia de la mujer, aumentando su porcentaje en un 82,2%, situándose en la actualidad en un 41,9%, frente al 58,1% del hombre.

En cuanto a la clase social, en 2007 el principal usuario de Internet es de clase media-media, seguido de la media-alta, con un decrecimiento de un 36,7% desde 1996, año en que se situaba como primera.

Otro aspecto al que se refiere el informe es a la zona geográfica de los usuarios. En España, las Comunidades Autónomas con mayor penetración son: Madrid, País Vasco y Cataluña. En el extremo contrario están Extremadura, Castilla-La Mancha y Galicia. En cualquier caso, en los últimos diez años el índice ha aumentado en todas las comunidades destacando en primer lugar Cantabria (2.975%) y siendo la menor la Rioja (677,5%).

El último punto del que se ocupa Tatum en relación al uso de Internet en España analiza si se han hecho realidad las previsiones del mercado. La respuesta es que no y se refiere a la causa de esta deficiencia, localizándola en el fracaso del sistema UMTS; esto es, los teléfonos de tercera generación.

En efecto, la Asociación de usuarios de Internet (AUI) vaticinó en el año 2000 que en cinco años el número de usuarios se acercaría a los 18,5 millones; sin embargo, en el 2005 los usuarios no superaban los 14 millones, de hecho sólo en el 2001 la previsión estuvo a la altura o ligeramente por encima de la predicción.

La segunda parte de su informe, centra la atención en los usuarios de Internet a nivel mundial. Estados Unidos es el país con mayor número de usuarios superando los 207 millones (España se sitúa en el nivel 13).

En la Unión Europea la penetración se sitúa en la mitad de la población (51,9%), si bien España, como se ha señalado, esta por debajo de la media, ocupando el quinto lugar por detrás de Alemania, Reino Unido, Francia e Italia.

Por lo que se refiere al idioma, el castellano es el cuarto más utilizado, por detrás del inglés, el chino y el japonés.

Analizando las costumbres por país, se observa una evolución que va desde una mayor dedicación a consultar páginas web en 2003 que tres años después. Como dato curioso, España es el país en que el usuario está más tiempo visitando cada página web.

2.4. Modelos de negocio en Internet

El entorno digital precisa nuevas formas de concebir el negocio asegurador. La configuración del mismo permite definir todos los factores clave de cualquier proyecto. El VII Informe de la consultora Capgemini publicado en octubre de 2007, analiza los modelos de negocio más significativos en el mercado asegurador on-line, y los reduce a los siguientes:

- Entidades aseguradoras multirramo. Esta denominación engloba a todas las compañías que operan fundamentalmente fuera de la red. Poseen una página web que utilizan mayoritariamente como canal de información.

- Entidades de banca-seguro. Entidades bancarias que simultanean servicios aseguradores on-line con su actividad tradicional.

- Aseguradores on-line. Actúan únicamente a través de la Red, comercializando sus productos y servicios on-line.

- Mediadores on-line. Tienen las mismas características que una aseguradora on-line pero adaptando sus servicios a la mediación.

Capítulo II
LA REGULACIÓN DE LOS SEGUROS PRIVADOS EN EL MARCO DE LAS TIC

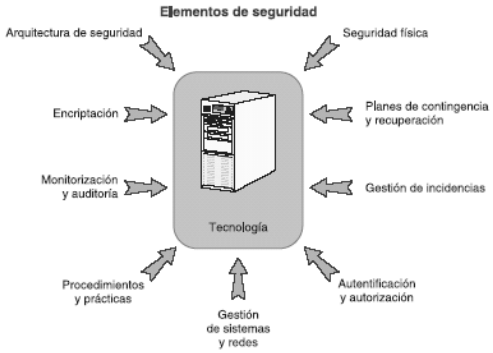
SUMARIO.- 1. EL ESTADO ACTUAL DEL SECTOR ASEGURADOR EN ESPAÑA: RÉGIMEN JURÍDICO REGULADOR. 2. LA REGULACIÓN DE LA UNIÓN EUROPEA Y SU INFLUENCIA EN LA NORMATIVA ESPAÑOLA DEL SEGURO PRIVADO. 3. LA LEY 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD). 3.1. Antecedentes. 3.2. Aspectos más destacables de la LOPD. 4. EL REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE, POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY 15/99. 5. EL REGISTRO DE CONTRATOS DE SEGURO DE COBERTURA DE FALLECIMIENTO. 5.1. El Registro como fichero común. 5.2. El derecho de acceso y rectificación. 5.3. La comunicación de datos por las compañías aseguradoras. 6. TEXTO REFUNDIDO DE LA LEY DE ORDENACIÓN Y SUPERVISIÓN DE LOS SEGUROS PRIVADOS, REAL DECRETO 6/2004, DE 29 DE OCTUBRE (TRLOSSP). 7. LA LEY 26/2006, DE MEDIACIÓN DE SEGUROS PRIVADOS. 7.1.- Los agentes de seguros como encargados del tratamiento. 7.2.- Los agentes vinculados. 7.3.- Los corredores de seguros y reaseguros como responsables del tratamiento. 7.4.- Los Agentes externos.

1. EL ESTADO ACTUAL DEL SECTOR ASEGURADOR EN ESPAÑA: RÉGIMEN JURÍDICO REGULADOR

La información que manejan las aseguradoras tiene en muchos casos un carácter crítico dado que se trata de datos que tienen reconocido el máximo nivel de confidencialidad en la LOPD. Los sistemas de información deben incorporar desde su primera definición todas las herramientas técnicas que respondan al cumplimiento de la normativa legal como el control de acceso, tratamiento de datos, identidad, integridad, no repudio, etc.

Existe tecnología que garantiza suficientemente la seguridad y la confidencialidad de la información. Estos mecanismos aseguran la privacidad de la información y previenen la manipulación o el uso indebido de datos esenciales, garantizando la integridad de datos, de las aplicaciones y de los equipos frente a posibles amenazas o ataques. Tal y como se muestra en el cuadro siguiente hay varias prácticas de seguridad que contribuyen a ello.

La autenticación del usuario es un aspecto clave para garantizar la seguridad. En este sentido se ha avanzado en los últimos años con tecnologías como la denominada PKI (Public Key Infraestructura) o mediante la utilización de rasgos biométricos inherentes a la persona como puede ser el iris, la huella digital o el reconocimiento de cara.



Fuente: Informe Telefónica: *Las TIC en la sanidad del futuro*, en: http:// www.telefonica.es, marzo, 2007.

La protección jurídica de la actividad aseguradora en relación a las TIC se focaliza en torno al cumplimiento de la normativa sobre protección de datos, contratación electrónica, publicidad en red y servicios de la sociedad de la información.

En este apartado se hace una aproximación a las cuestiones básicas de la regulación aplicada a los seguros privados en el marco de las nuevas tecnologías de la información y de las comunicaciones, haciendo hincapié en aquéllas que constituyen el sustrato de las reformas que se están gestando en este momento y que determinarán el comportamiento del mercado de seguros en poco tiempo en lo que se refiere al uso de las nuevas tecnologías on-line.

Aun cuando en este trabajo se analizan fundamentalmente aspectos relacionados con la regulación en el sentido de la seguridad jurídica en el marco de las nuevas tecnologías de la información y de las comunicaciones, es necesario hacer una breve descripción del marco legal que permite entender la evolución del mercado, en un primer momento, sanearlo y modernizarlo, a continuación, para prepararlo ante los nuevos desafíos.

La regulación en materia de seguros privados se recoge por primera vez en España en la Ley de Registro y Vigilancia de entidades aseguradoras de 14 de mayo de 1908 que durante casi cincuenta años se convirtió en el instrumento adecuado para el control del sector. Sus principios básicos se centraban en el control previo de la legalidad sobre aspectos contractuales y técnicos y regulaba cuestiones como la publicidad o las funciones de un órgano asesor y de audiencia pública que aún existe: la Junta Consultiva de Seguros.

El siguiente momento importante en este proceso se produce en 1954 con la Ley de Ordenación del Seguro Privado, de 16 de diciembre, que continúa con la concepción del control de la ley anterior en sentido de verificación previa de la legalidad de las pólizas; esto es, que las condiciones de las pólizas tuvieran el contenido fijado administrativamente.

Sin embargo, lo que a principios del siglo XX se reveló como idóneo para regular la actividad del sector no resultaba ya operativo a mediados de los 50 porque, de un lado, suponía un elevado nivel de restricciones a la actuación de las entidades aseguradora limitando sus capacidades de innovación y crecimiento y, de otro lado, el mercado empezaba a demandar medios de control suficientemente efectivos que permitieran introducir medidas correctoras cuando fuera necesario.

Lo más importante de la Ley de 1954 fue que fijó las características básicas del modelo tradicional del mercado asegurador español hasta los ochenta. Se trataba de un mercado muy regulado, de poco desarrollo y escaso peso en la economía.

Las deficiencias del mercado se debían fundamentalmente a la falta de adecuación de la oferta a la demanda y a la actuación administrativa. El sector se estructuraba en torno a un elevado número de entidades de reducido peso (en torno a 560 con forma de sociedad anónima o mutua y aproximadamente 600 bajo la forma de previsión social, frente a las menos de cuatrocientas que existen en la actualidad).

Por lo que se refiere a la demanda, la tasa de ahorro familiar era muy reducida y carente de actuaciones de fomento en seguros privados.

Desde el punto de vista de la actuación administrativa el control de la legalidad previa mediante la revisión de la documentación técnica y mercantil y el sometimiento a aprobación administrativa (previa) de las pólizas y tarifas frenaba el crecimiento del mercado y eliminaba la competencia, sin prestar atención al control de solvencia, por lo que se le considera como el paradigma del intervencionismo público en este sector.

Los setenta y las sucesivas crisis económicas destaparon los profundos problemas de solvencia patrimonial del sector y las prácticas irregulares que, en ocasiones acompañaba a la práctica del sector. Todo ello hizo necesario una reforma en profundidad de un mercado que ya comenzaba a utilizar las nuevas tecnologías[9].

Este conjunto de normas está encabezado por la Ley 50/1980, de 8 de octubre, de Contrato de Seguro. Esta norma vino a dotar al contrato de seguro de la regulación mínima de la que carecía, derogando los desfasados artículos del Código de Comercio de 1885. Estableció la regulación básica de los

[9] En la década de los 60 Catalana Occidente decidió apostar por la informática y fue la primera en incorporar la informática como herramienta en sus procesos de gestión de negocio, lo que permitió sustituir las máquinas de escribir por ordenadores, además de permitir la retirada de equipos voluminosos, pasando a rellenarse un parte asegurador desde formularios en blanco a imprimirlos directamente desde la pantalla, al tiempo que las bases de datos se actualizaban más rápidamente. *Las aseguradoras se suben al carro de Internet,* en: Revista Sociedad de la Información, mayo 2006, pág. 60.

derechos y obligaciones de las partes de la relación contractual y por tanto, hoy también se utiliza como marco para la contratación electrónica on/off line.

No menos importante fue la Ley 33/1984, de 2 de agosto, de Ordenación del Seguro Privado, así como el Real Decreto-Ley 10/1984, por el que se establecieron las medidas urgentes para el saneamiento del sector de los seguros privados reforzando los mecanismos públicos de control.

Respecto a la ordenación del mercado, es necesario destacar que se realizó un importante esfuerzo por normalizar el régimen jurídico de todas las entidades aseguradoras, incluidas las mutualidades de previsión social, promoviendo la concentración del mercado, así como la especialización separando los negocios de seguros de vida y de seguros distintos del de vida.

Otro de los problemas del sector era la escasa atención que se prestaba a la solvencia. La Ley de 1984, y su normativa de desarrollo, introdujeron innovaciones importantes, reconociendo el principio de solvencia fundamentalmente orientado a sus aspectos técnicos y financieros. Como exponente cabe citar las diferentes normas relativas a las condiciones de acceso al mercado, los mayores requisitos financieros (capital mínimo, provisiones técnicas, margen de solvencia o fondo de garantía), así como la implantación de un marco jurídico para actuar en caso de concurrir algún problema con entidades aseguradores. Mediante las medidas cautelares se asegura su saneamiento sin necesidad de sanciones ni la intervención pública directa. Asimismo la Ley reguló mecanismos de expulsión del mercado para aquellas entidades que no alcanzaran los requisitos financieros mínimos para desarrollar su actividad.

La otra norma básica en este proceso se publica el mismo año que la anterior, es el Real Decreto-Ley 10/1984, de 11 de julio, por el que se establecen las medidas urgentes para el saneamiento del sector de los seguros privados. Esta norma creó la Comisión Liquidadora de Entidades Aseguradora (CLEA) que permitió la liquidación de un elevado número de entidades en crisis, en su mayoría de escasa dimensión y capacidad financiera, que se mantenía en el mercado como consecuencia de la falta de competencia del mismo y de control en materia de solvencia.

El mecanismo fue novedoso y efectivo. Se procedió a comprar los créditos a los acreedores de estas entidades, favoreciendo no sólo su liquidación de manera ordenada sino también un mayor porcentaje de recuperación de esos créditos. Con ello se consiguió sanear el sector mediante la consolidación definitiva de los nuevos principios de ordenación de la actividad aseguradora e intensificando la supervisión del sector.

En paralelo, a este proceso de modernización del mercado asegurador a nivel interno, nuestro país se prepara para su incorporación a la Comunidad Europea en 1986 por lo que se encontraba inmerso en preparar la adaptación

de nuestra legislación a la entonces Comunidad Económica Europea que exigía como requisito indispensable la incorporación al ordenamiento español de la normativa comunitaria, lo que, indudablemente, facilitó las reformas que se vienen enumerando.

Conforme van eliminándose los controles previos sobre productos y precios las empresas se hacen más competitivas en diseño, comercialización de productos y en los precios que ofrecen a sus clientes.

2. LA REGULACIÓN DE LA UNIÓN EUROPEA Y SU INFLUENCIA EN LA NORMATIVA ESPAÑOLA DEL SEGURO PRIVADO

El nuevo marco legal, del que puede afirmarse que las dos normas aprobadas en 1984 constituyeron la espoleta transformadora clave del sector asegurador español cimentando su proceso de reforma y modernización, también propició la internacionalización del sector, no sólo por el saneamiento al que se ha aludido sino por la armonización de nuestra legislación a la comunitaria lo que atrajo a entidades extranjeras bajo el reclamo de las expectativas de crecimiento del sector en España.

La incorporación de España a la hoy Unión Europea supuso para el sector de los seguros privados la adaptación del acervo comunitario existente así como la aplicación de las directivas posteriores que se irán sucediendo a un ritmo intenso, sin olvidar que cada transposición suponía la incorporación a la norma interna no sólo de la comunitaria sino de todas aquellas modificaciones que en ese momento demandaba el mercado nacional.

En este contexto, la Ley 21/1990, de Adaptación a la Normativa Comunitaria de la Legislación de Seguros Privados, incorpora la Directiva sobre Derecho de Establecimiento en los seguros distintos del de vida, introduciendo otras modificaciones como el nuevo régimen jurídico del Consorcio de Compensación de Seguros, clave para la estabilidad del sector.

En 1992 se afronta uno de los temas más importantes para el mercado asegurador como es su comercialización. La Ley 9/1992, de 30 de abril, de Mediación en Seguros Privados, completará, junto con la Ley de Ordenación de 1984 (centrado en solvencia y reordenación del mercado), el marco de reforma por lo que se refiere a la distribución de los seguros privados.

Tres años después se aprueba la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, que supone el eje de la regulación actual y base para redactar el texto refundido vigente. En realidad esta ley tuvo como objeto integrar la actividad aseguradora española al marco jurídico comunitario, lo que suponía la adaptación de una serie de Directivas anteriores a la entrada de España en la Comunidad Europea y que, tras casi

nueve años de pertenencia a la misma no se habían incorporado a nuestro ordenamiento interno.

Las dos primeras generaciones de Directivas se habían encaminado a regular dos aspectos esenciales: la libertad de establecimiento y la libertad de prestación de servicios. La adaptación de la Ley 30/1995 supuso, entre otras cosas, la implantación de la autorización administrativa única en todos los ramos del seguro agilizando de este modo la actuación de las compañías aseguradoras en todo el marco del Espacio Económico Europeo (en adelante EEE) en virtud del derecho de establecimiento (a través de sucursal) o de la libre prestación de servicios (directamente desde España), sometida exclusivamente al control financiero de las autoridades españolas.

El principio de reciprocidad hace posible que cualquier entidad aseguradora domiciliada dentro del EEE pueda operar en nuestro país sujeta al control financiero de su Estado de origen.

Por su parte, la tercera generación de Directivas finaliza con la plena implantación del mercado Único del seguro.

En este proceso, la primera generación de Directivas incluye la Directiva 73/239/CEE, de 24 de julio, sobre seguro de daños, que suprime las restricciones a la libertad de establecimiento, y la Directiva 79/267/CEE, de 5 de marzo, sobre seguros de vida, armonizando las normas de acceso a la actividad aseguradora.

La segunda generación de Directivas comienza con la Directiva 88/357/CEE, de 22 de junio, sobre seguros de daños, que regula parcialmente la libre prestación de servicios en la Comunidad Europea y la Directiva 90/619/CEE, de 8 de noviembre, sobre el seguro de vida que mejora la libertad de establecimiento y regula la libre prestación de servicios.

La tercera Directiva de seguros de daños (no vida), Directiva 92/49/CEE, de 18 de junio, que recoge la única autorización administrativa y liberaliza la elección de los clientes en todo el territorio de la Unión Europea.

Ese mismo año se aprueba la tercera Directiva sobre seguros de vida, Directiva 92/96/CEE, de 10 de noviembre, que también obliga a una única autorización administrativa.

Al objetivo principal de la Ley de 1995 de transponer las Directivas comunitarias se unieron otras modificaciones que la modernización del mercado exigía[10]. El afán codificador de la citada ley hizo que sus reformas se

[10] Real Decreto 2014/1997, de 26 de diciembre, por el que se aprueba el Plan de Contabilidad de las entidades aseguradora y normas para la formulación de las cuentas de los grupos de entidades aseguradoras; Real Decreto 2486/1998, de 20 de noviembre, por el que se aprueba

extendiesen a toda la normativa sobre seguros privados. De este modo, se introducen modificaciones en los aspectos contractuales del seguro (las modificaciones alcanzan a la Ley de Contrato de Seguros, la Ley de Responsabilidad Civil así como a la normativa sobre circulación de vehículos a motor) y en la mediación (Ley de Mediación en Seguros Privados). Las reformas de carácter institucional se introducen de la mano de la regulación de la CLEA y de las modificaciones en el Estatuto Legal del Consorcio de Compensación de Seguros. Por último, también se revisan cuestiones básicas de previsión social, regulándose la instrumentación de compromisos por pensiones a través de la Ley de Regulación de Planes y Fondos de Pensiones.

El otro gran bloque de modificaciones normativas se dirigió a reforzar la protección del asegurado, mediante la presentación de quejas y reclamaciones ante la Dirección General de Seguros y Fondos de Pensiones. La protección se amplía a partir de entonces a los terceros perjudicados en el ámbito del seguro de responsabilidad civil y recoge, con carácter voluntario, la figura del defensor del asegurado en las compañías. En este esfuerzo también se incluyen mecanismos perfeccionados de protección de crédito de los asegurados frente a las entidades aseguradoras.

Por último, la reforma de 1995 afecta también a los procedimientos administrativos de ordenación y supervisión, aclarando los requisitos que han de cumplirse para la tramitación de los diversos procedimientos de autorización, modificación y revocación administrativa, así como para la disolución y liquidación de entidades aseguradoras y la puesta en marcha de medidas de control especial.

La siguiente etapa en este proceso evolutivo de la normativa aseguradora se produce ya entrado el siglo XXI con una importante ley: la Ley 44/2002, de medidas de reforma del sistema financiero, modificada un año después por la Ley 34/2003, para adaptarla a la normativa comunitaria sobre seguros privados. Esta última tuvo por finalidad principal transponer una serie de directivas comunitarias sobre aspectos concretos exigidos por las necesidades del mercado. De todas ellas, sin duda las relacionadas con el margen de solvencia[11] son las que más quebraderos de cabeza han traído a

---

el Reglamento de ordenación y Supervisión de Seguros Privados; Orden ministerial de 23 de diciembre de 1998, por la que se desarrollan determinados preceptos de la normativa reguladora de los seguros privados y se establecen las obligaciones de información como consecuencia de la introducción del euro; Real Decreto 996/2000, de 2 de junio, por el que se modifican determinados preceptos del Reglamento de Ordenación y Supervisión de los Seguros Privados y del Plan de Contabilidad de las entidades aseguradora, para adaptarlos a la Directiva 98/78/CE, de 27 de octubre, relativa a la supervisión adicional de la empresas de seguros que formen parte de un grupo de seguros.

[11] Directiva 2001/17/CE sobre saneamiento y liquidación de entidades aseguradoras; Directiva 2002/12 y 2002/13 sobre margen de solvencia de entidades aseguradoras de vida y de seguros distintos del de vida. La Directiva 2002/63/CE sobre seguros de vida, deroga la Directiva 2002/12 y refunde y codifica la normativa comunitaria sobre el seguro de vida.

las entidades aseguradoras. Las directivas refuerzan las exigencias cuantitativas en relación al fondo de garantía y al margen de solvencia, previendo tres tipos de medidas en las que las autoridades pueden intervenir en caso de que se vean amenazados los derechos de los asegurados: exigencia de un plan de recuperación financiera; obligar a las entidades de seguros a tener un margen de solvencia más alto que el reglamentario y revisar a la baja los elementos que integran el margen de solvencia disponible.

Por último, y sin ánimo de resultar exhaustivos debe citarse la ley 5/2005, sobre supervisión de los conglomerados financieros, por la que se modifican diversas normas del sector financiero y que tiene su origen en la Directiva 2002/87/CE, de 16 de diciembre, relativa a la supervisión adicional de las entidades de crédito, empresas de seguros y empresas de servicios de inversión de un conglomerado financiero.

Como conclusión a este apartado cabe decir que la regulación de seguros en España se ha caracterizado por un proceso de cambio desde el control previo de la legalidad de la documentación contractual y administrativa hasta la regulación de la solvencia, pasando de ser preventiva a ser más prospectiva, sin olvidar que el papel dinamizador que el mercado único de los seguros ha tenido en todo el proceso de saneamiento. La regulación indirecta del sector implica menos prescripción y ha ido ganando importancia por la libertad que ofrece a las entidades, si bien presenta inconvenientes como la mayor discrecionalidad de juicio para el supervisor y la complejidad analítica de las fórmulas utilizadas (por ejemplo, el de los de sistemas de capital basado en el riesgo: RBC) que incorpora instrumentos que requieren ser permanente y escrupulosamente adaptados[12].De cara al futuro, de nuevo la normativa comunitaria marca la pauta. Tres son los hitos a los que se enfrenta el sector. En primer lugar, el *proyecto Solvencia II*, que supone un replanteamiento tanto en los ámbitos de supervisión como de gestión de las entidades aseguradoras.

En segundo lugar, el nuevo procedimiento de creación de normas en el marco de los servicios financieros dentro del esquema conocido como *procedimiento Lamfalussy[13],* que inicialmente se aplicó al mercado de valores y que posteriormente se ha extendido al sector bancario de seguros. El procedimiento consiste en elaborar un diseño institucional que permita hacer más ágil y participativa la normativa comunitaria relacionada con los servicios financieros.

---

[12] ALVAREZ CAMIÑA, Sergio: *la regulación de los seguros privados*. Revista ICE, noviembre-diciembre, 2006, nº 833, p.112.

[13] El Sector Asegurador y de los Planes y Fondos de Pensiones, ICE, noviembre-diciembre 2006, nº 833, p.110.

Por lo que se refiere a los seguros y fondos de pensiones de empleo supone crear un sistema de cuatro niveles reguladores, en el que participan: la Comisión, el Consejo y el Parlamento, que se ocupan de aprobar los principios y directrices generales, y un grupo, llamado sistema de comitología, que se desglosa en dos partes: una de política reguladora (Comité de Seguros y Pensiones Ocupacionales Europeo, EIOPC) y otra de carácter supervisor (Comité de Supervisores Europeos de Seguros y Pensiones Ocupacionales, CEIOPS).

En tercer lugar, aquellas decisiones que se tomen en el seno de la Unión Europea en materia de política de estabilidad, integración y regulación de los servicios financieros, en aras a consolidar el mercado único. Todas las medidas incorporadas tienen un sentido muy concreto: incorporar por primera vez en la regulación comunitaria de seguros un enfoque dinámico y preventivo y preparar al sector para las reformas que introducirá el proyecto Solvencia II[14].

3. LA LEY 15/1999, DE 13 DE DICIEMBRE, REGULADORA DE DATOS DE CARÁCTER PERSONAL

La Ley Orgánica 15/1999, de 13 de diciembre, consagra el régimen jurídico fundamental de la protección de datos de carácter personal y tiene una importante repercusión en el ámbito asegurador en general, y de forma muy especial, desde la aprobación de la Ley 26/2006, de Mediación, en el marco concreto de la mediación y distribución de seguros privados. A efectos expositivos se incluye al final de este Capítulo un cuadro resumen de los aspectos más relevantes de la Ley en su aplicación al sector asegurador.

La configuración actual del sistema de protección de datos personales es el resultado de una evolución en paralelo de los esfuerzos nacionales por la regulación de la materia y los trabajos desarrollados en la esfera internacional en este ámbito.

3.1. Antecedentes

Los antecedentes de esta norma hay que buscarlos en el Convenio 108 del Consejo de Europa y en la Directiva 95/46/CE. Asimismo, un hecho relevante en la evolución histórica de la protección de datos personales fue la sentencia dictada por el Tribunal Constitucional Alemán de 15 de diciembre de 1983, en

[14] Los tres pilares que fundamentan el proyecto Solvencia II cuyo germen se encuentra en los Acuerdos de Basilea para el sector bancario, son: la adecuación de capital, los procesos de supervisión y la disciplina de mercado, incluyendo la difusión de la información financiera relevante. Internacional Association of Insurer Supervisors (2003): *Insurance Core Principles and Methodology*, Basiles, disponible en: www.iaisweb.org,

la que se establecen las bases de la autodeterminación informativa o consentimiento.

Lo más destacable del Convenio 108 es que en él se recogen por primera vez los principios básicos para la protección de datos (principio de calidad: los datos recabados deben ser pertinentes, no excesivos y mantenerle actualizados). Fija los criterios para la información, el consentimiento y el ejercicio de los derechos reconocidos a los titulares de datos.

De igual modo, enuncia los datos especialmente protegidos e indica la necesidad de establecer medidas de seguridad. Tampoco olvida asociar sanciones al incumplimiento de esas medidas e insta a los países firmantes a destinar los recursos necesarios para hacer efectivo todo el sistema.

Tras este Convenio la norma más reseñable en materia de protección de datos es la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Los aspectos más destacables de esta Directiva son:

- Se recogen medidas aplicables tanto a los ficheros automatizados como a los ficheros manuales (no automatizados).
- Se amplía el concepto de dato de carácter personal incluyendo en el mismo la imagen y el sonido.
- Se abre la puerta a un nuevo derecho como es el derecho de oposición.
- Se concede a los Estados miembros la posibilidad de regular medidas restrictivas que permitan conciliar el derecho a la intimidad con la libertad de expresión.
- Se incluyen los datos de afiliación sindical dentro del catálogo de datos especialmente protegidos.
- Se crea una nueva figura: el encargado del tratamiento.

La primera redacción de la Ley se publica en 1992 con la Ley Orgánica 5/1992, de 29 de octubre, sobre regulación del Tratamiento Automatizado de Datos de Carácter Personal, que desarrolla el párrafo 4 del artículo 18 de la Constitución española, y que se conocía como “LORTAD”. Esta norma fue derogada por la actual Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), al objeto de adaptar nuestro ordenamiento a la Directiva 95/46/CE.

Sin duda, uno de los puntos más destacables de la LORTAD fue el análisis en su Exposición de Motivos del concepto de intimidad contrastándolo con el de privacidad y argumentando el carácter más amplio del segundo frente al primero. La intimidad protege la esfera en que se desarrollan las facetas más

singularmente reservadas a la vida de la persona (domicilio donde realiza su vida cotidiana o comunicaciones a través de las que expresa sus sentimientos) frente a la privacidad que engloba una serie de facetas de carácter global del individuo que, aisladamente consideradas pueden carecer de trascendencia pero que, convenientemente unidas pueden trazar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

La intimidad se encuentra suficientemente protegida por las previsiones contenidas en los tres primeros apartados del artículo 18 de la Constitución y las leyes que lo desarrollan; sin embargo, la privacidad puede verse seriamente amenazada por la utilización de las tecnologías de la información y las comunicaciones.

Con todo, esta Ley fue objeto de numerosas críticas. Así, por ejemplo se destacaba el diferente trato dado por el jurista a los ficheros de titularidad pública y privada hasta el punto de provocar la sensación de nula protección para los titulares de datos personales respecto a los ficheros de titularidad pública desde el punto de vista de la efectividad de la defensa de su intimidad.

Otra de las críticas se dirigía al objeto mismo de la Ley que excluía de su ámbito a los ficheros manuales o en soporte papel.

La Ley fue desarrollada a través de diferentes disposiciones reglamentarias, algunas de las cuales siguieron en vigor tras la aprobación de la Ley 15/99, en particular los Reales Decretos 428/1993, de 26 de marzo;1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se oponían a la LOPD. Todas ellas has sido sustituidas por el Reglamento 1720/2007 de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, y en él se contemplan las materias pendientes de desarrollo.

Las carencias de la Ley llevaron a la Agencia Española de Protección de Datos a elaborar una serie de Instrucciones en materias concretas que, dado que no tienen carácter reglamentario, no habría que considerar ya vigentes y que, no obstante siguen siendo utilizadas como criterio interpretativo en lo que no contradigan a la LOPD. A los efectos de este trabajo las Instrucciones aprobadas por la Agencia en relación con la actividad aseguradora fueron tres:

- Instrucción 1/1995, de 1 de marzo, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito.
- Instrucción 2/1995, de 4 de mayo, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.
- Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

3.2. Aspectos más destacables de la Ley Orgánica de Protección de Datos

A. Estructura y contenido de la Ley

La LOPD se compone de 49 artículos estructurados en siete Títulos, a lo que hay que añadir seis disposiciones adicionales, tres transitorias, una derogatoria y tres disposiciones finales.

De los Títulos sólo uno, el IV (Disposiciones Sectoriales), se divide a su vez en dos Capítulos, uno dedicado a los ficheros de titularidad pública y otro dedicado a los ficheros de titularidad privada.

La Ley incluye un listado de definiciones entre las que se incluyen los conceptos de: dato de carácter personal, fichero, tratamiento de datos, responsable del fichero o tratamiento, afectado o interesado, persona física titular de los datos, procedimiento de disociación, encargado del tratamiento, consentimiento del interesado, cesión o comunicación de datos y fuentes accesibles al público.

El Titulo II recoge los principios de protección de datos regulando: la calidad de los datos, el derecho de información, el principio de consentimiento y la cesión de datos. De todos ellos nos ocuparemos en la II Parte de este trabajo, pretendiendo en este momento simplemente dibujar el contenido de la LOPD.

El Título III se refiere a los derechos de las personas y entre ellos deben destacarse: el derecho de impugnación, el derecho de información y acceso, el derecho de rectificación, de cancelación y el derecho de indemnización que se reconocen al titular de los datos.

El Título IV diferencia como se ha señalado entre ficheros de titularidad pública y privada. Dentro de los segundos, destaca la exigencia del consentimiento para recabar los datos; sin embargo, más adelante, el artículo 29 excepciona el principio de consentimiento para prestar servicios de solvencia patrimonial y crédito en beneficio de la transparencia y dinámica necesaria para prestar este tipo de servicios.

En estos casos, se debe diferenciar entre los ficheros llamados "de morosos" y los "de información comercial" o "para evaluar la solvencia".

El artículo 29 LOPD distingue estos dos tipos de ficheros en función de la fuente de la que procedan los datos. Así, por un lado, se encuentran los datos que se obtienen de fuentes accesibles al público[15] o directamente del afectado y, por otro, los que se obtengan del acreedor.

[15] Art 3 j) LOPD: Son fuentes accesibles al público *aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de*

Los ficheros denominados de “información comercial”, o ficheros “para evaluar la solvencia” recogen sus datos de fuentes accesibles al público o procedente de la información facilitada por el interesado o con su consentimiento (art. 29.1 LOPD).

Los ficheros “de morosos” se obtienen del acreedor o de quien actúe por su cuenta o interés. En este sentido, el precepto esta concebido como una norma condicionante de la licitud del tratamiento automático de los datos (de carácter personal) que sean necesarios para desarrollar la actividad comercial. Así es, a diferencia del apartado 1 del artículo 29 en que se reconoce la licitud de tratar automáticamente esos datos siempre que procedan de fuentes accesibles al público o hayan sido facilitados por el interesado o con su consentimiento; sin embargo, dado que los ficheros de morosos tienen una finalidad distinta a los de solvencia sólo será lícita su recogida si son aportados por los acreedores.

El Título V se reserva al Movimiento Internacional de Datos donde destaca la libertad como principio general en las transferencias de datos, modulada por el principio de territorialidad y por las recomendaciones de la Unión Europea en relación a los países con un nivel de protección no equivalente al europeo.

El órgano de control por excelencia es la Agencia de Protección de Datos cuya regulación se recoge en el Título VI y que convive con los órganos de control creados por las Comunidades Autónomas, reservándose la Agencia Estatal competencia exclusiva en materia de ficheros de titularidad privada.

El régimen de infracciones y sanciones del Título VII califica a las primeras en leves, graves y muy graves (art. 44), fijándose para los ficheros privados multas que oscilan entre 601, 01 euros hasta 601.012,10 euros graduándose la cuantía en función de la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, los beneficios obtenidos, el grado de intención, la reincidencia, los daños y perjuicios causados y cualquier otra circunstancia que sea relevante para determinar la antijuridicidad.

B. Ámbito de aplicación

La Ley de 1999 amplía su objeto incluyendo a partir de ese momento a los ficheros manuales estructurados.

---

acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos en su normativa específica y las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación

Respecto al ámbito geográfico de aplicación de la norma ésta alcanza no sólo a los tratamientos que tengan lugar en territorio español y cuyo responsable esté establecido en nuestro país sino también a aquél que no lo esté pero al que le sea aplicable la legislación española por utilizar para el tratamiento medios situados en el territorio español, salvo con fines de tránsito. Con esta redacción se reduce el número de ficheros que quedan fuera del ámbito de la norma sobre protección de datos (actividades domésticas, materias clasificadas, ficheros relativos a investigación del terrorismo y formas graves de delincuencia).

C. Definiciones

- Datos de carácter personal

Personas físicas

El ámbito de aplicación de la norma se refiere a todos los datos de carácter personal entendiendo por tal: "cualquier información concerniente a personas físicas identificadas o identificables" (art. 3, a) LOPD).

El objeto de protección no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (que otorga el artículo 18.1 de la Constitución) sino los datos de carácter personal por tanto también alcanza a los datos personales públicos que, por su propia naturaleza pueden ser accesibles al conocimiento de cualquiera[16].

El hecho de incluir los términos identificadas o identificables permite aplicar este supuesto no sólo a los datos que identifican a una persona directamente sino también a aquellos que permitan potencialmente identificar a una persona como ocurre con la dirección de correo electrónico o la dirección IP[17].

Por lo que se refiere a las direcciones de *correo electrónico*, cabe diferenciar dos supuestos:

[16] El Tribunal Constitucional ha elaborado una doctrina en la que la protección de datos de carácter personal evoluciona desde la consideración de derecho complementario del derecho a la intimidad personal y familiar hasta configurarse en un derecho fundamental independiente y autónomo del propio derecho a la intimidad.

[17] Las dudas suscitadas en torno a este precepto han ido siendo aclaradas por la Agencia Española de Protección de Datos en sus informes del año 1999 y 2003 (informe 327), disponibles en:
http://www.agpd.es

1. Por un lado, los casos en que voluntaria o involuntariamente la dirección de correo electrónico contiene información acerca de su titular: nombre y apellidos, empresa en la que trabaja, país de residencia –aparezcan o no éstos en la denominación del dominio utilizado-. En este caso, no hay duda que la dirección de correo identifica al titular de la cuenta por lo que dicha dirección debe ser considerada como dato de carácter personal.

2. Por otro lado, se plantea el supuesto de que la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (caso de combinaciones alfanuméricas sin significado o denominaciones abstractas). Un primer examen puede hacer concluir que no nos encontramos ante un dato de carácter personal.

   A pesar de ello, la dirección aparecerá referenciada a un dominio concreto de manera que resultará fácil identificar al titular mediante la consulta al servidor en que se gestione dicho dominio, sin que ello suponga un esfuerzo desproporcionado. Por lo que también este caso se haya amparado por la LOPD.

En este sentido, la APD en resolución de 20 de noviembre de 2006 sancionó a un particular con una multa de 601,01 euros por dejar a la vista direcciones de correo electrónico al enviar un mensaje con publicidad. El sujeto sancionado envió por correo electrónico un mensaje a 42 destinatarios diferentes cuyas direcciones estaban a la vista al aparecer en el campo CC (copia de carbón), en lugar de haberlas incorporado en CCO (copia de carbón oculta). La APD sancionó al particular por incumplimiento del artículo 10 de la LOPD dado que la dirección de correo electrónico es un dato personal que no puede utilizarse sin autorización de su propietario, ni hacerlo público a la vista de otros[18].

Respecto a la *dirección IP*, el Informe 327/2003 de la Agencia establece que el: "....TCP/IP es un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información cada uno de los cuales contiene una dirección IP del emisor y del destinatario.

Por otro lado, el DNS (sistema de nombres de dominio) es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP. Existen herramientas en la red que permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular".

Además, tanto los proveedores de acceso a Internet como los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP.

[18] PS/00072/2006, disponible en : http :www.agpd.es

En efecto, el cliente firma un contrato de acceso a Internet con un proveedor que crea y mantiene un fichero histórico con la dirección IP (fija o dinámica), el número de identificación del suscriptor, la fecha, hora y duración de la asignación de dirección.
Por otro lado, el usuario que accede a Internet está utilizando una red de telecomunicaciones (teléfono fijo o móvil), con lo que la compañía telefónica registrará el número marcado, la fecha, la hora y la duración de la llamada para su posterior facturación.

Todo ello significa que, con los datos de estas terceras partes se puede identificar a un usuario en Internet, por lo que estamos ante datos de carácter personal.

Personas jurídicas

Las personas jurídicas quedan excluidas del ámbito de protección de la norma. Nuestra norma no ha seguido el criterio acogido por el Convenio 108 del Consejo de Europa que preveía la posibilidad de proteger a las personas jurídicas en lo relativo a informaciones sobre grupos de personas, asociaciones, fundaciones, sociedades, corporaciones y cualquier organismo formado directa o indirectamente por personas físicas, que tengan personalidad jurídica. Ello no quiere decir que las personas físicas que integran esas personas jurídicas queden desprotegidas, de tal manera que en el momento en que se asocie la denominación de una persona jurídica a un nombre de contacto de una persona física se entiende que el fichero es objeto de protección por la LOPD.

En este sentido se ha pronunciado nuestro Tribunal Supremo en varias sentencias en las que reconoce el derecho al honor, intimidad e imagen de las personas jurídicas: SSTS de 21 de mayo de 1997, 28 de abril de 1989, 15 de abril de 1992, 26 de marzo de 1993 y de 9 de diciembre de 1993. También el Tribunal Constitucional se ha pronunciado al respecto en sentencias como la de 11 de noviembre de 1991 o de 26 de septiembre de 1995, en el sentido de no excluir la protección del artículo 18 de la Constitución a las personas jurídicas respecto a los ataques injustificados que afectan a su prestigio profesional y social y que *puede traducirse en una pérdida de la confianza de la clientela, de proveedores y concurrentes comerciales o de rechazo o minoración en el mercado de forma general (...)*[19].

Empresarios individuales o autónomos

Otra de las dudas más frecuentes que se suelen plantear en materia de protección de datos es determinar si la LOPD es aplicable a las personas que

[19] Sentencia de la Audiencia Provincial de Vizcaya, sección 5ª, en su sentencia de 29 de marzo de 2001, núm. 326/2001.

dentro del ámbito empresarial desarrollan su actividad como empresarios individuales o autónomos.

En este sentido, la AEPD en su Resolución de 21 de marzo de 2000, dictada en el Expediente E/00055/1999 señala que:

"Tanto la norma que se encontraba en vigor en la fecha en que (...) presentó denuncia contra (...) como la nueva Ley vigente en la actualidad limitan su objetivo a datos relativos a personas jurídicas. Dado que, en este caso, ha quedado acreditado que los informes que elabora (el denunciado) corresponden a personas físicas pero que desarrollan una actividad recogida en alguno de los epígrafes del Impuesto de Actividades Económicas, no es de aplicación la normativa sobre protección de datos de carácter personal."

Tras esta Resolución la Agencia ha ido dictando otras en las que se observa una clara contradicción con respecto a la anterior. Ante la duda, hay que recordar la STC 292/2000, de 30 de noviembre que establece que (FJ 6º):

"(...) 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 personales sean o no íntimos cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual que para ello está el artículo 18.1 de la Constitución sino los datos de carácter personal. Por consiguiente también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado, porque así lo garantiza su derecho a la protección de datos (...).

Y añade la sentencia del Tribunal Constitucional que (FJ 7º) "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, *o cuales puede este tercero recabar* (subrayado del autor), y que también permite al individuo saber quién posee esos datos personales y para qué (...)

No puede concluirse, por tanto, tal como hace notar el Abogado del Estado en la contestación, que los *empresarios individuales* y profesionales estén en su conjunto excluidos del ámbito de protección de la LOPD, sino que se hace necesario diferenciar (y la línea divisoria es confusa y difusa) cuándo un dato del empresario o profesional se refiere a la vida privada de la persona y cuándo a la empresa o profesión, pues sólo en el primer caso cabe aplicar la protección de la Ley Orgánica 15/1999".

Cabe concluir que cuando un dato relativo a un empresario individual o autónomo se refiere de forma clara a su condición de empresa, estaría fuera del ámbito de aplicación de la LOPD siempre y cuando no esté de algún modo relacionado con el ámbito de su vida privada.

- Soporte del fichero

La LOPD es aplicable a los datos almacenados en soporte automatizado y no automatizado, si bien la Disposición Adicional Primera concede un plazo a los responsables de los ficheros manuales hasta octubre de 2007 para adecuar dichos ficheros a las exigencias de la norma, lo que se refiere

fundamentalmente a facilitar a los interesados el ejercicio de los derechos recogidos en la LOPD.

La redacción dada por la Ley parece otorgar un período de no aplicación de la misma a los ficheros manuales; sin embargo, el criterio seguido por la Agencia Española de Protección de Datos y por los Tribunales españoles[20] es justo el contrario. En efecto, debe velarse por la protección de las personas titulares de los datos con independencia del soporte en que se encuentren ya que, de lo contrario, se podría eludir garantizar el tratamiento adecuado de los datos en aras a salvaguardar la intimidad de las personas[21].

- El fichero

La LOPD define el fichero como: "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

De ahí que, en relación con los ficheros manuales, las obligaciones exigibles al responsable del fichero sólo serán de aplicación cuando los mismos estén estructurados; esto es, organizados de forma que se pueda realizar una búsqueda que permita localizar esos datos conforme a un criterio determinado.

Así, el tratamiento automatizado de datos quedará siempre sometido a las normas de protección de datos mientras que el tratamiento no automatizado sólo es objeto de protección en tanto que los datos se encuentren ya contenidos en un fichero o cuando el tratamiento tenga por objeto la inclusión de los datos en un fichero.

En este sentido, resulta interesante destacar la definición de fichero no automatizado (fichero manual) recogida en el Reglamento de desarrollo de la LOPD:

"todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a

[20] En esta misma línea se manifiesta la directiva 95/46/CE en su Considerando 27.

[21] Resulta interesante el análisis del Gabinete Jurídico de la Memoria de la Agencia Española de Protección de Datos del año 2004, en relación a la aplicación de la LOPD a ficheros y tratamientos no automatizados: "... *en cuanto al plazo de doce años de la disposición adicional primera de la LOPD no puede sostenerse válidamente que se establezcan términos tan prolongados en el cumplimiento de los deberes por los que puedan resultar gravemente afectados derechos fundamentales de las personas. Es por ello que dicha previsión en lo que concierne a derechos fundamentales y a las libertades públicas de las personas, ha de aplicarse inmediatamente, según la doctrina del Tribunal Constitucional (STC 81/1992, de 28 de mayo)".*

sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica".

Por tanto, el dato fundamental que hay que tener en cuenta a la hora de aplicar la normativa de protección de datos es si los mismos se encuentran o no estructurados. En este sentido, resulta pertinente recordar que la Directiva de protección de datos en su considerando 27 establece que se aplicará a los ficheros y no a las carpetas que no estén estructuradas.

- Diferencia entre encargado del tratamiento y responsable del tratamiento

La Directiva de Protección de Datos incluye entre sus definiciones la distinción entre encargado del tratamiento y responsable del mismo. A estos efectos, la LOPD recoge la diferente posición de responsabilidad del responsable del fichero o tratamiento, como persona que decide sobre la finalidad, contenido y uso del tratamiento, a la del encargado del tratamiento que es la persona que trata los datos personales por cuenta de aquél (vid. El prestador de servicios).

Es precisamente la persona que decide sobre la finalidad, el tratamiento y el uso la responsable del fichero o del tratamiento, siendo el encargado del tratamiento únicamente la persona que trata los datos por cuenta de un tercero y sin posibilidad de decisión sobre ellos.

Resumen- comparativo:
Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y Reglamente 1720/2007 de Desarrollo de la Ley Orgánica de Protección de Datos

Asociación de contenidos

Artículo 1 LOPD: OBJETO

- **Ley 15/1999, de Protección de Datos de Carácter Personal**

  Protección de los derechos fundamentales de las personas físicas, y en especial su honor, intimidad personal y familiar respecto al tratamiento automatizado de datos de carácter personal.

- **Reglamento 1720/2007 de Desarrollo de LOPD**

  Tratamiento automatizado y no automatizado de datos de carácter personal.

Artículo 2 LOPD: ÁMBITO DE APLICACIÓN

- **Ley 15/199, de Protección de Datos de Carácter Personal**

  Dato de carácter personal:

  - De personas identificadas o identificables.
  - Registrados en soporte físico.
  - Ficheros públicos y privados.

  Excepciones:

  - Actividades personales y domésticas.
  - Materias clasificadas
  - Investigación de terrorismo y formas claves de delincuencia
  - Ficheros regulados por disposiciones específicas
    - Ley de Régimen Electoral
    - Legislación sobre Función Pública
    - Régimen del Personal Fuerzas Armadas
    - Registro Civil y Registro Central de Penados y Rebeldes
    - Grabaciones realizadas por las Fuerzas y Cuerpos de Seguridad

Principio de territorialidad:

Tratamiento realizados en territorio español en el marco de la actividad de un responsable del tratamiento situado en España.

Si el responsable del tratamiento no está establecido en España, se aplicará la LOPD atendiendo a las normas de Derecho Internacional Público.

Si el responsable del tratamiento no se encuentra establecido en territorio de la Unión Europea, se aplica la LOPD cuando utilice para el tratamiento medios situados en el territorio español, salvo que esos medios se utilicen únicamente con fines de tránsito.

Si el responsable del tratamiento no se encuentra establecido en territorio de la Unión Europea, se aplica la LOPD cuando utilice para el tratamiento medios situados en territorio español, salvo que esos medios se utilicen únicamente con fines de tránsito.

- ***Reglamento 1720/2007 de Desarrollo de LOPD***

  El Reglamento no se aplica a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

Artículo 3 LOPD: DEFINICIONES

- **Ley 15/1999, de Protección de Datos de Carácter Personal**

  ***Datos de carácter personal*:** cualquier información relativa a personas físicas identificadas o identificables.

  ***Fichero*:** conjunto organizado de datos de carácter personal cualquiera que sea su forma o modalidad de creación, organización o almacenamiento y acceso.

  ***Tratamiento de datos*:** operaciones y procedimientos técnicos o no que permitan la recogida de datos (grabación, conservación, elaboración, modificación, bloqueo y cancelación), así como las cesiones de datos (resultantes de comunicaciones, consultas, interconexiones y transferencias).

***Responsable del fichero o tratamiento*:** decide la finalidad, contenido y uso del tratamiento.

Afectado o interesado: persona física titular de los datos objeto de tratamiento.

***Procedimiento de disociación*:** tratamiento de datos de modo que la información obtenida no pueda asociarse a una persona identificad o identificable.

***Encargado del tratamiento*:** trata los datos personales por cuenta del responsable del tratamiento.

Consentimiento del interesado: *m*anifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado acepta el tratamiento de sus datos personales.

Cesión o comunicación*:* revelación de datos a una persona distinta al interesado.

Fuentes accesibles al público: censo promocional, los repertorios telefónicos, listas de grupos profesionales (nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo), diarios y boletines oficiales del Estado y los medios de comunicación**.**

- ***Reglamento 1720/2007 de Desarrollo de LOPD***

***Accesos autorizados*:** autorizaciones concedidas a un usuario para la utilización de los diversos recursos, incluidas las funciones atribuidas por delegación.

Autenticación: procedimiento de comprobación de identidad usuario.

Contraseña: información confidencial, frecuentemente constituida por cadena de caracteres, que puede ser usada en la autenticación de un usuario en el acceso a un recurso.

Control de acceso*:* mecanismo que en función de la identificación permite acceder a datos o recursos.

Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

Ficheros temporales*:* ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Identificación: procedimiento de reconocimiento de la identidad del usuario.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Perfil de usuario: accesos autorizados a un grupo de usuarios.

Recurso: cualquier parte componente de un sistema de información.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Sistema de información*:* conjunto de ficheros, tratamiento programas, soportes, y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de información podrás ser automatizados, no automatizados o parcialmente automatizados.

Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Transmisión de documentos*:* cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tienen la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

4. EL REAL DECRETO 1720/2007, de 21 DE DICIEMBRE, POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La necesidad de un texto reglamentario que desarrollara de manera integral la LOPD era un imperativo a efectos de garantizar la seguridad jurídica en la materia. Los problemas planteados por esta carencia se han ido subsanando mediante la aplicación de la disposición transitoria de la propia Ley a cuyos efectos: "*Hasta tanto 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, 1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley".*

No obstante, las citadas normas sólo presentaban soluciones parciales a las cuestiones que debían tener desarrollo reglamentario[22] con lo que el texto aprobado el 21 de diciembre cumple, si bien con algo de retraso, las previsiones de la Disposición Final Primera de la LOPD que impone al Gobierno la obligación de aprobar, o modificar las "disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley".

En cualquier caso, el Reglamento nace con la intención de no reiterar los contenidos de la norma superior y de desarrollar no sólo los principios de la Directiva 95/46/CE de Protección de Datos sino de rellenar el vacío legal que durante los años de vigencia de la Ley se ha constatado que necesita mayor desarrollo normativo.

Lo primero que llama la atención es que no sólo afecta a la LOPD sino a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico y a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que atribuyen competencias sancionadoras a la Agencia Española de Protección de Datos (AEPD), necesitadas de desarrollo reglamentario. En este sentido, el Reglamento desarrolla también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia, de ahí la especial dedicación que se ha prestado a este punto en el texto.

Mediante estas dos normas se amplía el ámbito competencial de la AEPD puesto que ambas normas ordenan la tutela no sólo de los derechos de las personas físicas sino también jurídicas.

El Reglamento se estructura en nueve Títulos que desarrollan los aspectos esenciales en esta materia. El desglose de cada uno ofrece una idea de los

[22] Vid. el cuadro que se incluye al final de este epígrafe en el que se comparan las cuestiones que deben ser desarrolladas vía reglamentaria , las soluciones dadas hasta el momento y las novedades introducidas en este sentido por el Real Decreto 1720/2007.

aspectos que hay que tener en cuenta a la hora de adecuar los tratamientos de carácter personal.

El Titulo I fija el objeto y su ámbito de aplicación, respetando lo preceptuado en la Directiva comunitaria sobre protección de datos en el sentido de incluir en su ámbito a los ficheros automatizados o no, pero no a las carpetas que no estén estructuradas.

Asimismo recoge una serie de definiciones que sirven de criterio interpretativo sin necesidad de analizar cuestiones de mayor profundidad.

Fija, por otro lado, el criterio a seguir en materia de cómputo de plazos acabando con las diferencias que existían en este sentido entre ficheros públicos y privados y aclara qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas que quedan excluidas del ámbito de aplicación de la protección de datos de carácter personal.

El Titulo II se refiere a los principios de protección de datos (artículos 4,5,6, y 12 LOPD) y ofrece, como la propia norma reconoce, un verdadero estatuto del encargado del tratamiento, haciendo, por otra parte, referencia a la forma de recabar el consentimiento y a su revocación. En este sentido, el texto presta especial atención a la captación de datos de menores y en el entorno de los servicios de comunicaciones electrónicas. Así, se refiere al deber de información incluyendo una disposición sobre la acreditación de su cumplimiento y otra sobre la información a menores de edad. El Tercer Capítulo se refiere al acceso a datos por terceros tratando las relaciones entre el responsable de los servicios y la conservación de los datos por el encargado del tratamiento.

El Título III se dedica a los derechos de las personas y, en particular al ejercicio, otorgamiento y denegación de los derechos de acceso, rectificación, cancelación y oposición, que configuran las facultades que se desprenden del derecho fundamental a la protección de datos, como así lo reconoce la Sentencia 292/2000 del Tribunal Constitucional.

El Titulo IV se centra en cuestiones concretas aplicables a determinados ficheros de titularidad privada como los ficheros sobre solvencia patrimonial y crédito y los utilizados para actividades de publicidad y prospección comercial.

El Título V clarifica las obligaciones materiales y formales previas al tratamiento de los datos, donde destacan las medidas previstas para la creación, modificación o supresión de ficheros de titularidad pública (en correspondencia con el artículo 20 LOPD) y la notificación e inscripción de ficheros en general -públicos o privados- (artículo 26 LOPD).

El Título VI (artículos 33 y 34 LOPD) está íntegramente dedicado a las transferencias internacionales de datos diferenciando en su regulación entre

aquéllas que se destinan a países que proporcionen un nivel adecuado de protección y aquéllos que no lo proporcionen.

El Título VII (artículo 32 LOPD) está dedicado a los Códigos Tipo, instrumento llamado a jugar un papel relevante como dinamizador del derecho fundamental a la protección de datos. Se contemplan sus particulares características en relación a su objeto, naturaleza, contenido y compromisos adicionales, así como las garantías de cumplimiento o depósito o la publicación de los mismos.

El Título VIII tiene una especial importancia porque se refiere a las medidas de seguridad con la repercusión que ello tiene en la organización, gestión e inversión de las organizaciones que tratan datos personales como ocurre en el caso del sector asegurador. El Reglamento trata de ser particularmente riguroso en tres aspectos: en atribuir los niveles de seguridad, en la fijación de las medidas que corresponde adoptar en cada caso y en la revisión de las mismas cuando sea necesario.

Por otro lado, regula con detalle el contenido y las obligaciones vinculadas al documento de seguridad.

La pretensión de regular la materia de manera que aparezcan contempladas las diferentes formas de organización material y personal de la seguridad ha llevado al legislador a estructurar este Titulo en cuatro capítulos. El Capítulo I contempla cuestiones de carácter general sobre las medidas de seguridad que se aplicarán tanto a los ficheros automatizados como no automatizados y ya se trate del responsable del fichero o tratamiento como del encargado del tratamiento. El Capítulo II se centra en una cuestión tan controvertida a veces como es el documento de seguridad buscando recoger las diferentes formas de organización material y personal que se plantean en la práctica. El Capítulo III contempla las medidas de seguridad aplicables a los ficheros y tratamiento automatizados y el Capítulo IV a las medidas de seguridad aplicables a los ficheros y tratamientos estructurados no automatizados o manuales.

En cuanto a la implantación de las medidas de seguridad aparecen recogidas en las Disposiciones Transitorias si bien su ubicación en el texto ha variado en los diferentes borradores pasando a situarse en la última versión al inicio del texto. En cualquier caso en cuanto a sus previsiones, el Reglamento concede un plazo de un año desde su entrada en vigor para notificar a la AEPD las modificaciones necesarias en los códigos tipo inscritos.

El mismo plazo se exige para los ficheros automatizados que existan a la fecha de entrada en vigor del Reglamento y que lleven asociadas medidas de nivel medio (Entidades Gestoras y Servicios Comunes de la Seguridad Social y aquéllos que contengan datos de carácter personal que ofrezcan una definición de las características o personalidad de los ciudadanos y permitan evaluar aspectos de su personalidad).

En el caso de las medidas de nivel alto el plazo se amplía dieciocho meses más desde la fecha anterior.

Mención aparte merecen los ficheros no automatizados que existan en la fecha de entrada en vigor del Real Decreto.

En este caso, los plazos, a contar siempre desde la entrada en vigor del Reglamento, son los siguientes:

- Un año, para las medidas de nivel básico.
- Dieciocho meses para las de nivel medio.
- Dos años para las medidas de seguridad de nivel alto.

Para los ficheros automatizados y no automatizados que se creen con posterioridad a la vigencia del Reglamento se exige que cumplan desde el momento de su creación con todas las medidas de seguridad previstas en el mismo.

Llegamos al Título IX que regula los procedimientos que se tramitan ante la AEPD como son: el de tutela de los derechos, ejercicio de potestad sancionadora, inscripción o cancelación de ficheros, transferencias internacionales de datos y otros procedimientos como los que se refieren a la exención del deber de información al interesado o la autorización para la conservación de datos para fines históricos, estadísticos o científicos. En relación a los ficheros de titularidad pública se contemplan únicamente las peculiaridades que diferencian a los distintos procedimientos de las normas previstas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativos Común.

Novedades del Reglamento 1720/2007
de Desarrollo de la Ley 15/1999, de 13 de diciembre
de Protección de Datos de Carácter Personal

- **Deber de información:** procedimiento que acredite el cumplimiento del deber de información

- **Consentimiento del afectado:** forma de recabar el consentimiento/menores.

- **Cesión de datos:** no es necesario consentimiento:

  a) cuando lo autorice ley o norma comunitaria,
  b) cuando figuren en fuentes acceso público,
  c) cuando responda al desarrollo de relación jurídica,
  d) cuando el destinatario sea Defensor del Pueblo, Ministerio Fiscal, Jueces, Tribunales, Tribunal de Cuentas, Instituciones análogas autonómicas,
  e) entre Administraciones Públicas.

- **Tratamiento de datos por cuenta de terceros:** encargado del tratamiento/ subcontratación.

- **Transferencia internacional de datos:** Art. 70.4: Grupos de empresas: autorización Agencia para envío datos personales países que no proporcionen nivel adecuado de protección.

- **Aspecto organizativo**

  - Contenido, estructura y forma del documento de seguridad.
  - Seguimiento de los procedimientos de actualización de los Documentos de Seguridad.
  - Nuevas tipologías de datos: datos de menores, datos de tráfico, datos de víctimas de violencia doméstica.
  - Novedades en el procedimiento de atención de derechos del afectado.
  - Derecho de oposición.
  - Plazo de respuesta.
  - Funciones y obligaciones de los responsables de seguridad: obligaciones de verificación y control.
  - Inventario de ficheros manuales.
  - Homogeneización del control del cumplimiento de medidas para ficheros automatizados y no automatizados.
  - Designación de responsabilidades y obligaciones entre propietarios de la información y usuarios dentro de una misma entidad.

- **Aspectos técnicos**

  A. Ficheros automatizados

  - Informes de auditoría: comunicación de fecha y tipo de auditor
  - Registro de acceso para ficheros de nivel medio: ficheros corporativos del sector financiero y de seguros; gestión y auditoría de los ficheros *logs*
  - Copias de respaldo: Nuevo proceso de verificación
  - Cifrado de dispositivos portátiles: cómo controlarlo

  B. Ficheros no automatizados

  - Medidas de nivel básico: almacenamiento de información: mecanismos que obstaculicen la apertura de ficheros, inventario de ficheros, almacenamiento en lugares controlados.

  - Criterios de archivo: conservación, localización y consulta de información

  - Medidas de nivel medio: seguridad en locales: equipamientos necesarios; control de acceso físico; control de copias o reproducciones.

- **Implementación**

  - Objetivos principales y complementarios
  - Fases
  - Documentos

- **Sector asegurador**

  - Flujo de datos personales entre empresas mismo grupo
  - Requisitos legales tratamiento de datos de asegurados, beneficiarios, terceros involucrados
  - Papel de los corredores, mediadores, compañías de seguros y reaseguros, peritos, empresas subcontratadas.
  - Custodia
  - Medidas de seguridad para los ficheros automatizados y no automatizados.

<table>
<tr><th colspan="2">Cuadro de contenido – cuestiones a desarrollar en la Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y soluciones del Reglamento 1720/2007 de Desarrollo de la Ley Orgánica de Protección de Datos</th></tr>
<tr><th colspan="2">Calidad de los datos</th></tr>
<tr><td>Art. 4.5,3º Ley 15/1999

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.</td><td>Reglamento 1720/2007

Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos (arts. 153 y 154).</td></tr>
<tr><th colspan="2">Seguridad de los datos</th></tr>
<tr><td>Art. 9.2º Ley 15/1999

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas</td><td>Reglamento 1720/2007

Prohibición de registrar datos en ficheros que no cumplan las condiciones de seguridad que determina el Reglamento:

- Capítulo I. Disposiciones generales: funciones del encargado del tratamiento, prestaciones de servicios sin acceso a datos personales, delegación de autorizaciones y acceso a datos a través de redes de comunicaciones.
- Capítulo II. Documento de seguridad.
- Capítulo III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados.
- Capítulo IV. Medidas aplicables a ficheros y tratamiento no automatizados.</td></tr>
</table>

Art. 9.3 Ley 15/1999 *Reglamentariamente* se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley	*Reglamento 1720/2007* El Reglamento establece los requisitos y condiciones que tienen que cumplir los ficheros y personas que traten datos especialmente protegidos. (Título V y Título VII)
Art. 17.1 Ley 15/1999 Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos *reglamentariamente*	*Reglamento 1720/2007* Título IX, Capítulo II: instrucción del procedimiento ; duración del procedimiento y efectos falta resolución; ejecución resolución
Tutela de derechos	
Art. 18.1 Ley 15/1999 Las actuaciones contrarias a lo dispuesto en la presente ley pueden ser objeto de reclamación por los interesados ante la AEPD, en la forma que *reglamentariamente* se determine	*Reglamento 1720/2007* Título IX, Capítulo III, IV, V
Notificación e inscripción registral	
Art. 26.2 Ley 15/1999 Por vía *reglamentaria* se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros	*Reglamento 1720/2007* Capítulo II, Título V: notificación ficheros titularidad pública, notificación ficheros titularidad privada, tratamiento datos en distintos soportes, ficheros en que exista más de un responsable, notificación de modificaciones, modelos y soportes para la notificación, inscripción de los ficheros, cancelación de inscripción, rectificación errores, inscripción de oficio fichero titularidad pública, colaboración con las Autoridades de control de las Comunidades Autónomas. Capítulo VI Título IX. Inscripción códigos tipo.

Cuadro de contenido – cuestiones a desarrollar en la Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y soluciones del Reglamento 1720/2007 de Desarrollo de la Ley Orgánica de Protección de Datos

Censo promocional	
Art. 31.3 Ley 15/1999 Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán *reglamentariamente*. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios que así lo hayan solicitado	*Reglamento 1720/2007* Procedimiento para solicitar no aparecer en el censo promocional (art. 48)
Censo promocional	
Disposición Transitoria. 2ª Ley 15/1999 *Utilización censo promocional* Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de la puesta a disposición de sus solicitantes y del control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional	*Reglamento 1720/2007* No previsto en el Reglamento. El Reglamento que desarrolle el censo promocional (remisión a otro Reglamento futuro) deberá regular los procedimientos de formación, oposición a aparecer en el mismo, puesta a disposición para los solicitantes, control de las listas difundidas y plazo de puesta en operación

Códigos tipo	
Art. 32.3 Ley 15/1999 Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y *reglamentaria* sobre la materia, debiendo, en este caso, el Directos de la AEPD requerir los solicitantes para que efectúen las correcciones oportunas	*Reglamento 1720/2007* Denegación de la inscripción (art. 147) si no se cumple lo dispuesto en el Título VII . Requisitos inscripción. Título IX, Capítulo VI
Agencia Española de Protección de Datos	
Art. 35.1 Ley 15/1999 La AEPD 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. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será *aprobado por el Gobierno.*	*Reglamento 1720/2007* No se hace referencia en el Reglamento. Aprobado en 1993 por Real Decreto 428/1993, de 26 de marzo
Art. 37.1 b) Ley 15/1999 Emitir las autorizaciones previstas en la Ley o en sus disposiciones *reglamentarias*	*Reglamento 1720/2007* Emitir las autorizaciones previstas en los Reglamentos aplicables. Ej.: Título IX, Capítulo V: autorización de transferencias internacionales de datos; Título IX, Capítulo VII: autorización conservación datos fines históricos, estadísticos o científicos.

Cuadro de contenido – cuestiones a desarrollar en la Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y soluciones del Reglamento 1720/2007 de Desarrollo de la Ley Orgánica de Protección de Datos	
Agencia Española de Protección de Datos	
Art. 37.1 n) Ley 15/1999 Cuantas otras le sean atribuidas por normas legales o *reglamentarias*	*Reglamento 1720/2007* Otras funciones atribuidas por vía reglamentaria
Art. 37.2 Ley 15/1999 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	*Reglamento 1720/2007* Art. 114: la AEPD hará pública sus resoluciones, con excepción de las correspondientes al Registro General de Protección de Datos y de aquéllas que resuelvan la inscripción de códigos tipo..La publicación se realizará preferentemente mediante inserción en sitio web de la Agencia en el plazo de un mes desde publicación. La publicación se realizará aplicando los criterios de disociación de datos.
Art. 38 Ley 15/1999. Consejo Consultivo a) Un representante de los usuarios y consumidores, seleccionado del modo que se prevea *reglamentariamente*. b) Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule *reglamentariamente*. c) El funcionamiento del consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan	*Reglamento 1720/2007* a) No previsto en Reglamento. Real Decreto 42/1993, de 26 de marzo. Procedimiento para la designación de un representante de los usuarios y los consumidores. b) No previsto en Reglamento. Real Decreto 42/1993, de 26 de marzo. Procedimiento para la designación de un representante de los ficheros privados. c) No previsto en Reglamento. Real Decreto 42/1993, 26 de marzo.

Art. 39.3 Ley 15/1999 *Registro General de Protección de Datos* Por vía *reglamentaria* se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes	*Reglamento 1720/2007* Capítulo II, Título V: notificación ficheros titularidad pública, otificación ficheros titularidad privada, tratamiento datos en distintos soportes, ficheros en que exista más de un responsable, notificación de modificaciones, modelos y soportes para la notificación, inscripción de los ficheros, cancelación de inscripción, rectificación errores, inscripción de oficio fichero titularidad pública y colaboración con las Autoridades de control de las Comunidades Autónomas.
Infracciones graves	
Art. 44.3 d) Ley 15/1999 Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones *reglamentarias de desarrollo*, cuando no constituya infracción muy grave.	*Reglamento 1720/2007* Incumplimiento medidas seguridad previstas reglamentariamente: - Título IX, Capítulo III. Procedimiento sancionador - Título VIII, Capítulo III. Tratamientos automatizados - Capítulo IV. Tratamientos no automatizados.
Art. 44.3 h) Ley 15/1999 Mantener los ficheros, locales, programas o equipos que contengan datos de carácter persona l sin las debidas condiciones de seguridad que por vía *reglamentaria* se determinen.	*Reglamento 1720/2007* - Título VIII, Capítulo III. Tratamientos automatizados - Capítulo IV Ttratamientos no automatizados. - Título IX: Procedimientos tramitados ante la AEPD: .tutela de derechos, potestad sancionadora, inscripción o cancelación ficheros, transferencias internacionales, inscripción códigos tipo, exención deber información y autorización conservación datos con fines históricos, estadísticos o científicos.

Cuadro de contenido – cuestiones a desarrollar en la Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y soluciones del Reglamento 1720/2007 de Desarrollo de la Ley Orgánica de Protección de Datos	
Procedimiento sancionador	
Art. 48.1 Ley 15/1999 Por vía *reglamentaria* se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título	*Reglamento 1720/2007* Procedimiento sancionador: Título IX, Capítulo III

5. EL REGISTRO DE CONTRATOS DE SEGUROS DE COBERTURA DE FALLECIMIENTO

El 15 de noviembre de 2005 se publica en el Boletín Oficial del Estado la Ley 20/2005, de 14 de noviembre, sobre la creación del Registro de Contratos de Seguros de cobertura de fallecimiento, cuyo desarrollo se ha llevado a cabo mediante el Real Decreto 398/2007, de 23 de marzo.

Con estas dos normas se completa el marco necesario para el funcionamiento del citado registro y que supone un gran paso en el ámbito de la protección de derechos de los interesados y un esfuerzo añadido para las compañías aseguradoras.

La finalidad del Registro es suministrar la información necesaria para que pueda conocerse por los posibles interesados, y con la mayor brevedad posible, si una persona fallecida tenía contratado un seguro para caso de fallecimiento, así como la entidad aseguradora con la que lo hubiese suscrito, para permitir a los posibles beneficiario dirigirse a ésta y constatar si figuran como beneficiarios y, en su caso reclamar de la entidad aseguradora la prestación derivada del contrato (artículo 2).

Se trata, por tanto, de dar a conocer si una persona fallecida estaba asegurada con un seguro de cobertura de fallecimiento, ya que en muchas ocasiones por desconocimiento de los beneficiarios de estos seguros, se dejaban de percibir las cantidades correspondientes, y por lo tanto se veía frustrado el cobro de cantidades que legítimamente correspondían a determinadas personas.

Con ello se protege a los posibles beneficiarios de un contrato de este tipo de manera que cuando se produzca el fallecimiento, pueda dirigirse a la compañía aseguradora y reclamar los derechos económicos que le correspondan.

La naturaleza pública del registro permite que las personas interesadas que acrediten un interés legítimo puedan consultarlo y obtener un certificado en el que conste en qué contratos vigentes figuraba como asegurado el fallecido y con qué entidad aseguradora, dando, de este modo cumplimiento a la característica de publicidad del Registro que se le exige.

Entrando en el ámbito de aplicación, la Ley 20/2005 establece que las compañías aseguradoras deberán inscribir en el Registro los contratos de:

1. seguros de vida con cobertura de fallecimiento, y
2. seguros de accidentes en los que se cubra la contingencia de la muerte del asegurado.

Excluye, expresamente los siguientes contratos:

a. los seguros que instrumenten compromisos por pensiones de las empresas con los trabajadores y beneficiarios,
b. los seguros en los que, en caso de fallecimiento del asegurado, coincidan tomador y beneficiario,
c. los contratos suscritos por mutualidad de previsión social que actúen como instrumento de previsión social empresarial, mutualidades de profesionales colegiados y mutualidades cuyo objeto exclusivo sea otorgar prestaciones o subsidios de docencia o educación.

5.1. El Registro como fichero común

El Registro de Contratos de Seguros de cobertura de Fallecimiento se gestiona por el Registro General de Actos de Última Voluntad (en adelante RGAUV), dependiente de la Dirección General de los Registros y del Notariado (en adelante DGRN) del Ministerio de Justicia y tiene el carácter de un fichero común.

En este fichero se prevé tratar los siguientes datos (artículo 5.2 de la Ley 20/2005):

a) *Datos identificativos de la persona asegurada*

1º. Nombre y apellidos,
2º. Número del documento Nacional de Identidad, Número de Identificación Fiscal o número del documento acreditativo de identidad que en cada caso corresponda.

b) *Datos identificativos de la entidad aseguradora*

1º Denominación social
2º Domicilio
3º Clave administrativa con la que figura inscrita en el registro administrativo de entidades aseguradora y reaseguradota previsto en el texto refundido de la Ley de Ordenación y Supervisión de los Seguros Privados, aprobado por Real Decreto Legislativo 6/2004, de 29 de octubre, y en su normativa reglamentaria de desarrollo.
4º Código de Identificación Fiscal.

c) *Datos identificativos del contrato de seguro*

1º Número de contrato o referencia al Reglamento de Prestaciones de la Mutualidad de Previsión Social, en su caso.
2º Tipo de cobertura

En el sector asegurador existen otros ficheros similares a éste como los ficheros comunes que contienen datos personales para la liquidación de siniestros y la colaboración estadístico actuarial o los ficheros comunes para prevenir el fraude en el seguro[23]. También en este sentido, pueden citarse otros ficheros comunes como son los de prestación de servicios de información sobre solvencia patrimonial y crédito (fichero de morosidad), al amparo del artículo 29 LOPD, o la Central de Información de Riesgos que se regula en el artículo 60 de la Ley 44/2002, de 20 de noviembre, de reforma del sistema financiero.

Al ser un fichero común se parte de la coexistencia de dos ficheros:

El primero, el de la compañía aseguradora que trata los datos de los tomadores del seguro, del asegurado y de los beneficiarios del seguro, con objeto de incluirlos en la póliza del seguro, y que convierte a estas empresas en responsables del fichero, debiendo ajustarse en su creación a la normativa de protección de datos.

El segundo, es el fichero que se crea con la puesta en marcha del Registro de Contratos de Seguros de cobertura de Fallecimiento, y del que es responsable el RGAUV, en virtud de la Ley 20/2005. De este modo, las compañías aseguradoras se convierten en cedentes de datos y el responsable del fichero común (RGAUV) en cesionario de éstos.

Por tanto la creación de este fichero común plantea una serie de interrogantes tanto para las compañías aseguradoras, como entidades informantes de los datos, como para el Registro de Actos de Última Voluntad que es el responsable del fichero común.

Estos interrogantes se refieren tanto a la calidad de los datos como al ejercicio de los derechos, y más concretamente al derecho de acceso y la comunicación de los datos.

5.2. El derecho de acceso y rectificación

Por lo que se refiere al derecho de acceso al contenido del Registro, el artículo 6 de la Ley 20/2005 se refiere a las personas legitimadas como las únicas que pueden consultarlo con el fin de obtener información sobre si el causante tenía algún contrato vigente y con qué compañía.

Para poder realizar la consulta se debe aportar el certificado de defunción como se recoge en el apartado 2 del artículo 6 en los siguientes términos:

[23] Regulados en el artículo 25.4 del Real Decreto-Ley 6/2004, de 29 de octubre, por el que se aprueba del texto refundido de la Ley de Ordenación y Supervisión del Seguro Privado, en base a la redacción dada por la LOPD a la Ley de Ordenación y Supervisión de los Seguros Privados.

> “El acceso al Registro sólo podrá realizarse una vez fallecido el asegurado, previa acreditación de tal circunstancia, y siempre que hayan transcurrido quince días desde la fecha de defunción. A tal efecto, se presentará el correspondiente certificado de defunción”.

Con esta redacción el legislador deja claro que la consulta que puedan realizar los posibles beneficiarios se refiere a datos personales de una persona fallecida, con lo que ya no será de aplicación la LOPD. Ello no significa que no deba protegerse y garantizarse el derecho fundamental a la protección de datos de los asegurados que se entiende desde el momento en que una compañía aseguradora comunica los datos de un contrato de seguro hasta que se produce el fallecimiento del asegurado.

Por otro lado, conviene llamar la atención sobre el contenido del derecho de acceso de la Ley 20/2005 dado que su denominación puede llevar a error.

En efecto, el ejercicio del derecho tal como aparece recogido en la norma parece excluir al propio interesado de la posibilidad de solicitar información al responsable del fichero sobre los datos del Registro; sin embargo, el sentido es otro, puesto que el derecho de acceso regulado en esta ley se refiere en realidad al derecho a realizar una consulta por parte de las personas legitimadas, y, por tanto, el titular de los datos, haciendo uso de la LOPD conserva el derecho a solicitar y obtener gratuitamente información de sus datos, así como de las comunicaciones que se realicen o se prevean realizar de los mismos (art.15 LOPD).

De este modo, los asegurados podrán ejercitar este derecho ante la Dirección General de los Registros y del Notariado y no ante el Registro de contratos de seguros y cobertura de fallecimiento.

El ejercicio de este derecho podrá efectuarse en cualquier momento, siendo enteramente diferente del derecho de terceros a obtener certificación del contenido del Registro (art. 14 RD 398/2007, de 23 de marzo, por el que se desarrolla la Ley 20/2005).

Si como consecuencia del acceso el interesado comprueba que los datos son erróneos, inexactos o excesivos, el asegurado puede ejercer el derecho de rectificación y cancelación ante la entidad aseguradora, en su condición de responsable del tratamiento.

Por tanto el ejercicio de los derechos del interesado no se sustancia directamente ante el Registro como sería lo previsible sino que en el proceso intervienen otros dos órganos: La DGRN (de quien depende el RGUV, responsable del fichero) y la entidad aseguradora (responsable del tratamiento), lo que, previsiblemente, añadirá dificultad al proceso.

Si el interesado quiere ejercitar su derecho de acceso deberá dirigirse a la DGRN que, en el plazo de un mes, a contar desde la presentación de la solicitud, debe facilitarle la totalidad de los datos que se refieran a él y que consten en el Registro desglosándolos.

Si por el contrario, el titular quiere ejercer sus derechos de rectificación y cancelación deberá dirigirse a la entidad aseguradora directamente.

5.3. La comunicación de datos por las compañías aseguradoras

Con la Ley 20/2005, las compañías aseguradoras pasan a tener un nuevo papel como entidades informantes de los datos personales de los asegurados al fichero común. Ya no son sólo responsables de su fichero de clientes sino que, además, se convierten en cedentes de datos que se remiten al Registro de contratos de seguro de cobertura de fallecimiento. Ello lleva a plantear la necesidad de adecuar esta nueva función a la normativa sobre protección de datos.

En este sentido, las compañías aseguradoras deben verificar el cumplimiento de la normativa sobre protección de datos prestando especial atención a los siguientes extremos:

- Análisis del flujo lógico de la información en la entidad aseguradora para garantizar el cumplimiento de los principios de protección de datos.

- Información en el proceso de recogida de los datos sobre la base del art. 5 LOPD en conexión con el apartado 1 del art.5 de la Ley 20/2005:

  > " las entidades aseguradoras que celebren o hayan celebrado contratos de seguros a los que sea de aplicación esta Ley, y siempre que los mismos se encuentren vigentes, tienen el deber de comunicar al Registro General de Actos de Última voluntad, con la periodicidad y mediante el procedimiento que se determine reglamentariamente, los datos que se especifican en el apartado siguiente. Tales datos podrán ser objeto de tratamiento automatizado.
  >
  > Asimismo, las entidades aseguradoras deberán comunicar al Registro General de Actos de Última Voluntad, en los términos, con el contenido, en la forma y en los plazos que reglamentariamente se establezcan, que la prestación derivada de un determinado contrato que figura en el Registro ha sido satisfecha".

- Revisión de las notificaciones de las inscripciones de ficheros de clientes por las compañías aseguradoras. En efecto, la creación del Registro supone que las compañías aseguradoras deberán realizar una comunicación que en principio no estaba prevista, por lo que es necesario notificar esta

modificación al Registro General de Protección de Datos de la Agencia de Protección de Datos, señalando la cesión e indicando la Ley por la que se efectúa, que, por otro lado, excluye este supuesto de la necesidad de obtener el consentimiento del interesado.

La notificación de la modificación se puede llevar a cabo cumplimentando los formularios correspondientes en papel, o bien utilizar la opción telemática disponible en la web de la Agencia.

- Medidas de seguridad. El último extremo a tener en cuenta es la adopción de las medidas de seguridad que permitan cumplir el Reglamento de desarrollo de la LOPD. De nuevo hay que tener presente que las medidas deben aplicarse tanto al responsable del fichero a que da lugar la creación del Registro como a las compañías aseguradoras, como entidades informantes de los datos.

  En concreto, por lo que se refiere a éstas últimas deberán tener en cuenta si han implantado las correspondientes medidas de seguridad en el fichero de datos de carácter personal en los que se traten los datos de los asegurados que van a ser comunicados al Registro y, en su caso, revisar el contenido del documento de seguridad, respecto a la cesión o comunicación de datos.

En consecuencia, el volumen, (se calcula que existen más de 120 millones de pólizas frente a los 50 millones que declara el Registro) y la complejidad del trabajo que esto puede ocasionar para las empresas aseguradoras parece hacer aconsejable la creación de un nuevo fichero para el cumplimiento de esta nueva función, incluido un fichero histórico.

6. EL TEXTO REFUNDIDO DE LA LEY DE ORDENACIÓN Y SUPERVISIÓN DE LOS SEGUROS PRIVADOS Y EL REAL DECRETO 6/2004, DE 29 DE OCTUBRE

La Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados (en adelante LOSSP) se refería en su artículo 24.3 a la LORTAD (LO 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal) y establecía la notificación al afectado en caso de introducción de sus datos personales en los ficheros de las aseguradoras.

Este artículo introdujo la posibilidad de colaboración sectorial entre entidades aseguradoras para la prevención del fraude, exigiendo el consentimiento para el tratamiento de los datos personales del interesado, y remitiéndose al art. 28 de la LORTAD (prestación de servicios de información sobre solvencia patrimonial y crédito) para su regulación y funcionamiento:

> "… Las entidades aseguradoras podrán establecer ficheros de datos personales que permitan la colaboración estadístico-actuarial y la prevención del fraude en la selección de riesgos y en la liquidación de siniestros. Estos últimos se regularán de conformidad con lo dispuesto en el artículo 28 de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, por lo que será necesaria la notificación al afectado en la primera introducción de sus datos en el fichero pero no el consentimiento del mismo".

Esta redacción del artículo 24.3 de la LOSSP hacía prácticamente imposible aplicar dicho artículo por una incompatibilidad del contenido de los diferentes ficheros que se intentaban regular.

La casuística en la aplicación de este precepto dio lugar a un sinfín de interpretaciones que hizo necesaria la concreción de su alcance. Se aprovechó la modificación de la LORTAD de 1992 y su sustitución por la Ley Orgánica 15/1999 (en adelante LOPD) para introducir en su Disposición Adicional Sexta la necesidad de consentimiento expreso, limitando esta exigencia a los datos de salud. De este modo, la redacción del artículo 24.3 de la LOSSP pasó a ser la siguiente:

> "…Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del 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.
>
> También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quien sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.
>
> En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

Esta redacción se ha mantenido en el vigente Real Decreto 6/2004, de 29 de octubre, que se aprueba el Texto Refundido de la Ley de Ordenación y Supervisión de los Seguros Privados (en adelante TRLOSSP) y deroga la ley del 1995. De este modo, el TRLOSSP exige únicamente el consentimiento

expreso para el tratamiento por las aseguradoras de los datos de salud (párr. final del apartado 4 del art. 25 TRLOSSP).

Con ello parece haberse solucionado el problema permitiendo la posibilidad de crear por parte de las entidades aseguradoras ficheros comunes para la liquidación de siniestros y la "colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora".

En cuanto al control de la actividad aseguradora por parte de la Administración General del Estado (Ministerio de Economía y Hacienda) el TRLOSSP abre la posibilidad de utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos para el desarrollo de su actividad dentro del marco de la LOPD. De este modo, las entidades aseguradoras podrán relacionarse con el Ministerio de Economía y Hacienda a través de estos medios técnicos (art. 70).

También se refiere el texto a la emisión de documentos utilizando los medios anteriores reconociendo su calidad de documento original, siempre y cuando se garantice la autenticidad e integridad del mismo.

El tercer momento en la implantación de las nuevas tecnologías en las relaciones entre la Administración y las entidades aseguradoras se recoge en la posibilidad de tramitar procedimientos administrativos con soporte informático los cuales, en cualquier caso, deberán garantizar la confidencialidad y seguridad de los datos de carácter personal incluidos en ellos.

Es precisamente el respeto de los datos de carácter personal, en relación con la actividad aseguradora la que ha llevado a regular con detalle la aplicación de la LOPD en el marco de la mediación de seguros y reaseguros, que se analiza a continuación.

7. LA LEY 26/2006, DE MEDIACIÓN DEL SEGURO PRIVADO (LMSRP)

La aprobación en julio del 2006 de la Ley de Mediación del Seguro Privado (en adelante LMSRP) vino a culminar el proceso de incremento de garantías de los asegurados al extender al ámbito de los mediadores los requerimientos de la Ley Orgánica de Protección de Datos.

A través de esta Ley se han logrado clarificar aspectos esenciales relacionados con el tratamiento de datos personales en el sector asegurador. En la aprobación del texto definitivo se tuvieron especialmente en cuenta las

observaciones de la Agencia Española de Protección de Datos en su informe preceptivo, elaborado en relación con el Anteproyecto del Gobierno24.

En dicho informe se proponía introducir una sección específica dedicada expresamente a la protección de datos de carácter personal que regulara las principales cuestiones en esta materia, dada su incidencia en la actividad de los mediadores de seguros privados. De hecho la Agencia Española de Protección de Datos ha abierto numerosos expedientes por cesión inconsentida de datos en los que finalmente se condena a entidades de reaseguro por cesión de datos del cliente asegurador (a modo de ejemplo puede citarse la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 20 de junio de 2005 y de 28 de septiembre de 2005), así como a mediadores de seguros por contratar seguros sin consentimiento específico del cliente (ej.: Sentencias de la Audiencia Nacional de 22 de junio de 2005 y de 15 de febrero de 2006).

La LMSRP en sus artículos 62 y 63 aclara algunos de los aspectos más relevantes para los mediadores en materia de protección de datos de carácter personal, reservando la Disposición Adicional Novena al tratamiento de estos datos en el contrato de reaseguro.

Por otro lado, la necesidad de proteger los datos personales junto con la exigencia de un consentimiento específico por parte del interesado ha dado forma al nuevo párrafo segundo del artículo 21 de la Ley de Contratos de Seguros Privados, introducido por la Disposición Adicional Décima.

Los principales retos a los que a partir de ahora debe hacer frente la mediación son dos: la concienciación de que se está ante un Derecho Fundamental y el Deber de Información. La asunción de estos derechos facilitará en gran medida las obligaciones derivadas de la LOPD.

7.1. Los agentes de seguros como encargados del tratamiento

Artículo 62. Condición de responsable o encargado del tratamiento.

1”. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:

a) Los agentes de seguros exclusivos y los operadores de banca-seguros exclusivos tendrán la condición de encargados del tratamiento de la entidad aseguradora con la que hubieran celebrado el correspondiente contrato de agencia, en los términos previstos en esta Ley.

[24] La Agencia Española de Protección de Datos ha emitido informes para clarificar la situación de los mediadores de seguros ante la falta de una regulación específica en materia de protección de datos y la problemática que ello planteaba a este sector en el desarrollo de su actividad diaria.

Artículo 63. Otras normas de protección de datos.

2º. Los agentes de seguros y operadores de bancaseguros únicamente podrán tratar los datos de los interesados en los términos y con el alcance que se desprenda del contrato de agencia de seguros y siempre en nombre y por cuenta de la entidad aseguradora con la que hubieran celebrado el contrato".

La figura del encargado del tratamiento aparece definida en el artículo 3 de la LOPD, en su párrafo g) en los siguientes términos: 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. Más adelante, el art. 43 somete a éstos y a los responsables de los ficheros al régimen sancionador de la citada Ley.

En cumplimiento de la previsión legal la LMSRP en su art. 62.1, a) se refiere a los agentes de seguros exclusivos y a los operadores de banca-seguros exclusivos como encargados de los tratamientos en nombre y por cuenta de la entidad aseguradora, que se conceptúa como responsable del tratamiento o del fichero.

Partiendo de estos dos preceptos, y dejando al margen la especial responsabilidad y sujeción a control de la entidad aseguradora frente a la AEPD y frente al afectado o interesado, los encargados del tratamiento juegan un importante papel en el marco de la LOPD.

El contrato de agencia de seguros exclusivo debe incluir las obligaciones del encargado del tratamiento frente al sujeto afectado.

Así, en primer lugar, el interesado debe haber dado su consentimiento específico a la cesión de sus datos personales necesario para la contratación del seguro, más aún cuando se trate de datos relacionados con la salud, conforme al art. 7.3 LOPD.
En segundo lugar, el contrato tiene que incluir el deber de secreto previsto en el art. 10 LOPD que abarca la obligación de custodia y de no divulgación de los datos, incluso una vez finalizada la relación mercantil con el interesado25.

En este sentido, incumplirá dicha obligación el encargado del tratamiento que se apodere, difunda, ceda o revele papeles, cartas, mensajes de correo electrónico o cualquier otro documento del afectado sin su consentimiento. Asimismo la interceptación de las telecomunicaciones del cliente o la utilización de artificios técnicos de escucha, de transmisión, de grabación o de reproducción de sonido o de imagen, o cualquier otra señal de comunicación

[25] La obligación de *no descubrimiento ni revelación de secretos* se encuentra protegida penalmente en los arts. 197 a 201 del Código Penal, Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de octubre.

será sancionada con penas de prisión de tres a cinco años que podrán elevarse hasta 7 si los hechos se realizan con fines lucrativos.

A esto se añade una inhabilitación profesional por tiempo de dos a seis años para los profesionales que incumplan su obligación de custodia.

En tercer lugar, el encargado del tratamiento debe hacer posible el ejercicio por parte del interesado de los derechos de acceso, oposición, rectificación y cancelación en los términos de los arts. 15 a 18 LOPD.

Por último, el encargado del tratamiento debe indemnizar al interesado por el incumplimiento de su función (art. 19 LOPD), si bien es necesario matizar que esta responsabilidad tiene que ser asumida por la entidad aseguradora en función del criterio de imputabilidad previsto en el art. 18 LMSRP26.

7.2. Los agentes vinculados

Artículo 62. Condición de responsable o encargado del tratamiento

1. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:

   b) Los agentes de seguros vinculados y los operadores de banca-seguros vinculados tendrán la condición de encargados del tratamiento de las entidades aseguradoras con las que hubieran celebrado el correspondiente contrato de agencia, en los términos previstos en esta Ley.

      Cuando el cliente hubiera firmado un contrato de seguro, los agentes de seguros vinculados y los operadores de banca-seguros vinculados deberán tratar los datos del contrato de forma que únicamente puedan ser conocidos por la entidad aseguradora con la que se hubiera celebrado el contrato, sin que puedan tener acceso a dichos datos las restantes entidades aseguradoras por cuenta de las cuales actúen.

Al igual que los agentes exclusivos, los agentes vinculados son encargados del tratamiento por cuenta de la entidad aseguradora del cliente si bien en este caso se plantean situaciones de conflicto concurrencial por la

[26] Art. 18: "Sin perjuicio de la responsabilidad penal o de otra índole en que pudiera incurrir el agente de seguros exclusivo en el ejercicio de su actividad de mediación de seguros privados, serán imputadas a las entidades aseguradoras con las que hubiera celebrado un contrato de agencia de seguros la responsabilidad civil profesional derivada de su actuación y de sus auxiliares externos y las infracciones de la legislación sobre mediación en seguros privados que hubieran cometido".

coexistencia de distintas entidades aseguradoras, incluso competidoras en el mismo ramo de la actividad, con diferentes contratos de agencia y un único agente vinculado.

Ello plantea importantes cautelas para evitar situaciones de competencia desleal y problemas añadidos desde la perspectiva de la LOPD.

En el contrato que firme la aseguradora con el agente vinculado debe figurar el consentimiento expreso de la primera aceptando la concurrencia con todos los aseguradores que tienen el contrato de agencia con el agente vinculado.

Cosa distinta, es el acceso a los datos del cliente. Este tipo de relaciones requieren prestar una especial atención al tratamiento de los datos, de ahí que el apartado 1, b) del art.62 LMSRP consagre este deber de manera que únicamente puedan ser conocidos por la entidad aseguradora con la que se hubiera celebrado el contrato a fin de impedir que los datos de una entidad aseguradora puedan ser conocidos por el resto de las aseguradoras con las que tiene contrato de agencia el agente vinculado, con la excepción del consentimiento del cliente.

Las mismas obligaciones apuntadas respecto a los agentes exclusivos desde la perspectiva de la LOPD deben predicarse respecto a los vinculados y de hecho la LMSRP les hace responsables civiles por el defectuoso tratamiento de datos personales (art. 23), si bien con carácter solidario con el responsable del tratamiento o del fichero (la entidad aseguradora), para el que ha mediado el agente vinculado.

7.3. Los corredores de seguros y reaseguros como responsables del tratamiento

Artículo *62. Condición de responsable o encargado del tratamiento*

1. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: b) Los corredores de seguros y los corredores de reaseguros tendrán la condición de responsables del tratamiento respecto de los datos de las personas que acudan a ellos.

Artículo 63. Otras normas de protección de datos.

3. Los corredores de seguros podrán tratar los datos de las personas que se dirijan a ellos, sin necesidad de contar con su consentimiento:

   a) Antes de que aquéllos celebren el contrato de seguro, con las finalidades de ofrecerles el asesoramiento independiente, profesional e imparcial al que se refiere esta Ley y de facilitar dichos datos a la

entidad aseguradora o reaseguradora con la que fuese a celebrarse el correspondiente contrato.

b) Después de celebrado el contrato de seguro, exclusivamente para ofrecerles el asesoramiento independiente, profesional e imparcial al que se refiere esta Ley o a los fines previstos en su artículo 26.3.

Para la utilización y tratamiento de los datos para cualquier otra finalidad distinta de las establecidas en las dos letras anteriores, los corredores de seguros deberán contar con el consentimiento de los interesados.

4. Resuelto el contrato de seguro en cuya mediación hubiera intervenido un corredor de seguros o un corredor de reaseguros, éste deberá proceder a la cancelación de los datos, a menos que el interesado le hubiera autorizado el tratamiento de sus datos para otras finalidades y, en particular, para la celebración de un nuevo contrato. En todo caso, el corredor de seguros y el corredor de reaseguros no podrán facilitar los datos del interesado a otra entidad distinta de aquella con la que el interesado hubiera celebrado el contrato resuelto si no media su consentimiento inequívoco para ello".

La LMSRP equipara a los corredores de seguros y reaseguros y los hace responsables del tratamiento de datos personales, como parte del contrato de corretaje[27].

La actuación de los corredores de seguros puede poner en peligro la protección de datos personales como así puso de relieve la AEPD en el procedimiento PS 377/2005 que dio lugar a la resolución de 23 de mayo de 2006. En este caso se impuso una sanción de 300.000 euros a un corredor de seguros por infracción muy grave por contratar un seguro sin autorización del cliente. En el supuesto el corredor satisface una serie de primas a un asegurador por él elegido mientras que el cliente- asegurado continuaba con un asegurador anterior con el que el corredor había roto sus relaciones. Este ejemplo se ha convertido hoy en uno de los casos más repetidos de denuncias ante la AEPD por vulneración de la protección de datos y es consecuencia, en muchos casos, de las luchas de las aseguradoras por la fuga de clientes como consecuencia de la actuación de los corredores. El corredor de seguros es el único responsable frente al cliente cuando éste ve vulnerados los derechos reconocidos en la LOPD (art. 30 LMSRP).

[27] El legislador ha seguido en este punto la recomendación del Informe 433/2003 de la AEPD en el que se analizaba la actuación continuada del corredor de seguros. Del informe se desprende que es una hipótesis meramente teórica que una persona física acuda a un corredor de reaseguros en demanda de un contrato de reaseguro puesto que los clientes de los corredores de reaseguros son las entidades aseguradoras cedentes que buscan la cobertura de un asegurador por lo general no establecido en territorio español, ni tampoco en el Espacio Económico Europeo, dado que las reaseguradoras suelen utilizar paraísos fiscales para desarrollar su función financiera.

7.4. Los auxiliares externos

Artículo 62. Condición de responsable o encargado del tratamiento

1. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: Los auxiliares externos a los que se refiere el artículo 8 de esta Ley tendrán la condición de encargados del tratamiento de los agentes o corredores de seguros con los que hubieran celebrado el correspondiente contrato mercantil. En este caso, sólo podrán tratar los datos para los fines previstos en el apartado 1 de dicho artículo 8.

Los auxiliares externos tanto de los agentes exclusivos o vinculados como de los corredores de seguros y reaseguros cuando traten datos de carácter personal reciben la calificación de encargados del tratamiento en virtud del contrato mercantil de colaboración en el que se fijen sus funciones.

El apartado 1 del art. 62 LMSRP se refiere a los auxiliares, cuando no son mediadores de seguros en sentido estricto. Sus funciones se recogen en el art. 8 del mismo texto limitándose éstas a tareas de captación de clientela y funciones auxiliares de tramitación administrativa.En el contrato de agencia que vincule a los aseguradores con los Agentes exclusivos o vinculados se debe hacer referencia expresa a los auxiliares externos y a su actividad colaboradora (art. 62 LMSRP). En este sentido, y conforme al art. 12.1 LOPD, no se considerará comunicación de datos el acceso del auxiliar externo a los datos de carácter personales de que disponga el asegurador al ser éste necesario para la prestación del servicio al responsable del tratamiento (agente o corredor).

El auxiliar deberá formalizar el contrato de encargo incluyendo sus cláusulas y respetando los procedimientos de captación de información del asegurador al tiempo que se compromete a no utilizarlos para finalidades distintas al propio contrato de seguro, ni tampoco cederlos, ni comunicarlos, ni siquiera para su conservación por terceras personas. De este modo, en el contrato se hará constar por escrito o por otra forma que permita acreditar su celebración que el auxiliar, como encargado del tratamiento tratará los datos conforme a las instrucciones del agente o corredor, como responsables del tratamiento (art. 12.2 LOPD).

Una vez cumplida la prestación contractual, los datos de carácter personal serán devueltos al responsable, junto con cualquier documento o soporte en el que conste algún dato de carácter personal que haya sido objeto de tratamiento (art. 12.3 LOPD) de lo que se deduce el deber de custodia que se exige al auxiliar externo y por tanto su obligación de adoptar las medidas de seguridad oportunas.

2ª Parte
PROBLEMÁTICA JURÍDICA DE LA APLICACIÓN DE LAS TIC EN EL SECTOR ASEGURADOR EN MATERIA DE PROTECCIÓN DE DATOS

Capítulo III
LOS DESAFÍOS JURÍDICOS DE LA PROTECCIÓN DE DATOS PERSONALES EN LA PRESTACIÓN DE SERVICIOS ON-LINE EN EL SECTOR ASEGURADOR

SUMARIO: 1. PLANTEAMIENTO. 2. EL DERECHO A LA AUTODETERMINACION INFORMATIVA. 3. METODOLOGÍA: ESTUDIO SOBRE LA WEB DE LAS PRINCIPALES COMPAÑÍAS ASEGURADORAS. CUADRO. 4. MODELOS DE NEGOCIO UTILIZADOS EN EL ESTUDIO. 5. EL USUARIO. 5.1.- Planteamiento. 5.2. Recomendaciones al usuario/cliente. 6. RECOGIDA DE DATOS. 6.1.- Información. 6.2.- El consentimiento. 6.3. Formas de recogida de datos. 7. TRATAMIENTO DE DATOS. 7.1.- El Principio de calidad en la recogida de datos personales. 7.2.- Datos especialmente protegidos. 8. CESIÓN DE DATOS. 8.1.- Regulación. 8.2.- Excepciones. 8.3.- Consentimiento. 8.4.- La comunicación de la cesión de datos. 8.5.- Datos disociados. 9. PRESTACIÓN DE SERVICIOS. 10.- OBLIGACIONES DEL RESPONSABLE DEL FICHERO. 11. LA RESPONSABILIDAD EN EL TRATAMIENTO DE DATOS

1. PLANTEAMIENTO

En este apartado se analizan en profundidad las novedades en materia de protección de datos enumeradas en el Capítulo anterior de este trabajo con el objeto de dar respuesta a los problemas prácticos que plantea la nueva normativa reguladora al sector asegurador en el marco de las Tecnologías de la Información y las Comunicaciones.

Para el desarrollo del objetivo apuntado se estructura el esquema en dos grandes bloques temáticos en los que se trata, por un lado, la protección de datos de carácter personal (Capítulo III), reservando la segunda parte del trabajo a aspectos relacionados con la actividad aseguradora en el nuevo entorno digital: identidad de las partes, contratos y la prueba (Capítulos. IV, V y VI).

2. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

La conciliación del empleo de las TIC y el tratamiento de la información con el derecho de los ciudadanos a su intimidad y a la libertad de decidir sobre la

automatización y transmisión de sus datos de carácter personal se aprueba con la Ley Orgánica 15/1999, de Protección de Datos Personales.

El reconocimiento constitucional en Europa del derecho a la intimidad es reciente. Fue la Constitución Portuguesa de 1976 la primera que lo recogió en su artículo 35. Le sigue la Española de 1978, art.18 (" Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen").

En nuestro país tanto el Tribunal Supremo como el Constitucional se han ocupado del tema, interpretando el art. 18 y definiendo este derecho como: derecho a mantener intacta, incontaminada e inviolada la zona íntima, familiar o recoleta del hombre (STC, de 8 de marzo, de 1984) y recordando su estricta vinculación a la dignidad de la persona, reconocida en el art. 10 CE, lo que implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener la calidad mínima de la vida humana y reconociendo como facultad esencial de la intimidad, núcleo central de la personalidad, la facultad de exclusión de los demás, tanto en lo que se refiere a la captación de información sobre una persona como a la divulgación ilegítima de esos datos (STC 197/1991, de 17 de octubre; STC 20/1992, de 14 de febrero; STC 57/1994, de 28 de febrero; STC 207/1996, de 16 de diciembre). El Constitucional nos ha recordado que, en ocasiones el ámbito personal y familiar tiene proyección hacia el exterior[28] y, en todo caso, no abarca los hechos derivados de las relaciones sociales y profesionales (STC 142/1993, de 22 de abril).

En nuestro país la doctrina se halla dividida en torno a la naturaleza jurídica de este derecho. Mientras que unos autores, como MENDIZABAL ALLENDE, admiten el derecho a la autodeterminación informativa o libertad informática como nuevo derecho fundamental, otros sostienen que el derecho a la autodeterminación informativa no comporta la aparición de un nuevo derecho fundamental sino que se deriva de la necesidad de garantizar derechos fundamentales ya reconocidos, entre los que ocupa un lugar de privilegio el derecho a la intimidad aunque entendido de una forma distinta[29].

[28] STC 231/1988, de 2 de diciembre: “No cabe dudar de que, dentro de las pautas de nuestra cultura, las imágenes en las que se muestran los momentos en los que el torero es introducido en la enfermería y examinado por los médicos, reproduciendo de forma directa y claramente perceptible las heridas sufridas, la situación y reacción del herido y la manifestación de su estado anímico, inciden negativamente causando dolor y angustia en los familiares cercanos del fallecido, ...” ...”Ha de retrazarse que las escenas vividas dentro de la enfermería...formen parte del espectáculo taurino, y “por ende”, del ejercicio de la profesión del mismo, lo que haría que la grabación de esas imágenes y su exhibición no tuviesen el carácter de “intromisión ilegítima” en la intimidad de esa persona...pero en ningún caso pueden considerarse públicas y parte del espectáculo....”.

[29] SUÑÉ LLINÁS, Emilio en el vol. I de su Tratado de Derecho Informático, ya citado, pp. 416-417.

Esta es la postura mantenida, entre otros, por SUÑÉ LLINÁS que se muestra sorprendido ante tal derecho pues: "partiendo de una Constitución Española que desarrolla la libertad informática como trasunto de la intimidad, a la que se añade también el derecho al honor (art. 18), se ponga tanto empeño en crear nuevos Derechos Fundamentales que, o mucho me equivoco, o en la misma medida en que crezcan pierden, lógicamente, carácter fundamental.

En otras palabras, el hecho de que todos los derechos sean importantes y de que su contenido se vea alterado por circunstancias de dinámica social, no ha de implicar necesariamente una ampliación significativa del catálogo de Derechos Fundamentales, so pena de que dicho carácter de "fundamental" se diluya".

La configuración del derecho a la intimidad se ha ido perfilando, con las aportaciones de la jurisprudencia constitucional que parte del reconocimiento expreso de la no existencia de derechos absolutos (STC 11/1981, de 8 de abril o la STC 290/2000, de 30 de noviembre) y de la fijación de los límites, en base al texto constitucional, a sus leyes de desarrollo y a la interpretación jurisprudencia (STC 11/1981, de 8 de abril; 2/1982, de 29 de enero y 91/1983, de 7 de noviembre). Precisamente es tarea del Tribunal Constitucional tutelar aquellas zonas no consideradas expresamente en la Constitución para evitar que determinados intereses esenciales de los ciudadanos queden a la intemperie sin protección jurídica ninguna.

Es cierto que el reconocimiento expreso de nuevos derechos fundamentales ofrece en nuestro ordenamiento mayores dificultades que en otros, puesto que, como ha recordado MENDIZÁBAL ALLENDE, pese a que nuestra Ley Fundamental de 1978 no incluye una *cláusula abierta* que permita, como ocurre con la Constitución norteamericana, añadir nuevos derechos fundamentales[30], lo que no quiere decir que todos los plasmados en el texto constitucional sean los únicos existentes sino que los ciudadanos conservan otros derechos no enumerados que es necesario tutelar y corresponde a la jurisprudencia asumir la cobertura jurídica de esos derechos no escritos.
No obstante, debe reconocerse, siguiendo la postura del Convenio 108 del Consejo de Europa, un núcleo irreductible a ese derecho fundamental, que ha de respetarse para no alterar su contenido esencial. Esta ha sido la postura mantenida por el Tribunal Constitucional en Sentencias como la SSTC11/1981, de 8 de abril; 196/1987, de 11 de diciembre; 120/1990, de 27 de junio y 137/1990, de 19 de julio, debiéndose justificar las limitaciones en el fin

[30] Vid. MENDIZÁBAL ALLENDE, Rafael, en ob, cit, el autor se refiere a la Enmienda IX de la Constitución de EEUU, votada por el Congreso, el 25 de septiembre de 1789, en la que se señalaba que: "*la enumeración que se hace en esta Constitución no deberá interpretarse como denegación o menoscabo de otros derechos que conserva el pueblo"*, p. 20.

En la línea de la consideración de la lista de derechos fundamentales como *numerus apertus* se han manifestado otros autores como ORTI VALLEJO o ALVAREZ RICO, M en: *La Libertad informática como derecho fundamental,* Revista Sociedad y Utopía. Revista de Ciencias Sociales, nº 13. Mayo 1999.

perseguido, como declaran las SSTC 62/1982, de 15 de octubre; 13/1985, de 31 de enero; 57/1994, de 28 de febrero y 35/1996, de 11 de marzo) y existiendo una proporcionalidad entre "el sacrificio del derecho y la situación en la que se halla aquél a quien se le impone" (SSTC 37/1989, de 15 de febrero; 57/1994, de 28 de febrero; 35/1996, de 11 de marzo).

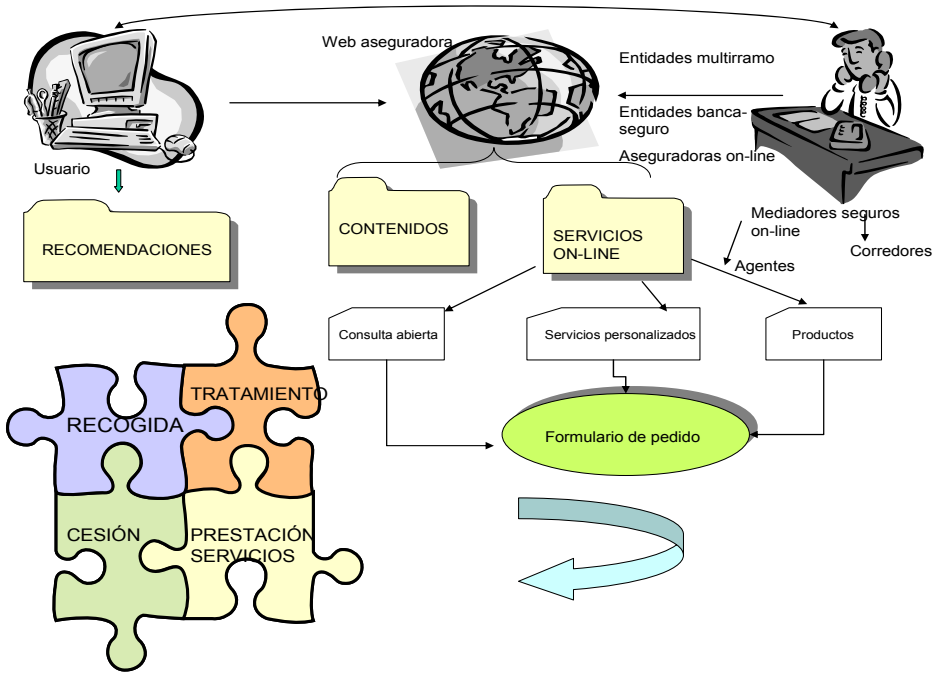
Todo lo anterior nos lleva a defender que existe un nuevo derecho a la libertad informática, deducible por vía interpretativa del propio texto constitucional, puesto que lo contrario supondría una tutela jurídica incompleta del ámbito del tratamiento automatizado de datos personales y que engloba no sólo el derecho a la intimidad sino otros derechos fundamentales como los recogidos en el artículo 20 de nuestra Constitución.

Junto a su consideración o no como derecho fundamental, uno de los problemas resueltos ha sido el del consenso internacional a la hora de hacer referencia a los derechos a proteger en el ámbito de las transferencias de datos personales en la Red.

En este sentido, la expresión utilizada en el marco de la Unión Europea para aludir a este conjunto de derechos es el de *privacidad* y este es el término que unifica la configuración del sistema de protección de los datos personales en el entorno de Internet.

En definitiva, estamos ante un nuevo derecho que faculta al interesado a decidir qué información quiere que sea conocida y cual no.

3. METODOLOGÍA: ESTUDIO SOBRE LA WEB DE LAS PRINCIPALES COMPAÑÍAS ASEGURADORAS



Fuente: elaboración propia

El comercio electrónico permite el uso de la información y de las tecnologías de la comunicación para orientar los negocios. Esto incluye el uso de Internet mediante todo tipo de herramientas de comunicación como el teléfono móvil, la televisión digital o las webs sites, entre otras.

En Internet el usuario decide donde quiere ir con un simple golpe de click, si no encuentra lo que busca se dirige hacia otro lugar, con lo que la competencia está a pocos segundos de distancia. En este sentido, este canal de comunicación abre una gran oportunidad para las entidades aseguradoras de estar en contacto con sus clientes pero hay que tener muy presente cuáles son las necesidades del cliente: acceso completo, información transparente, velocidad, seguridad, opciones, confidencialidad y precio competitivo.

El cliente debe poder acceder a los productos ofertados por la aseguradora desde cualquier lugar por lo que los puntos de contacto van cambiando por lo que en muchas ocasiones no es fácil de controlar por parte de las entidades aseguradoras.

Por otro lado, la actual evolución de Internet tiene un impacto directo en las operaciones que puede realizar el cliente, hasta el punto de llegar a

considerarlo como un co-productor que ayuda a mejorar la calidad de los servicios a éste y participa en su creación. De ahí que a largo plazo Internet esté llamada a convertirse en la herramienta más útil y eficiente para transmitir información lo que a su vez es crucial para las empresas.

En este sentido, los cambios para las entidades aseguradoras pasan por la reorientación de sus productos, por la organización de ventas y por la adaptación de sus sistemas de transferencia de información.

El planteamiento anterior explica los cambios que se están produciendo en el sector. Para analizarlos se va a utilizar el gráfico incluido al inicio de este epígrafe en el que, partiendo de un esquema sencillo, se intentan reproducir los posibles escenarios que pueden surgir en la nueva relación entre el cliente-usuario y los prestadores de servicios aseguradores on-line.

4. MODELOS DE NEGOCIO UTILIZADOS EN EL ESTUDIO

Internet está imponiendo nuevas formas de negocio en el sector asegurador y en este estudio se han utilizado los modelos más significativos en el mercado on-line, atendiendo a la siguiente clasificación:

a) **Entidades aseguradoras multirramo** (también denominadas asegura-radoras tradicionales). Con esta denominación se engloba a las compañías que operan fundamentalmente off-line. Todas cuentan con página web, si bien la utilizan mayoritariamente como canal de información. Se observa una evolución hacia los servicios on-line destinados a los mediadores y peritos.

b) **Entidades de banca-seguro**. Este modelo de negocio abarca a las entidades bancarias que junto a los servicios bancarios simultanean servicios aseguradores on-line cuya operativa está pensada para desarrollarse exclusivamente a través de la red.

c) **Los mediadores on-line** (brokers on-line o agentes). Son mediadores virtuales creados para funcionar en línea. Tienen las mismas características que cualquier aseguradora on-line pero adaptadas al negocio de la mediación de seguros.

d) **Aseguradoras on-line o de directo**. Son compañías que actúan exclusivamente a través de Internet, comercializando sus productos y servicios exclusivamente a través de la red.

De otro lado, y con objeto de acotar la muestra se recogen los resultados de las empresas aseguradoras que mejores resultados han obtenido en e-

business en el año 2006, utilizando los Informes de ICEA[31] y de Capgemini[32], publicados en septiembre y octubre de 2007, respectivamente.

El informe de la consultora Capgemini muestra una comparativa de websites del mercado asegurador español centrando la atención en los modelos de negocio y su funcionalidad. Frente a esto, la metodología utilizada por ICEA, que recoge los resultados de entidades aseguradoras con una cuota nacional de mercado del 53%, desglosa los resultados de acuerdo con el canal de venta mayoritario distinguiendo entre: mediadores on-line (agentes y corredores), instituciones financieras y venta directa.

Del informe de ICEA destacamos la cuota de mercado de cada modelo de negocio y las primas obtenidas en el Internet en 2006. La mayor cuota de negocio la ostentan los mediadores on-line (con una cuota de mercado del 33,84%), situándose el número de primas totales en miles de euros en 17.795.212, frente a los 7.258.604 obtenidos por las entidades financieras (cuota de mercado 13,80%) que se tomaron como muestra. La cuantía aún es menor en el caso de la venta directa (cuota de mercado de 5,14%), donde las primas totales en miles de euros no superaron los 3.000.000 de euros (2.702.107).

De los resultados anteriores se desprende que la mayor cuota de mercado sigue en manos de las entidades aseguradoras tradicionales (off line).

Los *mediadores on-line* analizados han sido: Segurosbroker, Puntoseguro y Lapoliza.com. Posicionándose en primer lugar Segurosbroker.

En general, las webs de estos mediadores destinan pocos recursos al diseño y focalizan la atención en las funciones de contratación, por lo que presentan una navegación muy sencilla y altos niveles de seguridad. Todas las webs analizadas cuentan con certificaciones externas que cumplen los requisitos de seguridad técnica y jurídica. De entre ellas destaca Segurosbroker que dispone de un servicio de Fechado Digital o "timestamping" prestado por la Fábrica Nacional de Moneda y Timbre.

Desde el punto de vista de los servicios, todas las webs incluyen cotizaciones para calcular presupuestos que pueden guardarse y asimismo pueden encontrarse herramientas que permiten realizar test comparativos; sin embargo, a pesar de facilitarse la contratación on-line no disponen de recursos para la reclamación de siniestros que deben tramitarse, en la mayoría de los casos, en la propia compañía aseguradora.

---

[31] *Las Tecnologías de la Información en el Sector Asegurador. Estadística año 2006.* Informe ICEA nº 1.034, septiembre 2007.

[32] *VII Informe del Sector Asegurador en Internet.* Capgemini, julio-septiembre 2006, publicado en octubre 2007.

Dentro de las *instituciones financieras* de nuestro país, los mejores resultados los ha obtenido e-bankinter, seguido de Bancaja, SCH-Seguros y BBVA.

En la mayoría de los casos estas webs forman parte de la institución bancaria a la que pertenecen y de ahí que en la navegación se produzcan intercambios entre ambas webs lo que dificulta su funcionamiento.

Desde el punto de vista técnico y de diseño, no hay diferencias significativas entre ellas y cuando la web de la aseguradora está integrada en la del banco los diseños son homogéneos.

De cara a los servicios que presta al cliente, se ha producido una rápida incorporación de los servicios de e-claims, que ha pasado en un solo año del 40% al 80% si bien no disponen, por la propia naturaleza del negocio, de servicios destinados a mediadores.

De las webs analizadas por Capgemini en el modelo de negocio de *venta directa* que en el 100% de los casos permite la contratación on-line (Direct Seguros, Línea Directa, Génesis y Fénix Directo), Línea Directa encabeza el ranking (55,8) marcando la diferencia los servicios que ofrece. El resto de entidades le siguen con alguna distancia y un estrecho margen entre ellas (entre el 48% y 43%).

Los aspectos técnicos y de diseño obtienen puntuaciones muy similares en todas ellas y el uso de certificaciones externas es general, cumpliendo en todos los casos los requisitos de seguridad técnica y jurídica.

En este grupo (venta directa) los criterios de negocio prevalecen sobre el diseño, todas las webs del sector tienen cotizadores para calcular presupuestos, siendo fácil encontrar herramientas que permiten realizar un test comparativo.

La totalidad de las webs de venta directa estudiadas permiten la contratación on-line de sus productos mediante procedimientos sencillos y guiados.

Por último, Capgemini incluye las entidades multirramo dentro de las nuevas formas de negocio del sector asegurador en el mercado on-line. Entre ellas destacan, como es ya tradicional, las webs del sector salud que aparecen en general como las mejor resueltas, con una alta calidad de realización y numerosas posibilidades. La entidades DKV, MAPFRE, Sanitas y Winterthur forman un grupo firmemente posicionado, sin grandes diferencias entre ellas y a considerable distancia del resto, en las que se observa la evolución tanto de los aspectos técnicos (para que la web resulte atractiva al cliente), como de negocio (con el fin de ampliar las funcionalidades de captación de negocio).

Frente a este grupo, el resto de entidades dan más importancia a los aspectos de negocio que a los de diseño, invirtiéndose más en la ampliación de funcionalidades (tarificadores, contratadores, e-claims,…).

5. EL USUARIO / CLIENTE

5.1. Planteamiento

El usuario/cliente que accede a la web de una compañía aseguradora persigue obtener información e interactuar con la compañía con el fin de dar respuesta a sus expectativas de servicio ahorrando tiempo.

Desde el punto de vista jurídico esto se articula a través del principio de participación del individuo que ampara, a su vez, una serie de derechos como son: el de obtener información de forma clara, precisa e inequívoca de la existencia del fichero automatizado de datos de carácter personal, el de conocer la finalidad de la recogida de los datos, las consecuencias de la obtención de los datos o de la negativa a suministrarlos, la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, así como conocer la identidad del responsable del fichero.

Entre todos ellos destaca el derecho de acceso sin el cual los demás no son efectivos ya que implica la condición previa para el ejercicio de los demás (cancelación o rectificación, por ejemplo). A pesar de ello, son pocas las normas nacionales que matizan el alcance de la expresión "derecho de acceso"[33].

En España, el derecho de acceso debe entenderse en sentido amplio, pues en caso contrario sólo alcanzaría a una operación técnica o mecánica tal como se describe en el art. 15.2 LOPD, precisándose, en los diferentes Reglamentos de desarrollo, el alcance de ese acceso[34]. En este sentido, el

[33] Así, la *Privacy Act* del Reino Unido de 1988, no excluye ningún dato del acceso, pero no considera datos personales "las indicaciones de las intenciones del usuario de los datos con respecto al individuo"; la ley noruega, por su parte, establece que el derecho de consulta no se aplica a los datos relativos a la salud. En Austria, y sólo en el sector privado, se permite únicamente que el interesado sea informado del origen de los datos y de los destinatarios en caso de cesión. RIGAUX, F: La protection de la vie privée à l'égard des données à caráctère personnel, en Annales de droit de Louvain, 1/1993.

[34] El RD 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LO 5/1992 (BOE de 21 de junio), precisa que la información que se diera al que ejerciese el derecho de acceso comprenderá "los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos". El Reglamento 994/1999, de 11 de junio, no aclara nada en relación a la información a facilitar en esos accesos pero si define que se ha de entender por acceso autorizado (autorización concedida a un usuario para la utilización de recursos) y por control

reciente Reglamento de desarrollo de la LOPD, de 21 de diciembre de 2007, especifica que el interesado tiene derecho a obtener información en relación a:

- si sus datos están siendo objeto de tratamiento,
- la finalidad del tratamiento,
- la información disponible sobre su origen,
- las comunicaciones realizadas o previstas.

El Reglamento recoge además la opción del interesado de solicitar información sobre datos concretos incluidos en el fichero o sobre la totalidad de sus datos sometidos a tratamiento.

La Directiva comunitaria (art. 12, *a)*) incluía en el acceso "el conocimiento de la lógica utilizada en los tratamientos automatizados referidos al interesado al menos en los casos de las decisiones automatizadas a las que se refiere el apartado 1 del artículo 15". En general, por tanto, las normas no distinguen sino que optan por prever el acceso a la información de carácter personal contenida en ficheros[35].

Para poder garantizar estos derechos se exige que conste claramente el nombre o razón social del responsable del fichero (art. 8.a) *del Convenio 108* [36]). Este requisito tiene su razón de ser en la diversidad normativa de los ordenamientos internos que se refieren a este principio.

En cuanto a quién debe facilitar la información sobre qué ficheros y qué tipo de datos personales existen sobre un sujeto concreto, se hace recaer esta función en el responsable del fichero, acogiendo en este sentido, la solución adoptada por la mayor parte de los Estados (art. 27.2 Real Decreto 1720/2007)[37].

Por su parte la Directiva 95/46/CE introdujo en su día dos importantes novedades respecto a la participación del interesado. La primera y esencial es el *consentimiento del interesado*. En este sentido, la Directiva definía este

---

de acceso (mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos).

[35] En este sentido la LOPD exceptúa del derecho de acceso a los datos sensibles registrados en los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado, a los registrados en ficheros de la Hacienda Pública y a aquellos otros en que así lo exija el interés público o intereses de terceros más dignos de protección (art. 23).

[36] Las Directrices de la OCDE se refieren a la identidad del responsable en su art. 12 (Principio de Transparencia). Por su parte la Directiva comunitaria, incluye este requisito entre la Condiciones generales para la licitud del tratamiento de datos personales (art. 10 *a). Información del interesado*).

[37] Una minoría atribuye esta competencia a una autoridad de tutela independiente del responsable del fichero.

concepto[38] para, a continuación, exigirlo[39] al interesado a fin de poder realizar un tratamiento automatizado de sus datos personales. La segunda novedad del texto comunitario ordenaba la notificación a terceros a los que se haya comunicado los datos, de aquellas rectificaciones, supresiones o bloqueos que se realicen, siempre y cuando no resulte imposible o desproporcionado.

5.2. Recomendaciones al usuario/cliente

A pesar de las previsiones legales enumeradas en el apartado anterior la complejidad de la casuística diaria llevó a la Agencia Española de Protección de Datos a elaborar un informe en el que se relacionaban las recomendaciones que el usuario debe tener presente en sus accesos a Internet a fin de salvaguardar su derecho a la intimidad como pieza fundamental para crear en el ciudadano "una cultura para la protección de datos en el nuevo entorno digital de la Sociedad de la Información" y en ello radica que cada persona pueda hacer un uso seguro de Internet.

Los riesgos para el usuario comienzan desde el momento que *navega por la Red* y son numerosos: desde las ventanas emergentes o "pop-up" que se abren automáticamente cuando se visitan determinadas páginas y que llevan aparejadas la instalación sin consentimiento de software malicioso hasta las propias operaciones de descarga de archivos que instalan software que persigue el borrado de datos o la ralentización del equipo, seguimiento de los sitios web que visita el usuario o el robo de contraseñas y datos personales.

Frente a esto, la **primera recomendación general** es asegurarse de la identidad del destinatario de los datos y facilitar únicamente los que sean estrictamente necesarios para la finalidad que se persigue. Esta primera regla debe aplicarse en ambas direcciones de la comunicación, debiendo la compañía aseguradora contar con un sistema seguro que garantice la identidad del cliente, si bien esto no añade demasiado si no se acompaña de **medidas concretas**.

Para ello, es aconsejable tener en cuenta lo siguiente:

---

[38] Art. 2. *"Definiciones.* A los efectos de la presente Directiva se entenderá por:
[…]
h) "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan".

[39] Art. 7. *Principios relativos a la legitimación del tratamiento de datos.*- Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:
a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato en que el interesado sea parte…, o
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, […]."

- Utilizar un software de antivirus y de seguridad específico con un navegador con opciones de seguridad más restrictivas y eficaces, configuradas por el propio usuario.

- Actualizar periódicamente el software prestando especial atención al sistema operativo, al software antivirus, al propio navegador y a las opciones de seguridad.

- La entrega y el intercambio de datos sólo deberá realizarse en aquellos sitios que tengan protocolos seguros y que respeten los principios de protección de datos, asegurándose que el sitio web cuenta con una política de privacidad que facilita información, como mínimo, sobre:

  - identidad del responsable,
  - dirección del responsable,
  - finalidad de los datos

- Debe protegerse el equipo por medio de una contraseña que restrinja el inicio de la sesión e impida a un tercero no autorizado acceder a el.

- Evitar acceder a los sitios webs utilizando como canal los enlaces incluidos en mensajes de correo electrónico o en sitios web de terceros.

- Para impedir la instalación de software malicioso deben activarse las utilidades que permiten el bloqueo de las ventanas emergentes.

- Borrar temporalmente los archivos temporales y las “cookies” o configurar el equipo para impedir el archivo de éstas.

- Antes de descargar archivos comprobar que la página cuenta con la acreditación suficiente (Ej.: *VeriSign* o productos similares).

- Cuando el equipo no es de uso personal es aconsejable desactivar las siguientes opciones:

  1. la opción que permite el archivo de contraseñas o guardar información relativa al inicio de las sesiones.
  2. la opción de los navegadores que posibilita mantener un historial de direcciones web, nombres de usuario y contraseñas con el fin de permitir su uso en la cumplimentación automática de formularios.

- Estar atentos a una posible instalación de software malicioso que se puede manifestar entre otros por los siguientes signos:

  1. Se ha producido un cambio en la página principal o en otros elementos de la configuración del navegador.
  2. Algunas páginas web no son accesibles.

3. Las ventanas emergentes aparecen intermitentemente.
4. Se han instalado nuevas barras de herramientas.
5. El equipo funciona con lentitud.

La **segunda recomendación general** se centra en el *correo electrónico*. Debe verificarse que el origen del mensaje proviene de una fuente de confianza y que disponemos de mecanismos de protección.

Pueden distinguirse tres tipos de riesgos en relación a la protección de los datos personales: recopilación de direcciones de correo electrónico[40], suplantación de la identidad y, como en el caso anterior, la instalación de software malicioso[41].

Hay que tener en cuenta que los servicios que permite el correo electrónico generalmente no contemplan el establecimiento de un canal que garantice la identidad del emisor y del receptor, ni siquiera mecanismos que aseguren la confidencialidad, por lo que debe sopesarse el riesgo de suplantación de la personalidad o la vulneración del secreto de las comunicaciones cuando se realiza una comunicación de información relevante o sensible a través de correo electrónico.

Las **medidas concretas** que deben adoptarse son:

- Utilizar código de usuario y contraseña para acceder al correo electrónico y cambiándolo periódicamente (al menos una vez al año).
- No utilizar la opción "guardar contraseña".
- Si no se quiere hacer pública una dirección de correo se debe configurar el navegado para que no la facilite a los servidores Web a los que se acceda.
- Tener presente que la dirección de correo electrónico y el resto de los datos proporcionados para ser incluidos en una directorio o lista de distribución son susceptibles de ser utilizados sin nuestro conocimiento para fines diferentes de aquellos para los que se suministraron.
- Cuando se envía un mensaje de correo a varios destinatarios se revela la dirección de los mismo que figura en los campos: "Destinatario" o "con copia" (CC) a todos los receptores del mensaje. Si quiere evitarse este

[40] Mediante los programas de *harvesting* ("cosecha") se recolectan direcciones de correo electrónico de la web que después son utilizadas para campañas publicitarias o para el envío masivo de comunicaciones, sin informar al titular de los datos. Idéntica finalidad tiene la técnica *hoax* o de cadena de mensajes que se añaden a cada comunicación si el receptor no se preocupa de borrar la cadena antes de reenviar la comunicación y que, posteriormente se utilizan para enviar mensajes de contenido engañoso, con el objeto de obtener direcciones de correo para un uso posterior.

[41] Los ficheros anexos pueden incluir software que esconde instrucciones para instalar programas nuevos o versiones modificadas. Tampoco es infrecuente la aparición de nuevos virus o gusanos a través del correo electrónico. Otro riesgo asociado es la difusión de mensajes de contenido engañoso o fraudulento para obtener información sensible de los usuarios.

extremo se pueden incluir los destinatarios del mensaje en el campo "con copia oculta" (CCO) de manera que ninguno de los receptores pueda acceder a la dirección de correo electrónico del resto de los destinatarios.
- Configurar el correo con el máximo nivel de protección posible y si se es usuario de un correo web optar por el proveedor que ofrezca como servicio un análisis de contenidos, además de configurar el navegador con el máximo nivel de seguridad posible.
- Mantener actualizados los programas cliente de correo electrónico, el navegador y el sistema operativo.
- No abrir los mensajes que ofrezcan dudas.
- Activar los filtros de correo no deseado.
- En la medida de lo posible no utilizar el correo electrónico proporcionado en el marco de una relación laboral para usos personales, dado que los mensajes de esas cuentas pueden ser monitorizados por las entidad responsable de los mismos y, en todo caso, solicitar información de las limitaciones de uso y de la posibilidad de monitorización de contenido del buzón de correo asociado.
- Evitar el envío de cadenas de mensajes.
- Cifrar el contenido de los mensajes para enviar por Internet documentos privados.
- Leer con detenimiento las condiciones de servicio del proveedor.

La **tercera recomendación** afecta a los *virus, gusanos*[42] *y ataques de ingeniería social*[43]*.* Los dos primeros entran dentro de la categoría de programas "malware" o software malicioso que se crean con intención de producir un daño o de recabar información de utilidad para aquellos que han creado el programa.

Por otro lado, en Internet también resulta una práctica habitual la utilización de técnicas de ingeniería social para recopilar información relevante de los usuarios para obtener algún tipo de beneficio, generalmente económico.

Si bien es cierto que la mayoría de estos ataques son detectados y rechazados por los servidores y entidades implicadas existe un "gap" de tiempo hasta que

[42] Programas diseñados para ser capaces de trasladarse a través de redes de computadores para realizar una actividad concreta que el código lleva incorporada. En principio su actividad no tiene peligro; sin embargo, estos programas pueden instalar también virus o programas que actúen en segundo plano sin que lo sepa el usuario o dirigirse a consumir el ancho de banda para realizar envío masivo de mails.

[43] Las práctica más conocidas de ingeniería social son el "phising" y el pharming". La primera suplanta la personalidad de un tercero de confianza y su principal objetivo ha sido hasta el momento obtener información de acceso de usuario de banca en Internet o sitios de subastas en los que es posible acceder a cuentas bancarias o tarjetas de crédito.
En pharming es una técnica más compleja desde el punto de vista técnico. Su objetivo es dirigir al usuario hacia un sitio web simulado.

se activa la protección en que el usuario o la entidad se encuentran desprotegidos, por lo que las **medidas concretas son:**

- No instalar software que no proceda de fuentes fiables.
- Actualizar periódicamente el sistema operativo y el antivirus, instalando cortafuegos y programas de detección y eliminación de software espía.
- Realizar periódicamente copias de seguridad.
- Rechazar los mensajes de correo que soliciten información sobre su identificación de usuario y palabras de paso.
- Adoptar sistemas adicionales de control de acceso a sitio web con información sensible como pueden ser tarjetas de coordenadas o dispositivos de generación de claves de acceso.
- Desconfiar de las ofertas que ofrezcan grandes beneficios en poco tiempo y con poco esfuerzo, dado que puede llevar aparejada la participación involuntaria en actividades tipificadas como delito.
- Comunicar al proveedor de servicios, al servicio al cliente de la entidad aseguradora, y a las Fuerzas y Cuerpos de Seguridad del Estado que se ha sido objeto de un ataque.

El **cuarto grupo de recomendaciones** afecta con carácter concreto al c*omercio y banca electrónica*. Internet se utiliza como canal de comunicación para la oferta de productos a través de portales de comercio electrónico que permiten su compra y venta. Para acceder a este servicio se suele solicitar el registro del usuario mediante su acreditación. En este momento es cuando pueden empezar los problemas para la entidad aseguradora a la hora de garantizarse que la persona que está contactando con ella es la que dice ser.

Frente a esto, las opciones son tres:

- la más generalizada es la de utilizar códigos de usuario y palabras de paso,

- si bien también es posible utilizar certificados digitales expedidos por la Fábrica Nacional de Moneda y Timbre, aunque esta opción no está operativa en las entidades aseguradoras analizadas, salvo en el modelo de negocio de banca-seguros, que aparece en las web de todas las entidades analizadas.

- El DNI electrónico se está abriendo paso con rapidez y es la tercera opción utilizada ya por la banca-seguros y que constituye otra opción segura de acreditación fehaciente de la identidad en Internet con la ventaja para el usuario de aparecer incorporado a un documento exigido en el comercio diario y para la actuación ante las Administraciones públicas, por lo que su tenencia no requiere un esfuerzo añadido para el usuario a diferencia de la opción anterior.

Las **medidas concretas** a tener en cuenta son:

- Navegar por portales conocidos.
- Utilizar, siempre que se ofrezca esta posibilidad, certificados digitales como medio para acreditar la identidad.
- Realizar los trámites desde un equipo libre de software malicioso.
- Comprobar que la dirección que figura en el navegador corresponde con el portal de la entidad a la que se quiere acceder.
- Nunca aportar datos personales si no se ha accedido a un entorno seguro (entorno seguro entre el navegador y el servidor al que se accede).
- Verificar queel certificado del sitio web al que hemos accedido ha sido emitido por la entidad (aseguradora, en su caso) a la que nos conectamos y por una Autoridad de Certificación que nos ofrezca confianza.
- Desconfiar de cualquier correo electrónico en el que se nos solicite información sobre nuestras claves.
- No utilizar las mismas contraseñas en los sistemas de autenticación de usuario para aquellos casos que requieran alta seguridad que para los que la seguridad sea baja.
- Cuando se utilicen certificados digitales, el titular de los mismos es el responsable de su custodia y conservación. En ningún caso, debe comunicarse a un tercero la clave privada de firma.[44]
- Si se utilizan certificados digitales almacenados en una tarjeta criptográfica no dejar ésta conectada al lector del ordenador. Cuando no sea necesario utilizar certificados se recomienda extraer la tarjeta.
- No dejar desatendido el ordenador mientras se está conectado y cuando se esté utilizando una conexión segura, para garantizar la seguridad se pueden utilizar protectores de pantalla con contraseña y activación de funciones de bloqueo del terminal.
- El acceso a las páginas de banca electrónica debe hacerse tecleando directamente la dirección en la barra de dirección del navegador.
- Para la compra on-line utilizar una tarjeta de crédito específica para esos fines y con un límite de gasto reducido.

La **quinta recomendación general** afecta a los *servicios de mensajería electrónica*[45] *y chats*. La principal diferencia entre unos y otros está en que mientras en los primeros la comunicación se establece entre dos personal, en los segundos la conversación se realiza en grupo.

Para un uso seguro de la *mensajería instantánea* hay que tener en cuenta lo siguiente:

[44] Si se sospecha que la clave privada está comprometida es recomendable solicitar inmediatamente la revocación a la Autoridad de Certificación, así como conoce la "Declaración de Prácticas de Certificación" de esa entidad certificadora.

[45] La mensajería instantánea es un sistema de comunicación similar al correo electrónico y más rápido. Los riesgos, por tanto, son similares a los del correo electrónico aunque con unos riesgos propios derivados del procedimiento de intercambio de mensajes.

- Para utilizar un programa de mensajería electrónica debe crearse un "*nick*", que equivale a una dirección de correo electrónico, para ello no proporcionar ni directa ni indirectamente información personal.
- Crear una barrera contra la mensajería instantánea no deseada, evitando que la dirección de correo electrónico aparezca en áreas públicas como directorios de Internet o perfiles de la comunidad en línea.
- No facilitar nunca información personal confidencial.
- Comunicarse únicamente con las personas que figuran en la lista de contactos o conocidos.
- No descargar archivos, ni vínculos de mensajes, ni abrir imágenes de remitentes desconocidos.
- Cuando se utilice un equipo público no seleccionar la característica de inicio de sesión automático puesto que los que usen el equipo después pueden ver el "nick" y utilizarlo para conectarse.

En cuanto a los chats:

- No enviar datos personales ni fotografías personales a salas de chats.
- En caso de introducir un apodo, no debe elegirse uno que revele la identidad personal.
- Antes de iniciar la conversación en línea consultar las políticas de privacidad y códigos de conducta del sitio del chat.

En la **sexta recomendación** se enmarcan los servicios *"peer to peer" (*también llamados P2P). Estos servicios permiten el intercambio de ficheros entre los dos extremos de la comunicación de manera que a la vez que se descargan se ponen a disposición del resto de la red la parte descargada sin necesidad de esperar a completar el fichero. Esta opción permite compartir cantidades enormes de información contenida en ficheros sin tener que depender de un único ordenador que almacene toda la información, puesto que se reparte entre todos los participantes tanto la carga de ancho de banda como de espacio en disco.

Para poder utilizar estas redes es preciso instalar un software en el ordenador que crea unos directorios en los que se almacenan los archivos descargados. La propia naturaleza de esta red precisa que se tengan en cuenta las siguientes recomendaciones:

- Mantener actualizado el software.
- Para poder utilizar las redes "P2P" es imprescindible instalar un programa, por lo que se recomienda hacerlo siempre de sitios reconocidos y, para mayor seguridad, de la página del creador del programa.
- Limitar el acceso a las direcciones IP de la red interna, estableciendo un puerto no estándar, por encima de 1024.
- Cuando se procede a la instalación automática del programa es aconsejable, con carácter previo, realizar una copia del estado del sistema,

con el fin de comprobar, una vez instalado el software, que sólo se ha instalado en que queremos. Esto se debe a que en muchos casos, los clientes más conocidos instalan a la vez software malicioso que rastrea nuestras conexiones.

- Los programas clientes continúan ejecutándose continuamente y cuando el ordenador está las 24 horas del día conectado, aumentan exponencialmente los riesgos por lo que es conveniente instalar un cortafuegos que limite el acceso a los puertos del equipo.
- Valorar los riesgos que supone instalar un servidor puesto que esto supone la publicación de la dirección IP, por lo que los demás miembros de la red conocerán dónde está el equipo y qué software tiene, sin que ello suponga una descarga más rápida de ficheros pero si un incremento espectacular del consumo del ancho de banda.
- Dado que al instalar el programa "P2P" se comparte una parte del disco duro de modo que toda la información que allí se deposite será también accesible por terceros, es aconsejable que el directorio que se va a compartir esté en una partición distinta de las del Sistema Operativo, si bien es preferible que se instale en un disco distinto.
- En aquellas redes en que sea necesario utilizar un nombre de usuario es mejor utilizar un pseudónimo que no sirva para la identificación personal.
- Los ficheros pueden contener información diferente a la que dicen contener, por lo que es preferible no descargar ficheros ejecutables o que puedan incluir software malicioso, por ejemplo, las macros de los documentos de texto.
- Limitar las conexiones a los puertos conocidos.

La **última recomendación** es para la *telefonía IP (VoIP)*[46]. Este servicio se utiliza por las empresas de telefonía que transmiten un gran volumen de llamadas. Los particulares lo utilizan a través de ordenadores conectados entre sí mediante redes "P2P", si bien la generalización de la banda ancha ha permitido el uso de aparatos similares a los teléfonos y con un número asignado.

El principal problema de este servicio deriva de su definición como telefonía. De hecho la Comisión del Mercado de las Telecomunicaciones lo ha diferenciado de la telefonía tradicional y de ahí que no se le aplique la regulación sobre servicios telefónicos. Este servicio ofrece un gran número de ventajas. Desde la movilidad de los que participan en la comunicación a la utilización del mismo número de teléfono con independencia de la ubicación física del usuario.

En este nuevo contexto, usuarios y entidades aseguradoras deben tener en cuenta las siguientes recomendaciones:

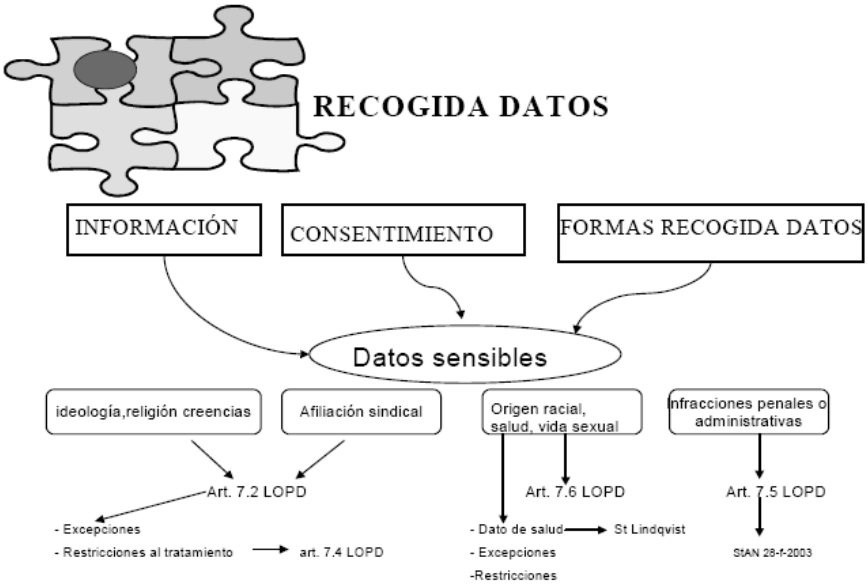
[46] Servicio de llamadas a través de Internet utilizando el protocolo IP. El sistema transmite llamadas de voz de manera similar al envío de correos electrónicos. Convierten la voz en paquetes de datos con el fin de transmitirlos como cualquier otra información.

- Utilizar en la comunicación una encriptación fuerte.
- Mantener actualizado el software del programa de telefonía IP.
- Si se acceder al sistema VoIP desde un ordenador de uso público es aconsejable eliminar todas las pruebas de uso, especialmente la información relativa al acceso al sistema, así como los ficheros temporales que puedan queda grabados.
- Algunos programas de VoIP permiten transmitir imágenes, por lo que, en caso de conectar una cámara al sistema VoIP debe asegurarse que sólo se transmiten las imágenes que se quiere transmitir. Hay que recordar que la imagen es también un dato de carácter personal.
- Algunos programas de VoIP permiten transmitir ficheros, por lo que es conveniente tener cuidado con los datos así obtenidos, vigilando que no contienen virus o software malicioso.
- Las llamadas no dependen de la localización física de la persona que llama, incluso el número que aparece en pantalla como el que, posteriormente, se refleja en la factura no tienen por qué coincidir con la persona que ha hecho la llamada, con los riesgos añadidos que eso supone para garantizar la identidad del que realiza la llamada.
- Por último, hay que tener en cuenta que el acceso a VoIP a través de conexiones inalámbricas añade a los riesgos anteriores los propios de estas redes como son: la interceptación de los paquetes mediante escuchas no autorizadas, un uso excesivo del ancho de banda, etc.

A pesar de la minuciosidad de todas estas recomendaciones, la efectividad de las operaciones que el usuario o las entidades aseguradoras realizan en red, obliga a minimizar el tiempo de puesta en práctica de todas ellas, en aras a la efectividad de la comunicación. Algunas de las recomendaciones analizadas resultan excesivas para el usuario y lo aconsejable es que, éste, desde el momento que contrata con un proveedor de servicios de Internet solicite la cobertura máxima de la seguridad de sus datos, trasladando, de este modo, a un tercero, esta tarea que, por otro lado, en muchos casos, escapa al conocimiento técnico del usuario medio.

Por lo que se refiere a las entidades aseguradoras, estas recomendaciones aparecen integradas en sus sistemas de seguridad técnica contando todas ellas con departamentos informáticos que trabajan diariamente por garantizar la máxima seguridad de las comunicaciones con sus clientes.

6. RECOGIDA DE DATOS



Fuente: elaboración propia

La legitimidad en la recogida de datos aparece recogida por primera vez en un texto de Naciones Unidas[47]. Diez años después, la OCDE se refiere a la justificación social en sus Directrices de 1980, y concretamente, en su apartado 7º exige que la recogida de datos de carácter personal se debe realizar por medios legítimos y leales, si bien el apartado 4º limita esta declaración excluyendo de su aplicación aquellos datos relacionados con la soberanía, la seguridad nacional y el orden público, que en cualquier caso, deberán ser los menos posibles

También el Consejo de Europa, en el Convenio 108, reconoce la justificación social que ha de regir la recolección y uso de datos personales en su artículo 5, al establecer que los datos de carácter personal que sean objeto de un tratamiento automatizado se obtendrán, tratarán y registrarán leal y legítimamente. Si bien se exceptúan los casos en que ese tratamiento constituya una medida necesaria en una sociedad democrática para la

[47] Naciones Unidas consagra con carácter general el principio de justificación social en sus *Principios rectores aplicables a los ficheros computerizados de datos personales* al señalar que todas las informaciones que se recaben relativas a las personas deben adecuarse a procedimientos leales y lícitos y, en cualquier caso no deben utilizarse para fines contrarios a los propósitos y principios de la Carta de San Francisco. Versión española de la versión revisada, aprobada por Resolución 45/95, de 14 de diciembre, de la Asamblea General de las Naciones Unidas (documento E/CN.4/1990/72, 20 de febrero de 1990).

represión de infracciones penales y para la protección de la persona concernida y de los derechos y libertades de otras personas (art. 9).

En el ámbito de la Unión Europea, la Directiva 95/46/CE[48], comienza recogiendo el principio de justificación social en el considerando 28, donde se refiere al tratamiento de datos personales de manera lícita y leal, y posteriormente, en el artículo 6, concreta el órgano sobre el que recae la competencia de velar que así sea, competencia que se reconoce a los Estados individualmente.

Se trata, por tanto, de un principio reconocido por todos de manera unánime, que sustenta el entramado que configura las normas de contenido de ámbito interno, cuyo nivel de aplicación recae en los propios Estados firmantes.

Lo primero que llama la atención de la LOPD es la falta de exigencia de consentimiento para el tratamiento y la cesión de los datos personales necesarios en las relaciones precontractuales. De ahí, que los sistemas de *(credit*) *scoring* se utilicen mayoritariamente para el cálculo del riesgo de una operación, para la contratación de pólizas o para la concesión de créditos. Estas técnicas implican, en la mayoría de los casos, el establecimiento de un perfil del interesado buscando automatizar la toma de decisiones sobre la concesión o no de la operación y con la finalidad de prevenir una posible pérdida económica como consecuencia de un incumplimiento del cliente.

La excepción de no requerir el consentimiento del interesado no supone, no obstante, que se obvie el cumplimiento del principio de información. Por ello en la fase de negociación resulta esencial analizar cómo se cumplen los principios de calidad de datos, prestando especial atención a la cancelación de los datos personales tratados, el principio de información y el consentimiento en la recogida y elaboración de perfiles, en su caso.

El nuevo Reglamento resulta ilustrativo en este punto puesto que a partir del 20 de abril de 2008, el responsable del fichero tiene la obligación de cancelar los datos de aquellas operaciones que no se hayan concedido y no utilizarlos para operaciones posteriores si no cuentan con la previa autorización de la Agencia de Protección de Datos.

De esta manera se intenta poner fin a la práctica habitual de la conservación de estos ficheros (de datos personales) en situación de bloqueados, pero no borrados, que permitía al responsable habilitarlos en cualquier momento para poder reutilizarlos según las necesidades.

Esto puede plantear problemas a la hora de cumplir con la obligación establecida en la propia LOPD de mantener esos ficheros por un plazo de

[48] Transpuesta a nuestro Derecho interno por la Ley 15/1999, de 13 de diciembre, de Protección de Datos Personales.

cinco años, período tras el cual prescribe la responsabilidad legal del responsable del fichero (art. 22.2 RD 1720/2007).

La novedad que introduce el Reglamento es, por tanto, la de no desbloquear el fichero sin la previa autorización de la Agencia, aclarando qué se entiende por cancelar los datos.

La cancelación supone el bloqueo de los datos reservando los mismos e impidiendo su tratamiento, excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales. Trascurrido el plazo se debe proceder a la supresión definitiva de esos datos.

6.1. Información

A. Marco normativo

Como tal principio aparece enunciado en las Directrices de la OCDE en el sentido de disponer con facilidad de los medios que permitan conocer la existencia y naturaleza de ficheros que contengan este tipo de datos, su finalidad, el responsable del fichero y el lugar habitual en que se realiza la actividad. Lo que predicaba, por tanto, la OCDE en 1980 era el derecho de obtener información sobre los datos personales, que a su vez debía plasmarse en una norma general de transparencia respecto a las novedades y prácticas que fueran apareciendo en este ámbito[49].

[49] La ONU por su parte, limita, en sus Principios rectores aplicables a los ficheros computerizados de datos personales, el principio de transparencia acotándolo en torno al derecho del interesado a saber si se está procesando información sobre él y a obtener rectificaciones o supresiones.

La misma vía de solución acogen el Consejo de Europa y la Unión Europea. El primero se refiere a las garantías complementarias que se reconocen a la persona *concernida*, como son el derecho a conocer la existencia de un fichero automatizado de datos de carácter personal, su finalidad, el responsable y la sede de la autoridad que controla el fichero, lo que coincide con la cláusula introducida por la OCDE en sus Directrices. El Convenio 108 amplía el elenco de garantías del interesado reconociendo entre otras facultades: la de obtener en tiempo razonable la confirmación de la existencia o no de un fichero de este tipo, la de, en su caso, pedir la rectificación o eliminación de los mismos, e incluso la de disponer de un recurso para el caso de que las anteriores peticiones no sean atendidas o lo sean en un modo que no satisfaga al interesado. Se exceptúa de este tratamiento transparente aquellos datos que se refieran a la seguridad del Estado, a la seguridad pública, a los intereses monetarios, a la represión de infracciones penales y a la protección del interesado o de los derechos y libertades de terceros más dignos de protección. Asimismo, el Convenio contiene una restricción bajo forma de ley que podrá limitar la información sobre estos datos cuando se utilicen con fines estadísticos y científicos, siempre y cuando no exista riesgo de vulnerar la vida privada de las personas afectadas.

Para la UE[50] la transparencia implica el deber de informar a los interesados sobre el objetivo del tratamiento y la identidad del responsable en un tercer país con dos únicas excepciones. La primera se refiere a los datos que no se han recabado del propio interesado. En este caso la información se facilitará al interesado si es posible, salvo que ello suponga esfuerzos "desproporcionados o si el registro o la comunicación de los datos están expresamente exigidos en la ley" (art. 11.2). La segunda alude a la seguridad del Estado, y se refiere a actuaciones penales, a supuestos en que se vean afectados intereses económicos y financieros de importancia (art. 13).

El principio de información se recoge en el artículo 5 de la LOPD que señala:

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 de 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 le sean planteadas.
c) De las consecuencias jurídicas de la obtención de los datos o de la ne-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.

La jurisprudencia ha ido interpretando el alcance de este artículo en sentido restrictivo insistiendo en la obligación de informar al interesado incluso en el caso de que éste ofrezca voluntariamente sus datos y conozca la finalidad para la que van a ser utilizados[51].

Además no basta con la simple existencia de consentimiento sino que éste debe ser informado; esto es, no sólo legal sino leal[52].

Por lo que afecta a la finalidad, la información que se de al titular de los datos no puede ser genérica, utilizando fórmulas como: “proporcionar mejores servicios al cliente”, sino que debe especificarse para qué se van a utilizar y quienes van a ser sus destinatarios[53].

---

[50] Directiva 95/46/CEE cit.

[51] Sentencia de 31 de enero de 2003, de la Audiencia Nacional, núm. Rec. 3290/2001, caso “Gran Hermano”.

[52] St. Audiencia Nacional, 13 de septiembre de 2002, núm. Rec. 1065/1999.

[53] St. Audiencia Nacional de 11 de abril de 2005, recogida en la Memoria de la Agencia Española de Protección de Datos del año 2006, contra un operador de telecomunicaciones

Por su parte, el nuevo Reglamento de Protección de Datos exige que el cumplimiento se lleve a cabo a través de un medio que permita acreditarlo, debiendo conservarse esta acreditación por parte del responsable del tratamiento mientras persista el tratamiento de los datos del afectado.

Esta novedad supone una dificultad añadida para la entidad aseguradora que recaba datos personales y la obliga a modificar la gestión de esta operación con el fin de conservar la prueba que demuestra que se ha dado cumplimiento al Reglamento. Para ello puede utilizar medios informáticos o telemáticos, en concreto el escaneado de la documentación en soporte papel, siempre que se pueda garantizar que no se han alterado los soportes originales.

B. Aplicación de la normativa sobre protección de datos

De la letra del artículo 5 de la LOPD se desprende que cualquier entidad aseguradora que, en cumplimiento de sus funciones, recoja y trate datos de carácter personal debe informar previamente al interesado de todos los requisitos enumerados, recayendo la carga de la prueba de su cumplimiento en el responsable del tratamiento. Cuando, además, se utilicen cuestionarios u otros impresos para la recogida, deben figurar en los mismos, en forma legible todos los requisitos enumerados más arriba (art. 5.3).

La cláusula general es completada a lo largo del articulado de la ley en el sentido de prohibir el uso de los datos para finalidades incompatibles (art. 4.2) y declarando nulo el consentimiento cuando se cedan datos sin permitir al interesado conocer el uso a que se destinarán los datos o el tipo de actividad del cesionario (art. 11.3).

Los apartados b) y c) deben ponerse en relación con el artículo 4.1 que establece que sólo podrán recogerse y someterse a tratamiento los datos de carácter personal cuando sean *adecuados, pertinentes y no excesivos*.

En este sentido la Agencia de Protección de Datos en su Memoria del año 2002 señala en relación al artículo 5:

> "….En las citadas condiciones generales se establecía que los datos personales que se recababan en un apartado concreto del contrato tienen el carácter de opcionales, informándose de las consecuencias que se aplicarían en caso de que dichos datos no fuesen aportados. La deficiencia radicaba en que el apartado concreto de datos opcionales que se indicaba en las condiciones generales no tenía correspondencia

---

que había enviado una carta no personalizada a sus cliente en relación al cumplimiento del deber de información y cesión a empresas del grupo para la oferta de productos y servicios, pero omitiendo el dato esencial relativo a la finalidad de la incorporación de los datos y a los destinatarios de los mismos utilizando la fórmula genérica: "*proporcionarles los mejores servicios*".

alguna en el contrato. Esta situación, que ya había sido detectada anteriormente y que motivó en su día que el Director de la Agencia instara al citado operador para que la subsanara, seguía persistiendo, siente este hecho constitutivo de una infracción del artículo 5.1 de la LOPD".

La identidad y dirección del responsable del tratamiento a que se refiere el apartado e) no resulta tan obvia como en un principio pudiera parecer, más aún en grupos empresariales donde convergen diferentes figuras como: el proveedor de acceso, los proveedores de contenido, los vendedores on-line (mediadores en nuestro caso), la entidades multirramo, la banca-seguro, o las aseguradoras on-line.

Además, el uso de nombres comerciales o marcas puede confundir al interesado en lo que se refiere al conocimiento de la empresa que efectúa el tratamiento.

Con todo, el artículo 5.3 de la LOPD recoge una excepción al cumplimiento de los requisitos generales de manera que no será necesaria la información a que se refieren las letras b), c) y d) si el contenido de ellas se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Otra cosa es que los datos de carácter personal no se recaben directamente del interesado. En este caso, el responsable del fichero debe informarle de forma precisa, expresa e inequívoca, dentro del plazo de tres meses siguientes al registro de los datos.

No obstante, lo anterior no será de aplicación:

1. Cuando así lo prevea expresamente una ley,
2. Cuando el tratamiento tenga fines históricos, estadísticos o científicos,
3. Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos u organismo autónomo correspondiente, en atención al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
4. Cuando los datos procedan de fuentes accesibles al público y se destinen a publicidad o prospección comercial, si bien en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de su derechos.

Pero, ¿qué se ha de entender por datos históricos con fines científicos o de investigación? y, ¿cuándo los esfuerzos se consideran desproporcionados a efectos de la LOPD?.

Los datos históricos con fines científicos o de investigación se delimitan sobre la base de la Ley 16/1985, de 25 de junio, reguladora del Patrimonio Histórico Español que establece que "los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de 25 años desde sus muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos". Por tanto, siempre que se cumplan los requisitos de plazo es posible tratar los datos personales, incluida la divulgación. En caso contrario, es necesario recabar el consentimiento de los afectados[54].

El incumplimiento del deber de información cuando los datos se recogen directamente del interesado lleva aparejada una multa leve de ente 601.01 a 60.101,22 euros.

En cuanto al carácter desproporcionado de los esfuerzos que eximen del cumplimento del artículo 5 de la Ley debe apreciarse por la propia Agencia Estatal de Protección de datos mediante un procedimiento a solicitud del interesado.

Iniciado el procedimiento la Agencia requerirá al solicitante para que acredite la desproporcionalidad del esfuerzo que supone la notificación, cuantificando el coste, en la fase probatoria, así como las medidas compensatorias a adoptar por el responsable del tratamiento.

Para valorar si procede o no la aplicación de la excepción del artículo 5.4 la Agencia utilizará como criterios: la antigüedad de los datos, el número de afectados y las medidas compensatorias que se vayan a adoptar.

El procedimiento concluye con una resolución dictada por el Director de la Agencia[55].

C. Recomendaciones

En relación a la recogida de datos a través de un sitio en Internet se debe tener en cuenta lo siguiente a efectos de garantizar el cumplimiento del deber de información recogido en la LOPD:

[54] El artículo 9 del Reglamento de desarrollo de la LOPD, RD 1720/2007, de 21 de diciembre, recoge expresamente este extremo en el apartado 1º del artículo 9.

[55] A pesar de que el artículo 12 del Estatuto de la Agencia de Protección de Datos no incluye ninguna referencia a este procedimiento, cabe apreciar su competencia en base a la función de dirección y representación de la Agencia, atribuida por el artículo 36.1 de la LOPD. Memoria de la AEPD del año 2002.

1. Incluir en las páginas web desde las que se recaben datos de carácter personal la información exigida por el artículo 5 de la LOPD. Esta información debe ser claramente visible y debe poder obtenerse con facilidad y de forma directa y permanente por el interesado. Además, es recomendable que en todas y cada una de las páginas en las que se soliciten datos personales que se pueda acceder directamente a información completa sobre la política de privacidad de la entidad.
2. El título del encabezado que deba seleccionarse para recabar datos personales debe resaltarse, ser explícito y específico. Por ejemplo, el encabezado podría ser el siguiente: "Esta página recoge y trata datos personales relacionados con usted. Si desea más información pinche aquí".
3. Se debe especificar claramente el nombre o denominación social (identidad del responsable) y el domicilio (postal y electrónico) del responsable del fichero al que se incorporarán los datos personales solicitados, así como una referencia al código de inscripción asignado por el Registro General de Protección de Datos.
4. En el caso de que los datos vayan a ser incorporados inicialmente a los ficheros de distintos responsables, se referirá toda la información anterior a cada uno de ellos. Deben enumerarse los destinatarios o las categorías de destinatarios de la información recogida. Al recoger datos personales los sitios web se deben señalar si lo comunicarán o lo pondrán a disposición de terceros y por qué motivos.
5. En el caso anterior, los usuarios de Internet deben tener la posibilidad de oponerse a ello marcando una casilla relativa a la comunicación de datos para fines distintos de la prestación del servicio solicitado.
6. Si se prevé que la entidad aseguradora responsable del fichero transfiera los datos a países no miembros de la Unión Europea, hay que indicar si esos países ofrecen una adecuada protección de los interesados respectos a sus datos personales, debiendo facilitarse información específica sobre la identidad y la dirección de los destinatarios (dirección postal y electrónica).
7. Si se realiza una transacción comercial a través de Internet utilizando "servicios de pasarela de pago" prestados por entidades financieras no se almacenarán datos que puedan relacionar la identificación del medio de pago con la identidad de su titular, salvo que sea legítimo para los intereses que persigan.
8. Se considera una buena práctica que el responsable de una web que transfiere el control a otra web informe convenientemente al usuario.

6.2. El consentimiento

A. Marco normativo

La LOPD española recoge y amplia la regulación comunitaria del consentimiento como principio ocupando un lugar protagonista en todo el

sistema protector, de manera que *no sólo afecta a la recogida de los datos sino que se hace extensiva a otras operaciones que integran el tratamiento automatizado de los datos* (tratamiento, comunicación y cesión, entre otros). De ahí que se considere un acierto que la LOPD (art. 3, *h)*) defina qué ha de entenderse por consentimiento, lo que, por otro lado denota el "esfuerzo de adaptación de los viejos conceptos del Derecho a las nuevas realidades"[56], si bien se echaba en falta que el legislador precisara algo la forma de expresar la voluntad lo que ha generado no pocos problemas en la práctica.

En este sentido, el artículo 3,h) define el consentimiento como:

> "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".

A lo que el artículo 6 de la LOPD añade: salvo que la ley disponga otra cosa.

Frente a esto, el nuevo Reglamento introduce un capítulo (Capítulo II del Título II) dedicado a las formas de recabar el consentimiento y a la revocación del mismo que se analizan más adelante (arts. 12 a 17).

Como principio general se exige prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho, lo que quiere decir que el responsable del tratamiento no puede tratar los datos argumentando que el interesado no ha respondido a la solicitud del consentimiento, excluyendo, de este modo, el silencio positivo que hasta la entrada en vigor del Reglamento se utilizaba como principio general en aplicación del Real Decreto 425/2005, de 15 de abril, para la comunicaciones electrónicas con fines de prospección comercial.

El tratamiento automatizado de datos de carácter personal requiere el consentimiento inequívoco del afectado (art. 6.1)[57]. La protección concedida a esta cláusula se refuerza más adelante (art. 6.3 y 11.4)) con la posibilidad de revocar ese consentimiento cuando exista una causa justificada, a lo que se añade el procedimiento incluido en el RD 1720/2007 que incorpora como novedad la obligación del responsable del fichero de ofrecer al titular de los

[56] ALVAREZ RICO, M.: *Consideraciones sobre el Proyecto de Ley por el que se modifica la LORTAD (Ley 5/1992), de tratamiento automatizado de datos de carácter personal.* Libro de Actas de las Segundas Jornadas de Informática y Sociedad (JIS´98), celebradas en Madrid los días 24, 25 y 26 de noviembre de 1998. Edita el Departamento de Lenguajes y Sistemas Informáticos e Ingeniería del Software de la Universidad Pontificia de Salamanca. Campus de Madrid, págs. 255 a 258.

[57] La LOPD recoge la definición de consentimiento en el artículo 3, *h)*, lo cual supone una novedad respecto a la Ley 5/99, que si bien exigía el consentimiento no especificaba que debía entenderse por tal. La letra del artículo señala que el consentimiento del interesado es: " toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".

datos un medio sencillo y gratuito para la revocación del consentimiento, sin que eso le suponga, en ningún caso, ingresos añadidos para la entidad aseguradora responsable.

De este modo, son tres los requisitos que el Reglamento exige para obtener el consentimiento:

- Prueba del consentimiento
- Consentimiento referido a un tratamiento o serie de tratamientos
- Consentimiento para la comunicación o cesión
  - el afectado debe ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos,
  - el tipo de actividad desarrollada por el cesionario,
  - en otro caso, el consentimiento es nulo.

El tratamiento de datos de salud puede tener lugar sin consentimiento del interesado

Por tanto**,** *la regla general es el consentimiento* del afectado no sólo para la recogida de los datos sino también para cualquier tratamiento posterior[58], si bien este principio *se exceptúa* cuando:

1. se realice con el objeto de prestar atención sanitaria y el tratamiento sea realizado por un profesional sanitario sujeto al secreto profesional o por persona sujeta a una obligación equivalente de secreto (artículo 8 LOPD),
2. exista autorización legal,
3. se trate de datos recogidos de fuentes accesibles al público,
4. se dirija al Poder Judicial o Defensor del Pueblo[59],
5. se produzca entre Administraciones públicas[60] siempre y cuando la finalidad del tratamiento sea histórica, estadística o científica,
6. cuando la cesión de los datos personales sea necesaria para solucionar un problema urgente de salud.

No se considera como comunicación de datos aquellos accesos de terceras personas cuando sea necesario para la prestación de un servicio al responsable del tratamiento. Este último punto constituye una novedad importante respecto a la regulación de la LORTAD, e incorpora de este modo

[58] El RD 1720/2007, exige, además, que cuando se solicite el consentimiento del afectado para la cesión de sus datos, este deberá ser informado de forma que conozca **inequívocamente** la finalidad y el **tipo de actividad desarrollada** por el cesionario (art. 12.2).

[59] Esta figura al igual que el Tribunal de Cuentas, tanto a nivel nacional como autonómico se han introducido en el texto del 99 y no aparecían en la Ley 5/92.

[60] Nuevo apartado introducido por la LOPD.

la definición de "encargado del tratamiento"[61], distinto del concepto de "tercero"[62], recogidos ambos en la Directiva.

Tampoco será necesario el consentimiento cuando los datos de carácter personal (art. 6.2 LOPD):

1. Se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias;
2. Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;
3. Cuando el tratamiento de datos tenga por finalidad proteger un interés vital del interesado para la prevención o para el diagnóstico médicos, para la prestación de asistencia sanitaria o tratamientos médicos, o para la gestión de servicios sanitarios, siempre y cuando este tratamiento se realice por un profesional sometido al secreto profesional u otra persona con una obligación equivalente de secreto (art. 7.6 LOPD).
4. Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para los intereses legítimos del responsable del fichero o del tercero a quien se comuniquen los datos.

En resumen, el requisito general del consentimiento se matiza con todo un grupo de excepciones dentro de las que se encuentran también las relaciones contractuales que, en la mayoría de los casos, conectan al cliente con la entidad aseguradora, y de ahí que en muchos casos no sea necesario exigirlo (una vez firmado el contrato por ambas partes). No obstante, ello puede llevar a la extra-utilización del principio, lo que ha dado lugar a varias sanciones de la AEPD y a pronunciamientos de nuestros tribunales.

Por otro lado, cuando los datos que se recogen entran dentro del supuesto de *datos especialmente protegidos* el consentimiento se refuerza y no se aplica lo anterior, de manera que el interesado debe otorgar su consentimiento de manera:

a. *expresa,* cuando se recojan datos referidos al origen racial, salud y a la vida sexual,
b. *expresa y por escrito* cuando los datos de carácter personal revelen la ideología, afiliación sindical, religión y creencias (se exceptúan los ficheros de datos relativos a sus asociados o miembros).

---

[61] Art. 2,*e):" la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;"*

[62] Art. 2, *f):" la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;"*

En cualquier caso, el consentimiento que se solicite debe ir referido a un tratamiento o a una serie de tratamientos concretos, delimitando la finalidad para la que se recaban.

B. Aplicación de la normativa sobre protección de datos

Para la correcta recogida del consentimiento por parte de las entidades aseguradoras debe tenerse en cuenta que éste debe ser libre, *inequívoco, específico* e *informado*.

Estos cuatro extremos deben ser entendidos de la siguiente manera[63]:

1. *Libre*. Supone que el consentimiento se debe obtener sin la intervención de vicio alguno en el mismo en los términos del Código Civil.
2. *Específico*. Referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento (art. 4.2 LOPD).
3. *Informado*. El interesado debe conocer con anterioridad al tratamiento la existencia del mismo y las finalidades. A este respecto, El Reglamento de desarrollo de la LOPD establece que cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a ellos deberá expresarse en un lenguaje fácilmente comprensible por aquéllos a efectos de cumplir con las exigencias de consentimiento informado (art.13.3).
4. *Inequívoco*. El concepto *inequívoco* es un concepto jurídicamente indeterminado del que puede afirmarse (como se detalla más arriba) que incluye tres tipos de manifestaciones: tácita, expresa y por escrito. En cualquier caso, debe insistirse en que el sentido incorporado por el legislador, implica la *imposibilidad de deducir el consentimiento de los actos realizados por el afectado* (consentimiento presunto), siendo necesario que exista una acción u omisión que implique la existencia de consentimiento[64].

La necesidad del consentimiento debe entenderse de manera restrictiva en el sentido de solicitar los datos estrictamente necesarios; esto es: adecuados, pertinentes y no excesivos en relación al ámbito y a las finalidades para las que se hayan obtenido. Esta interpretación ha sido corroborada por la Audiencia Nacional en su sentencia de 29 de junio de 2003[65]. En este caso una entidad bancaria exige al interesado abrir una cuenta corriente para cobrar la prestación de desempleo, sin que, la apertura de esa cuenta fuera requisito necesario para proceder al pago de la prestación. Señala la sentencia que:

[63] Memoria de la AEPD del año 2000.

[64] En este sentido vid. ST. Audiencia Nacional de 31 de enero de 2003 citada anteriormente.

[65] Núm. Rec. 785/2003.

> "Es cierto que el INEM recogió los datos de los perceptores de la prestación por desempleo para el ejercicio de sus funciones y que esta recogida de datos es uno de los supuestos *excluidos de consentimiento del afectado* (subrayado del autor) en aplicación del artículo 6.2 de la Ley Orgánica 15/1999 pero lo que no se justifica es que CAJA realizara la preapertura de una cuenta corriente a nombre de Rita y que, posteriormente, sin necesidad de emplearla en el abono de la correspondiente prestación, mantuviera la cuenta corriente abierta y que tratara los datos facilitando a la Agencia Tributaria la obligada información sobre las percepciones que se habían abonado en dicha cuenta (…). Precisamente eso, la grabación, conservación y elaboración de datos es lo que realizó la CAJA con los datos de la denunciante para preabrir una cuenta corriente innecesaria para la prestación que debía abonar".

En el supuesto anterior existe una clara extralimitación de la actividad de la entidad bancaria dado que para el pago de la prestación no resulta en modo alguno necesario contar con una cuenta abierta en el banco encargado de realizar los pagos sino simplemente demostrar la identidad de la persona que recibe el mismo.

Con todo, proliferan en Internet cuestionarios, impresos y formularios en los que se solicitan más datos (edad, número de hijos, identificación del cónyuge, aficiones, lugares de vacaciones…) de los necesarios para iniciar, cumplir o mantener una relación contractual y que, posteriormente se utilizan para elaborar perfiles del usuario a efectos de dirigir campañas publicitarias.

En el redireccionamiento de estos datos se utilizan técnicas de *scoring*, *datamining* y *data warehouse* que exigen el consentimiento expreso del interesado por su carácter de graves prácticas invasoras de la intimidad del ciudadano.

La Audiencia Nacional confirmó la consideración anterior en su sentencia de 14 de junio de 2002[66] en la que entiende que:

> Los datos sometidos al procedimiento de *scoring* no son datos obtenidos de fuentes accesibles al público, lejos de ello son datos que da el mismo cliente al solicitar el alta, indicándosele en el contrato que dichos datos tendrán como finalidad mantener la relación contractual con el cliente y prestar al mismo el servicio. No existe, por tanto, prestación de consentimiento para someter los datos al procedimiento de *scoring*, ni el afectado ha sido advertido, antes al contrario, de que los datos que facilita van a ser sometidos a dicho procedimiento.

Otra sentencia interesante en relación al consentimiento es la de 15 de febrero de 2006, de la Audiencia Nacional[67] en el supuesto de una correduría

[66] Núm. Rec. 650/2001
67 Núm. Rec. 258/2004

de seguros que tramitó la contratación de un seguro de hogar de la afectada a pesar de la devolución del contrato sin firmar:

> "… El corredor no es un mero comisionista y es un asesor que debe informar al cliente y buscarle la cobertura que mejor se adapte a sus intereses, pero también lo es que *no está habilitado para contratar en su nombre* (subrayado del autor) una nueva póliza de seguro por lo que la compañía excedió sus funciones de mediadora…ya que sin averiguar quien había resuelto el contrato (la aseguradora o la asegurada) o si esta última deseaba una nueva cobertura *aseguradora contrató una nueva póliza sin haber consultado, asesorado e informado a la cliente, imponiendo indirectamente la celebración de un nuevo contrato y sin su consentimiento los datos que la afectada había otorgado para una determinada gestión de un seguro, en un determinado momento*…"

El nuevo Reglamento de desarrollo de la LOPD trata de solucionar la numerosa casuística que la falta de indefinición de la norma a este respecto ha ido generando estos años. A este respecto, obliga al responsable del tratamiento a solicitar el consentimiento del afectado *durante el proceso de formación del contrato para finalidades que no guarden relación directa* con el mantenimiento, desarrollo o control de la relación contractual, permitiendo, en todo caso, al interesado manifestar expresamente su negativa al tratamiento o comunicación de datos.

C. Especial referencia a los datos de salud recabados por el sector asegurador

La LOPD no exige que el consentimiento se recabe por escrito, sin embargo la obligación de obtener el consentimiento de *forma expresa* implica que en la parte de los formularios dedicados a la protección de datos o en las demás formas de recogida de estas categorías de datos se haga una mención específica al tratamiento o la cesión prevista. Por tanto cuando se recaben varios tipos de datos entre los que se encuentren los que hagan referencia a la salud del interesado, los formularios (o formas análogas de recogida de datos) deberán incluir una *cláusula* que mencione que *cumplimentando la misma el interesado consiente de forma expresa al tratamiento de sus datos* con la finalidad indicada.

En este sentido la Agencia de Protección de Datos sancionó a una Mutua[68] que sin el consentimiento del trabajador y para completar los resultados obtenidos durante una visita médica a la que éste acudió voluntariamente, utilizó los resultados de un reconocimiento médico anterior.

---

[68] Resolución R/00740/2004 de la Agencia Española de Protección de Datos.

Por otro lado, la LOPD contempla dos excepciones a la regla del consentimiento expreso para el tratamiento de datos que hagan referencia a la salud del interesado:

- Por previsión legal y
- Para salvaguardar el interés vital del interesado.

De este modo, no es necesario contar con el consentimiento expreso del interesado cuando el tratamiento responde a un mandato legal. De ahí la importancia de la norma que exige la recogida de datos que haga referencia a la salud tenga rango de ley, puesto que, en caso contrario no es de aplicación la excepción mencionada.

El primer supuesto destacable en el marco asegurador lo proporciona la Sentencia de la sección octava del Tribunal Superior de Justicia de Madrid, de 12 de julio de 2000[69]. Esta sentencia se pronuncia sobre la legalidad de un tratamiento realizado por una entidad aseguradora de los datos de salud del tomador del seguro sin haber recabado previamente su consentimiento expreso.

En el formulario de obligado cumplimiento por parte del tomador como requisito para poder optar al seguro se solicita información sobre sus antecedentes de salud sin incluir ninguna cláusula de información sobre el posterior tratamiento de sus datos. La Agencia Española de protección de Datos sancionó a la aseguradora por incurrir en una infracción muy grave consistente en el tratamiento de datos de salud del denunciante sin su consentimiento.

El Tribunal anuló la sanción por considerar que *el tratamiento de datos es necesario para el mantenimiento de la relación contractual y plasmado en la póliza del seguro, pudiendo la aseguradora acogerse a la excepción al consentimiento prevista en el artículo 6.2 de la LOPD[70].*

En este sentido, los informes periciales relativos a accidentes de tráfico pueden ser tratados por las entidades aseguradoras con fines de indemnización sin necesidad de contar con el consentimiento del interesado,

[69] Esta Sentencia fue dictada bajo la vigencia de la LORTAD si bien las disposiciones aplicables se recogen también en la LOPD por lo que pueden trasladarse los criterios de aplicación a los tratamientos sometidos a esta norma. Con todo la Agencia Española de Protección de Datos sigue exigiendo el consentimiento expreso por lo que lo más recomendable es seguir en este caso la prescripción del artículo 7.3 que exige la recogida del consentimiento expreso del afectado como requisito previo al tratamiento de sus datos de salud.

[70] Art.6.2 LOPD: "no será preciso el consentimiento cuando los datos de carácter personal se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato".

dado que tanto la Ley 50/1980 como la Ley 30/1995 establecen que las aseguradoras deben recabar y conservar la información relativa a la salud de los terceros que deben ser indemnizados como consecuencia de un seguro de responsabilidad civil y de ahí se entiende que concurren las excepciones al tratamiento sin consentimiento del afectado y previstas en los artículos 6.1, 7.3 y 11.2 a) de la LOPD.

Tampoco es necesario recabar el consentimiento expreso de un paciente que haya pasado por algún centro sanitario público para la cesión de sus datos de salud a las compañías aseguradoras, en relación a la asistencia sanitaria recibida como consecuencia de un accidente de circulación, siempre y cuando estos datos fueran necesarios a efectos de facturar los servicios prestados. Esta habilitación tiene como base la habilitación legal incluida en la Ley 14/1986, de 25 de abril, General de Sanidad, que habilita a dichos centros a facturar los servicios prestados en estas ocasiones y a reclamar al tercero responsable el coste de los mismos[71].

Otro ejemplo en este sentido lo proporciona la Agencia Española de Protección de Datos que considera cesión de datos, amparada en una norma de rango legal, la comunicación de los datos de salud de los trabajadores de un Consorcio sanitario a una Mutua y de ésta a una empresa de visitadores médicos subcontratada al efecto. Estas cesiones se realizaban sobre la base de conciertos entre la Mutua y las empresas a las que prestaba sus servicios y dentro del marco de la prestación relativa a las bajas por accidentes de trabajo y enfermedades de la Seguridad Social.

La Mutua contrataba con entidades implantadas en poblaciones en las que no tenía presencia física y para realizar orientación diagnóstica y visitas domiciliadas, entre otros servicios.

Por otro lado, el Consorcio no facilitaba datos relativos a los diagnósticos de los trabajadores en situación de baja laboral, sino que éstos eran obtenidos por la Mutua en el desempeño de sus funciones, incorporándolos a continuación a sus propios ficheros. Esta actividad y la cesión se ajusta correctamente a la protección de datos personales dado que las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social que contraten, mediante conciertos, con medios privados para hacer efectivas las prestaciones sanitarias, encuentran su habilitación legal en la Ley General de la Seguridad social y en su normativa de desarrollo[72] .

Lo anterior no significa que el interesado no deba ser informado en los términos del artículo 5 de la LOPD, y, en particular, ajustándose al principio de finalidad. En este sentido la Audiencia Nacional, en su sentencia de 15 de

[71] Informe 526/2003, de la Agencia Española de Protección de Datos, relativo a la cesión de datos de salud a aseguradoras de asistencia sanitaria por centros sanitarios públicos.

[72] Memoria 2001, de la Agencia Española de Protección de Datos, pp. 260-261.

junio de 2001, confirmó la sanción impuesta por la Agencia Española de Protección de Datos por infracción del deber de información a un Centro de Transfusión que recaba en papel datos de los donantes de sangre para incluirlos posteriormente en un fichero automatizado de historias clínicas, sin informar a los donantes de este extremo ni de la posibilidad de ejercer sus derechos de acceso, rectificación y cancelación, basándose en la excepción al deber de información cuando pueda deducirse claramente de las circunstancias que rodean la recogida de datos.

La Audiencia Nacional consideró que no concurría la excepción al deber de información dado que un donante proporciona sus datos para que pueda comprobarse su aptitud a ser donante sin que ello deba implicar que se realice un tratamiento posterior de sus datos.

D. Recomendaciones

Conveniente destacar en relación a los datos de salud que, a pesar de la Sentencia del Tribunal de Justicia de Madrid de 12 de julio de 2000, favorable al tratamiento de estos datos sin el consentimiento del interesado, es recomendable solicitar en todo caso la recogida del *consentimiento expreso del afectado para el tratamiento de sus datos de salud,* puesto que éste es el criterio de la Agencia Española de protección de Datos, por lo que continúa imponiendo sanciones a todas aquellas aseguradoras que infringen este extremo.

6.3. Formas de recogida de datos

A. Aplicación de la normativa sobre protección de datos

La correcta recogida de datos personales y la carga de la prueba recae, como se ha apuntado más arriba, en el responsable del fichero o del tratamiento por lo que es éste el encargado de delimitar los criterios básicos que garanticen el cumplimiento de los principios de información y consentimiento.

La expresión *consentimiento previo del afectado* del artículo 11 (comunicación de datos) de la LOPD debe interpretarse de diferente manera en función de las tres formas básicas en que éste se exige a lo largo del articulado de la ley. De este modo cabe distinguir entre consentimiento expreso, tácito y presunto. La Agencia de Protección de Datos ha interpretado a través de sus diferentes Memorias el alcance de estas formas básicas en el siguiente sentido:

El *consentimiento expreso* se manifiesta mediante un acto positivo y declarativo de la voluntad.

El *consentimiento tácito* se produce cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, esto es, cuando el silencio se presume o se presupone como un acto de aceptación.

Por último, el *consentimiento presunto*, no se deduce ni de una declaración, ni de un acto de silencio positivo sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación.

Lógicamente el medio idóneo para acreditar el consentimiento por parte del responsable del fichero es la obtención de forma expresa, acompañado de la firma del titular.

Pero además, debe tenerse en cuenta que el responsable debe también custodiar ese consentimiento puesto que en el caso de solicitud por parte de la Agencia de Protección de Datos debe presentar toda la documentación.

Por ello, se debe ser especialmente cuidado no sólo con los términos en los que se solicita el consentimiento sino también en su posterior tratamiento.

Respecto al *consentimiento tácito* quedan *expresamente excluidos los datos de salud,* origen racial o vida sexual o lo que es lo mismo, el consentimiento tácito es válido siempre que no se trate de datos especialmente protegidos, recayendo, en todo caso, en la entidad aseguradora que solicite el consentimiento la carga de la prueba.

En relación al *consentimiento presunto*, la Agencia de Protección de Datos también se ha manifestado en contra de que de los actos realizados por el interesado se puedan presuponer la obtención del consentimiento para realizar el tratamiento de sus datos personales con una finalidad determinada[73].

Por tanto, todo se reduce a contar con los medios de prueba suficientes para acreditar que se ha solicitado y obtenido el correspondiente consentimiento (envío de comunicación, recepción por el interesado, otorgamiento de plazo prudencial para que éste tenga conocimiento, consecuencias de no contestar a la solicitud, utilizar el último domicilio facilitado por el cliente.

Los medios más habituales de comunicación entre los responsables de los ficheros y los titulares de los datos son: el medio escrito, el teléfono e Internet, dado que el objeto de este estudio es el entorno digital, nos centramos a continuación en las formas de recabar el consentimiento en este medio y en sus ventajas e inconvenientes desde el prisma de la legalidad.

[73] ECIJA Abogados. Factbook de Protección de Datos Personales. Editorial Thomson. Aranzadi. Cizur Menor, Navarra, 2003, p. 74.

B. Recomendaciones

En este sentido, resultan ilustrativas las recomendaciones de la Agencia de Protección de Datos reflejados en los resultados de la inspección de oficio realizada al sector del comercio electrónico en el año 2000, así como el documento del Grupo del artículo 29 de la Directiva 45/96/CE, relativo a los "requisitos mínimos para la recogida en línea de datos personales". Lo más destacable de estas dos Recomendaciones en lo que se refiere al consentimiento es lo siguiente:

1. Únicamente cabe el tratamiento para un fin específico si concurren alguno de los siguientes casos:

   - consentimiento inequívoco del interesado,
   - tratamiento necesario para la ejecución de un contrato en el que interesado es parte,
   - tratamiento necesario para cumplimiento de obligación jurídica a la que esté sujeto el responsable del tratamiento,
   - tratamiento necesario para satisfacción de interés legítimo del responsable del tratamiento o tercero que comunique datos, siempre que no prevalezca el interés de la persona titular de los datos.

2. Debe reconocerse el derecho de oposición previa petición y sin gastos para el interesado a que sus datos se cedan o usen con fines de marketing directo.
3. Cuando el usuario facilita voluntariamente sus datos de carácter personal a través de Internet para una finalidad distinta a la mera ejecución de la transacción comercial, se entiende que consiente en el tratamiento en los términos en los que fue convenientemente informado en el momento de la recogida de datos.
4. Si la ley no lo impide, cuando el interesado revoque su consentimiento para el tratamiento de datos, el responsable del fichero habilitará los medios oportunos para excluir el tratamiento de los mismos.
5. Se debe habilitar una casilla para que el usuario pueda marcar la opción de oponerse al tratamiento y para las cesiones sobre las que se solicita consentimiento.
6. Una vez cumplimentados todos los datos deberá mostrarse la pantalla completa y cumplimentada en una nueva pantalla como requisito previo a la obtención del consentimiento y con la opción de impresión.
7. Se debe mencionar *con claridad* la existencia de procedimientos automáticos de recogida de datos, antes de utilizarlos. Además, se debe informar al cliente del nombre de dominio de servidor de sitios que transmite los procedimientos automáticos de recogida, la finalidad de dichos procedimientos, plazo de validez, si es requisito o no para visitar el sitio y la opción de oponerse, además de las consecuencias de desactivas dichos procedimientos.

8. En el caso de que en la recogida de los datos participen varios responsables del tratamiento, el cliente debe recibir información sobre la identidad de estos responsables y la finalidad del tratamiento en relación con cada controlador.
9. La información y la posibilidad de oponerse a la recogida debe comunicarse *antes de utilizar cualquier procedimiento automático de recogida de datos* que desencadene la conexión del ordenador del cliente con otro sitio web; por ejemplo, cuando el sitio web conecta automáticamente al usuario con otro sitio para mostrarle publicidad en forma de panel publicitario, con el fin de evitar que este segundo sitio recopile sus datos sin que el usuario sea consciente de ello.
   Si el servidor del responsable del tratamiento coloca una *cookie* esta información debe facilitarse al cliente antes de que ésta se envíe al disco duro del usuario y no limitarla al nombre del sitio transmisor y al período de validez de la cookie.

Con todo, estas recomendaciones no han sido suficientes para garantizar la protección de los interesados y de ahí que el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD dedique parte de su articulado (artículos 14 y 15) a las formas de recogida de los datos, a fin de facilitar la obtención del consentimiento.

El procedimiento establecido en el Reglamento tiene un carácter opcional, lo que quiere decir que no hay obligación de obtener el consentimiento de la forma en él prescrita y está orientado a favorecer el consentimiento en forma tácita que, en ningún caso, es aplicable a los datos de salud.

El procedimiento previsto en el Reglamento es el siguiente:

1. El responsable puede dirigirse al afectado informándole en los términos del artículo 5 de la LOPD.
2. Se debe conceder un plazo de 30 días (naturales) para que el interesado manifieste su negativa al tratamiento.
3. Se debe advertir expresamente de que en caso de no contestar se entenderá que da su consentimiento tácito.
4. El responsable debe gestionar el envío y el rechazo. Lo más fácil es llevarlo a cabo con un procedimiento auditable encargado a un tercero.
5. Se debe facilitar al interesado un medio sencillo y gratuito de manifestar su negativa al tratamiento (prefranqueo, número telefónico gratuito, servicio de atención al público).

Si se utiliza este procedimiento no podrá volverse a solicitar el consentimiento respecto a los mismos tratamientos y para las mismas finalidades en el **plazo de un año** a contar desde la fecha de la anterior solicitud.

El procedimiento descrito recoge, por tanto, la solución prevista para la prestación de servicios de comunicaciones electrónicas en aquello

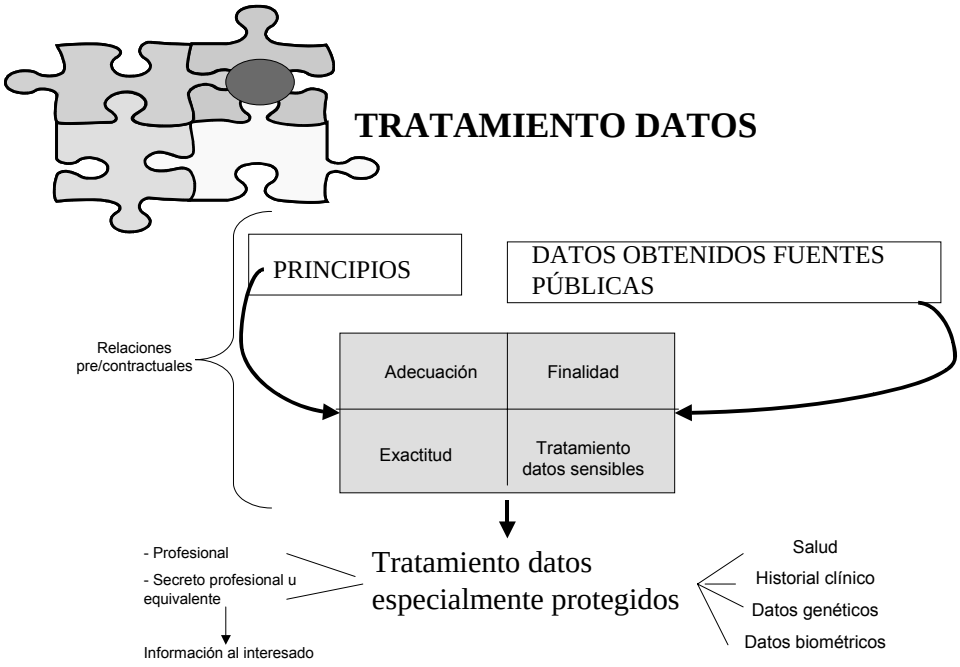
relacionado con el tratamiento de datos de tráfico con fines de promoción comercial[74], y lo amplia al consentimiento en general. El art. 65. 3 señala, a este respecto que el operador debe dirigirse al interesado con una antelación de un mes e informarle sobre los servicios para los que se efectuará el tratamiento y la duración que tendría, solicitando en ese momento el consentimiento. La comunicación debe realizarse por un medio que garantice la recepción. Si trascurrido este plazo el interesado no se hubiese manifestado al respecto se entiende que consiente en el tratamiento de datos para esta finalidad, siempre que este extremo se haya hecho constar en la comunicación enviada al efecto.

El Reglamento de desarrollo de la LOPD introduce como novedad respecto a la normativa específica recogida en el párrafo anterior, el cómputo del plazo que pasa a fijarse en días (30 días). El silencio se mantiene positivo si se respeta el período señalado y se gestiona la devolución o rechazo por cualquier causa, en cuyo caso, no podrá procederse al tratamiento. Por tanto, no hay que modificar la forma en que hasta ahora se obtenía el consentimiento tácito, puesto que para la prestación de servicios de comunicaciones electrónicas, servicio universal y protección de usuarios, los datos de tráfico se remitían a su normativa específica en la que ya se recogía el consentimiento tácito.

En conclusión, el nuevo procedimiento incorporado por el Reglamento agiliza la recogida del consentimiento para los casos en que esté no deba ser recabado de forma expresa o expresa y por escrito, de manera que en el supuesto de contratación de una póliza de salud todos los datos de este tipo deben contar con el consentimiento expreso del asegurado, no así los relacionados con: nombre, dirección, profesión, etc, para los que el consentimiento puede ser incluso tácito.

[74] Artículo 65.3 del Real Decreto 424/2005, de 15 de abril. BOE, de 29 de abril de 2005.

7. TRATAMIENTO DE DATOS



Fuente: elaboración propia

El tratamiento de datos personales consiste en cualquier operación o procedimiento técnico, ya sea automatizado o no, que permita realizar:

1. la recogida de datos de carácter personal
2. la grabación de datos de carácter personal
3. la conservación de datos de carácter personal
4. la elaboración, modificación y consulta de datos de carácter personal
5. la cancelación, bloqueo o supresión de datos de carácter personal
6. la cesión de datos que resulten de las consultas, interconexiones y transferencias de los mismos

La referencia al tratamiento se contempla como uno de los requisitos de calidad de los ficheros de datos personales debiendo ponerse en relación con los principios de adecuación, pertinencia, proporcionalidad y finalidad. Para comprender el alcance del tratamiento a la luz de la LOPD es necesario desgranar cada uno de estos principios.

7.1. El principio de calidad en la recogida de datos personales

A. Marco normativo

El principio de calidad se desgrana en una amplia gama de principios o subprincipios, sin que exista una definición compartida por todos sobre lo que ha de entenderse por calidad de los datos. Los distintos textos multilaterales se refieren a los requisitos que los datos personales tratados por medios automatizados deben cumplir para adjudicarles el apelativo de datos de calidad; sin embargo los criterios varían de unos a otros y así, mientras la OCDE distingue claramente entre calidad, especificación y transparencia, el Consejo de Europa y la UE engloban éstos dos últimos dentro de la calidad. Esto indica la importancia del principio pero siembra las dudas sobre sus características identificadoras pues éstas aparecen bajo el manto protector de diferentes principios (o subprincipios) fundamentales, según el texto multilateral que utilicemos, aplicables todos ellos en el ámbito interno[75].

La UE sigue la misma estructura y orden del Consejo de Europa e incluye entre los requisitos: el de especificación (tanto del fin del fichero como de la exactitud y actualidad de los datos) y el de limitación (conservación cuantitativa y cualitativa).

También ha sido ésta la estructura utilizada en la LOPD (art. 4) donde se incluye un catálogo de obligaciones aplicables a todos (sector público y privado) los que manejan datos personales automatizados. No obstante, hay que destacar lo desafortunado de la redacción de la Ley al señalar que " los datos de carácter personal sólo se podrán recoger para su tratamiento automatizado, así como someterlos a dicho tratamiento cuando tales datos sean adecuados, pertinente y no excesivos…", pues el precepto parece distinguir varios momentos: el de la obtención, el de la recogida y el del tratamiento, pero sin indicar una secuencia, de lo que cabe deducir que la pertinencia es aplicable en toda obtención de datos, tanto en el momento de la

[75] En los Principios Rectores de Naciones Unidas, no se menciona el requisito de la calidad, a pesar de que la versión que utilizamos en este trabajo fue aprobada en 1995, años después del Convenio 108 y de las Directrices de la OCDE que, por el contrario, dedican todo un artículo a este principio.
El tratamiento que en estos dos últimos textos se hace de la calidad es bien distinto. Por un lado, las Directrices de la OCDE enumeran en su artículo 8 como principios de calidad: la pertinencia y necesidad de fines a alcanzar, así como la exactitud y actualización constante de los datos (ver principio de limitación).
Por su parte, el Convenio 108 del Consejo de Europa concede una gran importancia a este principio y estructura en cuatro apartados las exigencias de calidad de los datos personales. El primer apartado se refiere a la licitud y legitimidad en la obtención de datos (ver principio de limitación). El segundo a la especificidad del fichero (ver principio de especificación del fin); el tercero a la adecuación, pertinencia y no exceso en relación con la finalidad (ver principio de especificación del fin) y el cuarto a su conservación, cuyo análisis en este trabajo se está realizando, haciendo uso como recordaremos de la clasificación formulada por la OCDE, dentro del principio de transparencia.

obtención, como en el de la recogida (ya sea directa o indirecta), o si se produce durante el tratamiento.

La ley española exige, por tanto, que los datos sean los pertinentes y adecuados según el objeto del fichero. Pero además, no deben ser excesivos en relación al ámbito y a las finalidades legítimas para las que se hayan obtenido.

B. Aplicación de la normativa sobre protección de datos

- *Datos adecuados, pertinentes y no excesivos*

  El artículo 4.1. de la LOPD dispone:

  Los datos de carácter personal sólo se podrán recoge para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuado, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Este artículo debe ponerse en relación con el apartado a) del artículo 5 en lo que se refiere al consentimiento informado y con el 4.2 que prohibe que los datos se utilicen para finalidades incompatibles con aquéllas para las que los datos fueron recogidos.

Sobre la pertinencia se pronunció el Tribunal Supremo español en su Sentencia (Sala Tercera, Sección Sexta) de 14 de noviembre de 1992, en relación a un cuestionario distribuido entre el personal de las Fuerzas Armadas en el que se pedían informaciones no pertinentes para el fin previsto (según el Sindicato de Comisiones Obreras). En concreto se planteó entre otras cuestiones la de la pertinencia de solicitar al personal extranjero datos acerca de las entradas y salidas en territorio español, ruta de viajes y finalidad de éstos, así como los motivos de solicitar la nacionalidad española. El Tribunal Supremo estimó que la petición de estos datos era necesaria para finalidad perseguida por el cuestionario que no era otra que determinar la aptitud de los interesados para no revelar secretos relacionados con la Seguridad del Estado, y por tanto, no se vulneraban tampoco los artículos 10 y 13 de la Constitución Española.

A pesar de todo, existen numerosos ejemplos de recogida de datos excesivos o no adecuados, por ejemplo, la Agencia de Protección de Datos ha destacado en su Informe de Conclusiones del Plan de Inspección de Oficio al Sector de la Banca a Distancia la práctica de no siempre especificar cuáles de los datos recabados son obligatorios y cuáles no. Hechos como solicitar el número de hijos sin especificar si es voluntario o/y cuál es la finalidad de recabar dicha información han sido objeto de la imposición de sanciones

graves y confirmada por la Audiencia Nacional en su sentencia de 6 de julio de 2001[76] en los siguientes términos:

> *Sin duda la conducta de la entidad recurrente (solicitud al interesado de los datos relativos a cuenta bancaria o VISA de forma obligatoria cuando el servicio lo había pagado por adelantado y contra reembolso por un año) recabando o intentando recabar unos datos de carácter personal para su tratamiento automatizado que resultaban completamente innecesarios e inadecuados en relación con el ámbito y las finalidades legítimas para las que se han obtenido, debe ser constitutiva de infracción, al vulnerar uno de los principios y garantías establecidas en la Ley Orgánica 5/1992 (hoy Ley orgánica 15/1999, LOPD) (…).*
>
> *Y aunque los datos en cuestión no llegaron a ser incorporados a los ficheros de…, ello no implica que falte el necesario tratamiento automatizados de los mismos para que se produzca el tipo sancionador (…).*
>
> *Antes al contrario se vislumbra una clara y decidida voluntad de no prestar el servicio contratado –a pesar de estar satisfecho su importe-, si no se le facilitan unos datos bancarios, que de una forma arbitraria e injustificada se solicitan al afectado; a la par que contumaz proceder, dando lugar a la devolución del abono (única solución que le quedaba al cliente, aparte de la de "pasar por el aro"), en lugar de atender a la solicitud primitiva de aquel de permitirle el acceso a (…)".*

A la luz de lo anterior, en la recogida y posterior tratamiento de los datos únicamente deben solicitarse los que sean necesarios para la contratación y para el mantenimiento y cumplimiento del contrato. Sólo éstos deber tener el carácter de obligatorios en la comunicación que haga el interesado, otro campo no incluido en lo anterior, debe contar con el consentimiento inequívoco del cliente.

- *Finalidad de los datos*

La práctica totalidad de principios de protección de datos aluden de una u otra manera a la finalidad en el tratamiento de datos se encuentra recogida en casi todos los principios, hasta tal punto que su cumplimiento o no lleva a calificar el tratamiento como de legítimo o ilegítimo.

El término finalidad es recogido en el artículo 4.2 de la LOPD en estos términos:

[76] St. núm. Rec. 314/2000

> Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

El alcance de la expresión finalidad incompatible debe interpretarse de forma sistemática relacionándola con el principio de autodeterminación pues una interpretación amplia lo vaciaría de sentido[77].

En el ámbito asegurador, la Agencia de Protección de Datos destaca la importancia del principio de finalidad en relación con el consentimiento, en su Memoria del año 2005, en los siguientes términos:

> *…lo que se plantea es que una compañía aseguradora tramitó el siniestro de una declaración amistosa de accidente de automóvil sin que en ésta constara firma de seguro. Ello ocasionó que los datos del siniestro se registraran en el fichero de siniestros de la compañía y en el Fichero Histórico de Seguros del Automóvil, que gestiona la entidad Tecnologías de la Información y Redes para las Entidades Aseguradoras, además de ocasionar el aumento de la prima anual del citado seguro. En tal supuesto se declaró la infracción del artículo 4.3 de la LOPD por cuanto que, con independencia de que en todo caso la entidad aseguradora debiera tramitar el siniestro como consecuencia de la responsabilidad civil derivada del mismo, dicha tramitación debió realizarse con la debida diligencia y garantías por parte de la aseguradora, de modo que la comunicación al Fichero Histórico de Seguros del Automóvil se efectúe con las debidas garantías de exactitud y veracidad respecto a la situación actual del asegurado*[78].

En este sentido, la Audiencia Nacional analiza en su sentencia de 2 de marzo de 2005 el caso del envío de una carta de una entidad bancaria a un cliente, a un domicilio distinto al indicado por el afectado, cliente de la entidad bancaria, que ésta conoce por las gestiones efectuada con la Administración Pública (domicilio fiscal):

> *…la actora remitió al denunciante una carta sobre regularización de su cuenta corriente a una dirección que efectivamente constaba, como de dicho denunciante, en el fichero de clientes de tal entidad bancaria, más no como domicilio de correspondencia de tal cuenta corriente, sino como domicilio fiscal del mismo. Así las cosas, esta Sala considera que no cabe afirmar en el supuesto que utilizase datos de carácter personal de dicho cliente con una finalidad distinta de aquella para la que habían sido recabados.*

[77] Audiencia Nacional, St. 14 de junio de 2002. Núm. Rec. 650/2001.

[78] Resolución R/00206/2005, Procedimiento Sancionador PS/00089/2004.

Los ejemplos de incumplimiento del principio de finalidad del 4.2 de la LOPD son numerosos. La Audiencia Nacional analiza la cesión de datos de un particular a una empresa que le prestaba servicios de adquisición y matriculación de un vehículo. Esta entidad le ofreció un servicio de seguro del automóvil que el afectado denegó al contar con una póliza de seguro de automóvil en vigor:

> *…cuando la gestoría "S" informó a "T Auto" que el seguro del denunciante estaba próximo a su vencimiento, dicha entidad (a través de su departamento de gestión), utilizó los datos que del señor obraban en sus ficheros para remitirle una carta ofreciéndole una serie de ventajas si contrataba el seguro del vehículo con "M" con esos datos. Esa utilización de los datos personales del comprador del vehículo que se habían facilitado para la adquisición y matriculación del vehículo, con una finalidad distinta para la que fueron recogidos (remitirle publicidad de una compañía aseguradora, "M") supone, como acertadamente señala la resolución recurrida, una infracción del artículo 4.2 de la LOPD e integra la conducta típica apreciada por la que ha sido sancionada la demandante.*

En otras ocasiones, la finalidad modifica la legitimidad que exceptúa la obligación de exigir el consentimiento. En efecto, en el Informe jurídico de la Agencia de Protección de Datos del años 2005[79] se ocupa de la utilización que hace una entidad de crédito de los datos de su personal que son objeto de tratamiento por la misma como consecuencia de la contratación por parte de ese personal de algún producto financiero con la entidad para la que prestan sus servicios.

Para el desarrollo de ambas relaciones no se necesita, en principio el consentimiento del interesado, si bien este principio debe ponerse en relación con los artículos 4.1 y 4.2 de la LOPD que consagra los principios de proporcionalidad y *finalidad*.

La Agencia considera que únicamente puede exceptuarse el consentimiento en el supuesto de existir una vinculación directa e insoslayable entre las dos relaciones contractuales, y pone como ejemplo, que se ofreciese un producto específico o en condiciones muy beneficiosas a su personal, en cuyo caso, *siempre que el afectado tuviese conocimiento de la necesidad de que determinados datos relacionados con su vínculo laboral con la entidad* financiera deben ser valorados para obtener el producto financiero que le ofrecen, cabría considerar al tratamiento en el ámbito de los dispuesto en el artículo 6.2 de la LOPD, en caso, contrario, se estaría vulnerando el artículo 4.2 de la LOPD, salvo que la entidad contase con el consentimiento.

[79] Informe jurídico 7/72005, disponible en: www.agpd.s/Canal_Documentacione/InformesJuridicos.

- *Datos actualizados*

Los apartados 3 y 4 del artículo 4 de la LOPD recogen el deber de actualización de los datos:

> 3. Los datos de carácter personal serán exactos y puestos al día de forma que responsan con veracidad a la situación real del afectado.
>
> 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

La obligación recogida en la ley es doble. Por un lado, se exige mantener los datos actualizados y, por otro, corregir los errores, al referirse a las actualizaciones de oficio que deben realizar los responsables de los ficheros.

En la práctica, los responsables de los ficheros encuentran una gran dificultad para demostrar la documentación que justifique que se han realizado las operaciones anteriores. La ausencia de prueba supone un incumplimiento del principio de calidad, pero además las sanciones pueden verse agravadas cuando se realicen o prevean realizarse cesiones de esos datos.

El sector más afectado por estos preceptos es el bancario y las sanciones de la Agencia de Protección de Datos, así como las decisiones de los tribunales se dirigen mayoritariamente contra él.

A este respecto, una de las interpretaciones más destacadas fue la de la Audiencia Nacional en relación con el mantenimiento del saldo cero, si bien se puede trasladar esta obligación al marco de las relaciones contractuales en el sector asegurador. Esta obligación debe interpretarse en sentido bilateral; esto es, dado que el responsable del fichero no puede estar continuamente pendiente de de mantener los datos del asegurado de acuerdo con la situación actual, deber ser el propio asegurado el que comunique al responsable del tratamiento las modificaciones necesarias para mantener y cumplir con esa obligación. Por su parte, el responsable del tratamiento tiene la obligación de tratar adecuadamente dicha modificación solicitada por el interesado.

Esto implica dos cosas: que la aseguradora sólo puede utilizar los datos facilitados por el cliente y no otros nuevos, aunque tenga conocimiento de ellos (por ejemplo, ante el impago de una póliza la aseguradora se dirige a una entidad bancaria, diferente a la que figura en el contrato, para el cobro de la deuda), que, por otro lado, tampoco puede actualizarlos si el cliente no se los facilita o consiente en ello (por ejemplo, envío de correspondencia a una

dirección diferente de la que figura en el contrato de seguros, por conocer que es en aquélla en la que el asegurado reside habitualmente).

En estos casos, lo aconsejable es informar al interesado de su obligación de mantener actualizados los datos en el momento de la recogida de los mismos y prever la forma de comunicación de cualquier variación de datos que efectúe.

En otras ocasiones, es el propio responsable del fichero el que intenta ponerse en contacto con el asegurado para actualizar los datos, en este caso, es importante que la aseguradora cuente con un procedimiento que permita demostrar ante la Agencia de protección de Datos que ha intentado actualizar los datos y que cuenta con un motivo justificado para ello.

En aquellos casos en los que exista alguna dificultad para probar la modificación de los datos, puede valorarse por el responsable el realizar un envío posterior al titular de los datos donde se reflejen las modificaciones y solicitando su validación o modificación.

Lógicamente la prestación de este servicio por terceras empresas ayuda a mantener los datos actualizados y minimiza los riesgos, al utilizar estas terceras partes procedimientos ágiles que permiten la puesta al día. Cosa distinta es el cumplimiento de este principio cuando se cuenta con servicios externos como los prestados por: inspectores, abogados, procuradores, empresas de recobro,etc, puesto que esto hace aumentar el riesgo de desactualización por cobros totales o parciales que se hayan ir pudiendo hacer.

7.2. Datos especialmente protegidos

A. Marco normativo

Bajo la denominación de categorías especiales de datos se engloban una serie de garantías o derechos adicionales que se aplican a tipos específicos de tratamientos y para los que se prevé una protección reforzada en función de su naturaleza y del objetivo para el que se destinen. Se trata, en unos casos, de datos que deben ser protegidos con más mimo dada su sensibilidad social. En otros casos, la particularidad está en el destino de mercado que se de a los datos transferidos. Una tercera categoría vendría dada por los datos que se transfieren para adoptar decisiones individuales automatizadas.

Especial interés revisten *datos sensibles* como los relativos a la salud, origen racial, ideología política, convicciones religiosas, vida sexual, infracciones administrativas o condenas penales. Desde que comienzan a elaborarse los primeros trabajos legislativos la cuestión de si algunos datos ofrecían una

vulnerabilidad especial y por tanto necesitaban mayor protección se planteó como problema. La doctrina en general se ha mostrado reacia a definir estos datos por considerar que los datos no son "intrínsecamente neutros"[80], sino en función del contexto en que se utilicen. Frente a esta postura, las legislaciones nacionales, excepto la alemana[81], incluyen la noción de datos sensibles *per se*. La sensibilidad que se tiene hacia esos datos depende del entorno jurídico y sociológico de cada país. Así, por ejemplo, mientras que en unos países la afiliación a un partido político no puede entrañar riesgos para la intimidad de la persona, en otros se consideran sensibles puesto que denotan una orientación política determinada.

El Convenio 108 intenta resolver la disparidad (art. 6) pronunciándose a favor de los datos sensibles *per se*. Con ello se regulaba el principio de que estos datos no pueden elaborarse automáticamente, salvo si el Derecho interno preveía las oportunas garantías. Aunque casi todas las leyes de protección de datos recogen el concepto el régimen concreto varía mucho de unas a otras. De ahí que la UE con ánimo de armonizar legislaciones (en la Directiva 95/46/CE) optara por una norma específica que prohibía su tratamiento como cláusula general. El art. 8.1 define una serie de supuestos que excepcionan la norma. En primer lugar, el caso de que el interesado haya dado su consentimiento explícito, salvo norma nacional en contrario. En segundo lugar, se exceptúan aquellos casos en que el tratamiento sea necesario por parte del responsable del fichero para cumplir con sus obligaciones y derechos en materia laboral, que sea necesario para salvaguardar el interés vital del interesado, o cuando el tratamiento lo efectúe una entidad sin finalidad lucrativa (con fines políticos, filosóficos, religiosos o sindicales) y siempre que no se comuniquen a terceros. Mención aparte se hace de los datos relativos a la salud, los cuales se podrán tratar siempre que se utilicen para la asistencia sanitaria o la gestión de servicios de este tipo. Aún reconoce más excepciones que reserva a los Estados fundadas en la salvaguarda del orden público. Por último, no están cubiertos por la prohibición los datos relativos a condenas penales, infracciones, medidas de seguridad o procesos civiles, si bien su tratamiento está sometido a requisitos adicionales (art. 8).

Por su parte la Ley española ha definido el sistema protector de los datos sensibles perfilándolo en torno a un régimen general y a contextos especiales. De este modo, el art. 7 se refiere al régimen general y regula el principio del consentimiento del interesado para acceder a estos datos. Esta regla se exceptúa en la nueva redacción de la Ley en dos ocasiones. En primer lugar (art. 7.2), para el caso de los ficheros cuya titularidad corresponda a partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas,

[80] LUCAS, A. Le droit de l'informatique. PUF. Paris, 1987.

[81] La Ley alemana no recoge el concepto por considerar que las cuestiones que plantea quedan resueltas con la norma del interés prevalente. Vid. HEREDERO HIGUERAS: La Directiva comunitaria de protección de datos de carácter personal.. Aranzadi Editorial. Pamplona, 1997, pág. 116.

asociaciones, fundaciones y otras entidades sin ánimo de lucro (cuya finalidad sea política, religiosa, filosófica o sindical), y que contengan datos relativos a sus asociados (en caso de cesión de estos datos se exige el previo consentimiento). La segunda excepción se recoge en el párrafo 6º y supone una trascripción literal del párrafo 3º del art. 8 de la Directiva. Con este nuevo apartado se introduce la posibilidad de tratar los datos sensibles en caso de necesidad en el ámbito médico y sanitario, siempre que el tratamiento se realice por un profesional sujeto al secreto profesional[82].

Las categorías especiales de datos sensibles se refieren a los datos sobre la salud (art. 8), el uso de datos sensibles por las Fuerzas y Cuerpos de Seguridad del Estado (art. 22) y a las infracciones administrativas referidas a estos datos (art. 43).

La segunda categoría de datos especiales se refiere a aquellos datos cuyo destino exclusivo sea la *mercadotecnia directa*. En estos casos, se reconoce al interesado el derecho a oponerse a que sus datos sean destinados a la prospección[83] La LOPD reconoce como novedad respecto al texto del 92 este derecho al referirse a los procedimientos (de oposición, acceso, rectificación o cancelación)[84]; sin embargo, no define qué se ha de entender por derecho de oposición ni en qué casos cabe ejercitarlo, como sí hace para los derechos de acceso, rectificación y cancelación. De ahí que para su interpretación habrá que remitirse a la Directiva comunitaria que no sólo prevé la oposición respecto a los tratamientos destinados a la prospección sino, al menos, en los casos en que esté implicado el interés público o sea necesario para satisfacer el interés legítimo del responsable del tratamiento[85].

Por último, en el ámbito de la UE se prevé una tercera categoría de datos personales especiales formadas por *decisiones individuales automatizadas* con efectos jurídicos (art. 15)[86]. Se reconoce así el derecho del interesado a que no se evalúen datos determinados (relativos a aspectos de la personalidad de un individuo, su rendimiento laboral, crédito, fiabilidad, conducta, etc,) y posteriormente se tomen decisiones individuales que les

[82] El TS considera que "el secreto médico es una modalidad de secreto profesional, un medio para proteger derechos fundamentales, pero no un derecho fundamental en sí mismo, sino un deber enderezado a evitar intromisiones ilegítimas en el ámbito de protección de la LO 1/82, de 5 de mayo". STC, de 2 de julio de 1991.

[83] En la Recomendación R (85) 20 del Comité de Ministros del Consejo de Europa se reconocía en el apartado 4 el derecho de toda persona a negarse a que sus datos sean incluidos en una lista de prospección comercial, a que los que figuren en esas listas sean cedidos a terceros, y a que tales datos sean borrados de las listas de prospección; vid. también: Art. 14 de la Directiva comunitaria y art. 8, *c)* del Convenio 108.

[84] Art. 17 LOPD.

[85] Art. 14, *a)*.

[86] Art. 13.1 LOPD.

afecten y con efectos jurídicos en base únicamente a un tratamiento automatizado de éstos. Se exceptúa de este supuesto el consentimiento contractual a que esa evaluación sea realizada, o bien que sea necesario para salvaguardar sus intereses legítimos, o, en último caso, cuando esta actividad esté autorizada por ley. De este modo el interesado tiene derecho a conocer la lógica aplicada a la decisión, y asimismo se traslada a los Estados la obligación de adoptar medidas para proteger el interés legítimo de la persona[87].

B. Aplicación de la normativa sobre protección de datos

La Agencia Española de Protección de Datos interpreta de forma extensiva la expresión de datos que hagan referencia al origen racial, a la salud y a la vida sexual del interesado.

Merece una referencia especial el concepto de dato de salud por su trascendencia en la vida empresarial y ante el silencio de la LOPD. La Agencia de Protección de Datos definió el concepto conforme a lo dispuesto en el Convenio 108 en la Recomendación número R(97) 5, del Comité de Ministros del consejo de Europa, referente a la protección de datos médicos. De una lectura conjunta de ambos textos se desprende que un dato de salud es cualquier información relativa a la salud pasada, presente y futura, física o mental, de un individuo, incluyendo informaciones relativas al abuso del alcohol o al consumo de drogas[88], así como las informaciones genéticas. En esta categoría se incluyen también los datos psicológicos, extraídos de expedientes médicos, las propias manifestaciones de los sujetos encuestados o las apreciaciones del encuestador ante las citadas afirmaciones.

Es interesante destacar en este punto el criterio del Tribunal de Justicia de las Comunidades Europeas en su sentencia Lindqvist, de 6 de noviembre de 2003, que dictamina que: "la indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud en el sentido del artículo 8, apartado 1 de la Directiva 95/46". La sentencia utiliza el concepto de salud incluido en el artículo 8.1 de la Directiva 95/46/CE "de modo que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona".

Más concretamente, el Reglamento 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Datos de Carácter Personal, incorpora una definición de datos de carácter personal relacionados con la salud que resulta una copia

[87] Art. 13.3 LOPD

[88] La AEPD califica de dato de salud la indicación de que una persona es drogodependiente y de la sustancia que consume, teniendo en cuenta la relación directa entre esos datos y la asistencia prestada por el responsable del tratamiento. Informe 182/2004 de la AEPD.

literal del apartado 45 del Convenio 108 del consejo de Europa de 1981, Así, en su artículo 5.1, g) se refiere a estos datos incluyendo en su ámbito las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

La indicación del grado de minusvalía para la aplicación del, por ejemplo, cálculo de retenciones del IRPF, las fechas de alta y baja de los trabajadores por enfermedad, la indicación de baja por maternidad, incluso si se asocia a un código que identifique la causa de la baja con una enfermedad profesional, una accidente laboral o una enfermedad común son considerados como datos de salud.

En cualquier caso, la empresa no podrá acceder a la información sanitaria resultante de los tratamientos dirigidos a la prevención de riesgos laborales, dado que la finalidad que se persigue es la promoción de la salud del trabajador y por lo tanto, en ningún caso le otorga poder para disponer sobre los datos recabados al trabajador. Tampoco se podrá subcontratar el control del absentismo laboral en base al seguimiento del estado de las enfermedades comunes de sus empleados si no cuenta con en consentimiento expreso de los mismos (Resolución R/00262/2005 AEPD).

Al contrario, la mera indicación de la condición de fumador, sin indicar la cantidad consumida, no es un dato de salud en cuanto no se puede evaluar si este consumo es abusivo (Informe 129/2005 de la AEPD).

- *El tratamiento de datos del historial clínico*

El artículo 8 de la LOPD autoriza a las instituciones y centros sanitarios públicos y privados y a los profesionales correspondientes el tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo previsto en la legislación estatal o autonómica sobre sanidad.

No obstante esta autorización no puede interpretarse de forma genérica sino que su alcance debe limitarse a los dos supuestos en los que únicamente será de aplicación:

1. Cuando una disposición normativa así lo disponga con carácter específico, o bien,
2. En los casos previstos en el artículo 7.6 de la LOPD (prevención o diagnóstico médico, prestación de asistencia sanitaria, tratamientos médicos o gestión de servicios sanitarios) cuando resulte necesario e imprescindible y se justifique en cada caso concreto.

La aprobación de la Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de los derechos y obligaciones en materia de información y documentación clínica, fija como objetivo adaptar la Ley General de Sanidad 14/1986, de 25 de abril, a la situación actual y concretar los derechos u las obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias. La Ley relativa a la Autonomía del Paciente permite de este modo resolver dudas relativas al tratamiento de datos de salud incluidos en los historiales clínicos de los pacientes.

La historia clínica es el conjunto de documentos que contienen datos, valoraciones e informaciones de cualquier índole sobre la situación evolución clínica de un paciente a lo largo de un proceso asistencial (artículo 4). Se trata, por tanto, como a continuación concreta la propia Ley (artículo 14.1), de un fichero en el cual se recogen todas las informaciones relativas a los cuidados médicos que se prestan al paciente durante su estancia en el centro sanitario.

La finalidad de estos tratamientos se dirige a facilitar la asistencia sanitaria dejando constancia de aquellas informaciones que a juicio del médico permitan un conocimiento del estado de salud del paciente. La configuración del historial clínico, junto con la inclusión en la propia ley de su contenido mínimo y de la finalidad del mismo, responde a las previsiones del artículo 4.2 de la LOPD.

La segunda cuestión que resuelve la Ley 41/2002 es la relativa al responsable del tratamiento. Si bien es cierto que el profesional sanitario debe colaborar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial, el centro sanitario es el responsable de la gestión y custodia de los historiales clínicos (artículo 17.4).

¿Quiere esto decir que el profesional sanitario no es responsable de la gestión y custodia de sus historiales clínicos?. En este sentido, resulta de interés la Sentencia de la sección octava de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid, de 12 de julio de 2000. En este supuesto el Tribunal estima el recurso contencioso-administrativo interpuesto por un profesional médico contra la resolución de la Agencia Española de Protección de Datos que impuso una sanción de carácter grave por obstrucción de la actividad inspectora.

La sentencia se fundamenta para estimar el recurso en el hecho de que los datos se encuentran incorporados a un fichero mantenido por personas físicas con fines exclusivamente personales, relacionándolo con el deber de secreto del profesional de la medicina y deben ser compatibles con las normas de protección de datos permitiendo el ejercicio del derecho de acceso, limitando el acceso a la información sensible a terceros.

Cuando el profesional sanitario trabaja por cuenta de un centro sanitario no es considerado como responsable del tratamiento de los datos que componen el historial clínico, con independencia de su deber de colaborar en la actualización de los datos a fin de cumplir el principio de calidad de los mismos.

En cualquier caso, por tanto, las historias clínicas cualquiera que sea el formato en que se encuentren deben cumplir las medidas de seguridad previstas en el Reglamento 1720/2007, de 21 de diciembre.

- El tratamiento de datos genéticos

El Reglamento 1720/2007, de 21 de diciembre, recoge por primera vez la información genética dentro de los datos relacionados con la salud confiriéndole así la protección reforzada que la LOPD reserva a los datos especialmente protegidos.

Esta inclusión responde a las numerosas preocupaciones que los últimos descubrimientos del ADN humano han suscitado. Se trata de una cuestión de afecta de lleno al derecho fundamental a la protección de datos. A estos efectos la Agencia Española de Protección de Datos ya se había pronunciado en relación a una consulta planteada sobre la viabilidad de la creación de diversos ficheros que contengan muestras genéticas para la identificación de cadáveres de personas desaparecidas[89] y recordó que *los datos genéticos tienen la consideración de datos de salud*, independientemente del carácter codificante o no del análisis del ADN.

Por dato genético se entiende *todo dato, cualquiera que sea su clase, relativo a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no*[90].

Por su parte, la Declaración Internacional sobre Datos Genéticos Humanos de la UNESCO (DIDGH) los define como información sobre las características hereditarias de las personas, obtenida por el análisis de ácidos nucleicos u otros análisis científicos (artículo 2 i).

Un sector mayoritario considera, al igual que el Parlamento Europeo, que el tratamiento de los datos genéticos en el sector seguros debe estar prohibido y no ser autorizado, salvo en circunstancias excepcionales previstas en una

[89] Recogido en la Memoria del año 2000 de la Agencia Española de Protección de Datos.

[90] Recomendación nº R (97) 5 del Consejo de Europa

Ley. En la Unión Europea el uso de datos genéticos con fines aseguradores no responde a ninguna de las finalidades legítimas que permiten el tratamiento de datos. Tampoco la LOPD reconoce ninguna habilitación a favor de las entidades aseguradoras que legitime este tratamiento, ni siquiera en las normas sectoriales relativas al tratamiento de datos de salud. Por tanto, las aseguradoras no pueden solicitar al tomador del seguro que se someta a un análisis genético ni antes, ni durante, ni después de la negociación del seguro, ni tampoco que se le comuniquen los resultados de datos genéticos realizados con anterioridad.

La posibilidad de discriminación en este terreno es muy elevada y puede conllevar la no obtención de la póliza por parte del cliente o de su familia en función del perfil genético. Esto llevaría a que no se asegurara o a que se obligará a pagar primas extras, declarando el riesgo como inasegurable y todo ello sobre la base de un único elemento: el posible riesgo de una enfermedad que puede que no se manifieste nunca[91].

También se ha manifestado en este sentido el Parlamento Europeo señalado que: a reducción de las posibilidades de recurrir a los seguros de vida o enfermedad a causa de la utilización de datos genéticos dará lugar a nuevas jerarquías sociales mediante la clasificación de los individuos en función de su predisposición genética, lo que se traduciría en una auténtica reducción de ciudadanía y en la negación del derecho de un acceso equitativo a una asistencia médica de calidad[92].

En suma, los datos genéticos únicamente pueden ser tratados atendiendo al fin legítimo del tratamiento, siendo cancelados en caso de cumplirse éste y no siendo posible conservarlos para otros fines y mucho menos elaborar perfiles genéticos de la población, lo que se denomina codificación genética o mantener bancos de ADN obtenidos sin el consentimiento del interesado.

La creación de este tipo de ficheros debe ser lo más específica posible y la conservación de este tipo de datos sólo sería posible en el caso de que una norma con rango de Ley lo permitiese, sobre la base del artículo 7.3 de la LOPD.

- *El tratamiento de datos biométricos*

Los datos biométricos son datos de identificación de rasgos fisiológicos o de comportamiento de una persona viva que presentan tres características:

[91] Mangialardi,E.: "El proyecto genoma humano y el seguro de personas", en *Revista Española de Seguros,* nº 1005, enero-marzo 2001, pp. 7-19.

[92] Informe del Parlamento Europeo sobre las repercusiones éticas, jurídicas, económicas y sociales de la genética humana. Final A5-0391/2001, 8 de noviembre de 2001.

1. *universales*, dado que el elemento biométrico esta presente en todos los individuos,
2. *únicos*, puesto que se trata de un elemento propio de cada individuo,
3. y/o *permanentes*, puesto que cada persona conserva a lo largo de su vida dicha característica.

Los datos biométricos (relativos a la huella digital o al ADN) se utilizan fundamentalmente con fines de identificación y autenticación fiables, si bien los riesgos de la generalización de su uso lleva a plantear las mismas preocupaciones e inquietudes en relación al individuo puesto que aún se desconocen las posibilidades informativas que el uso de esta tecnología puede suponer para el titular de los datos, aumentando el riesgo de elaborar perfiles exhaustivos de las personas[93].

Existen hasta el momento dos técnicas biométricas que permiten definir las características del sistema que se emplee. La primera técnica se basa en el aspecto físico y en la fisiología de cada persona. Se comprueban las huellas dactilares, el análisis de la imagen del dedo, se reconoce el iris, se analiza la retina, se hace un reconocimiento facial, la geometría de la mano, se reconoce la forma del oído, se detecta el olor corporal, se hace un reconocimiento vocal, se analiza la estructura del ADN, los poros de la piel, etc. La segunda, se fija en el comportamiento: comprobación de la firma manuscrita, análisis del tecleado, del andar, etc.

La cuestión al respecto es determinar el régimen aplicable a los datos biométricos. La posición mayoritaria aboga por incluir estos datos como datos sensibles, receptores de la protección especial que confiere la LOPD; sin embargo, esta consideración supondría una modificación de nuestra legislación, puesto que ni siquiera el nuevo Reglamento 1720/2007 aprovecha la ocasión para incorporar a los datos biométricos dentro de los datos de salud como ha ocurrido con los datos genéticos.

Los datos de huella digital, por ejemplo, son datos biométricos considerados como datos de carácter personal por la Agencia de Protección de Datos Española y no contienen ningún aspecto concreto de la personalidad, sino que su función se limita a identificar a la persona, por lo que su tratamiento no tiene mayor trascendencia que el de los datos relativos a un número de identificación personal. Por otro lado, este tratamiento puede quedar fuera de la obligación de recabar el consentimiento previo por acogerse a la excepción incluida en el artículo 6.2 de la LOPD que dispone que el consentimiento del interesado no es preciso cuando los datos "se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o

[93] *Tratamiento de Datos Especialmente Protegidos,* en: Estudio Práctico sobre la Protección de Datos de Carácter Personal, ALMUZARA, C y otros. Editorial Lex Nova, Valladolid, 2007.

un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato"[94].

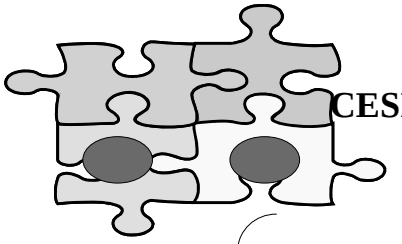
La Agencia Española de Protección de Datos se pronunció también sobre la legitimidad de los tratamientos de datos biométricos con fines identificativos en su Memoria del 2001 señalando que la utilización de datos biométricos entendidos como "aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión, no tiene mayor impacto en la intimidad de los ciudadanos que otras técnicas tradicionales de identificación menos exactas que se emplearon con anterioridad".

Por tanto, cuando los datos biométricos se traten con fines exclusivamente identificativos, respetando los principios de protección recogidos en la LOPD, no suponen ningún riesgo añadido para los derechos y libertades de los individuos teniendo en cuenta que no proporcionan información sobre la personalidad de individuo. *A sensu contrario*, el tratamiento puede poner en peligro el derecho fundamental de los afectados cuando el tratamiento de dichos datos pueda proporcionar información sobre la personalidad del individuo[95].

[94] Memoria de la Agencia Española de Protección de Datos de año 1999, en relación a la legitimidad del tratamiento de los datos de huella digital de trabajadores para fines de control del absentismo laboral, pp. 403-404.

[95] Grupo de Trabajo del artículo 29. Tratamiento de datos biométricos, 1 de agosto de 2003. WP80. La Comisión es consciente de la evolución de las técnicas de recogida y tratamiento de datos de carácter personal sin que los interesados sean conscientes de ello, si bien considera que es necesaria una aplicación flexible de la Directiva 95/46/CE, de Protección de Datos personales, para conseguir el objetivo de proteger los derechos y libertades de los afectados, sin que sea necesario, de momento, una modificación de la norma.

8. CESIÓN DE DATOS



Fuente: elaboración propia

8.1. Regulación

La cesión o comunicación de datos aparece recogida en la norma española dentro del Título II dedicado a los Principios de Protección, ampliando de este modo el catálogo recogido en la norma comunitaria en el sentido de otorgarle categoría de principio mientras que la Directiva se refiere a la cesión de datos como un supuesto más de uso de datos personales.

Frente a la exigencia del consentimiento que ya figura en la Directiva, la norma nacional incluye varias excepciones. La primera es la excepción legal a la que no se alude en la Directiva. Tampoco es necesario el consentimiento cuando los datos de carácter personal se recaben para el ejercicio de las funciones propias de las Administraciones públicas, o cuando los datos figuren en fuentes accesibles al público.

Diferente tratamiento reciben el resto de las excepciones contenidas en la ley respecto a la norma europea. Mientras ésta última dispone que sólo podrá efectuarse el tratamiento (entendido en sentido amplio) si es necesario para la ejecución de un contrato en el que el interesado sea parte (la ley española concreta el alcance del precepto en los siguientes términos: *"cuando se*

refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesario para su mantenimiento o cumplimiento"), o para el cumplimiento de una obligación jurídica, o bien para proteger el interés vital del interesado, la ley española admite esos tratamientos sin necesidad de que el interesado de su consentimiento.

También para estos casos en que no es necesario el consentimiento del afectado para el tratamiento de sus datos, la LOPD ha previsto una protección suplementaria (art. 6.4) que viene dada por la *facultad de oposición* que se reconoce al interesado cuando concurran motivos fundados y legítimos (Derecho reconocido en la Directiva comunitaria en el art. 14, *a)* como derecho independiente).

La LOPD define en su artículo 3, i), la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado". Más adelante, el artículo 11 de la misma ley regula el principio de cesión de datos bajo el título: comunicación de datos señalando que:

> *Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*

La regla general para la cesión o comunicación de datos es, por tanto, el consentimiento del interesado. Para que el consentimiento sea válidamente otorgado es necesario que se haya informado al interesado de la finalidad a la que se destinarán los datos y la actividad del cesionario.

En cualquier caso el consentimiento para la comunicación o cesión tiene carácter revocable.

Si se procede a la disociación de los datos como paso previo a la cesión o comunicación no será necesario ni siquiera informar sobre extremo al interesado.

8.2. Excepciones

El consentimiento exigido en el apartado anterior no será preciso (art. 11) LOPD:

- Cuando la cesión está autorizada en una Ley.
- Cuando se trate de datos recogidos de fuentes accesibles al públicos.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión 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.

- 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.
- Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- 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 de sanidad estatal o autonómica.

El **Reglamento 1720/2007**, de 21 de diciembre, amplía el catálogo de excepciones eximiendo del consentimiento cuando así lo autorice no sólo una norma con rango de ley sino también una norma de derecho comunitario y, en particular, cuando concurran alguno de los supuestos siguientes:

- que la cesión tenga por objeto la satisfacción de un interés legítimo del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades de los interesados en relación a la protección de su datos personales, y especialmente en lo que se refiere a su honor o a su intimidad personal y familiar.
- Que la cesión de datos sea necesaria para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

Cuando se trate de datos que figuran en fuentes accesibles al público, el nuevo Reglamento concreta el alcance de la redacción dada por la LOPD y limita la excepción del consentimiento a los casos en que el tercero al que se comuniquen los datos tenga un interés legítimo para su conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado. La norma aún resulta más restrictiva con las Administraciones Públicas, exigiendo para ellas una habilitación con rango de ley para realizar comunicaciones de datos recogidos de fuentes públicas (artículo 10.2, b)).

En relación de las comunicaciones hechas al Defensor del Pueblo, Ministerio Fiscal o Jueces y Tribunales del de Cuentas, el Reglamento amplia el ámbito de excepción a las instituciones autonómicas que tengan funciones análogas a los anteriores que se desarrollen en el marco de las funciones que le atribuye expresamente una ley (art.10.4, b)).

También se encuentran exceptuadas del consentimiento la cesión de datos recogidos o elaborados por una Administración Publica con destino a otra o cuando la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias(art. 10.4,c)).

En relación a los datos de salud, el Reglamento vuelve a recordar la ausencia de consentimiento para la comunicación de datos incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

8.3. Consentimiento

Como se ha visto en el apartado dedicado al consentimiento la LOPD sólo exige el consentimiento expreso para el tratamiento de los datos especialmente protegidos que hagan referencia al origen racial, a la salud y a la vida sexual; y el consentimiento expreso y por escrito para los datos que revelen ideología, afiliación sindical, religión o creencias. Por tanto, la obligación general de exigir el consentimiento no tiene porque ser necesariamente expresa y puede otorgarse utilizando cualquiera de las formas admitidas en derecho. En este sentido, el nuevo Reglamento viene a aclarar el alcance de esta obligación incorporando un procedimiento voluntario de recogida del consentimiento que fomenta el de carácter tácito (no aplicable a los datos especialmente protegidos).

Con todo, una correcta solicitud del consentimiento por parte de la entidad aseguradora debe especificar el cesionario al que van a comunicarse los datos o el tipo de actividad de aquél al que se pretendan comunicar (art. 11.3 LOPD).

En este sentido, uno de los problemas que más se plantean es el del consentimiento para la cesión de datos entre empresas pertenecientes al mismo grupo[96].

A pesar de los intentos de modificar la LOPD en el sentido de no exigir el consentimiento para la cesión de datos personales de los clientes dentro del mismo grupo empresarial, hoy por hoy las comunicaciones de datos entre empresas del mismo grupo empresarial tienen el mismo tratamiento que si estás se efectúan con terceros (derecho de información y consentimiento).

El Reglamento ha introducido una importante paradoja en el artículo 70.4 que exige la autorización del Director de la Agencia Española de Protección de Datos para las transferencias de datos personales a Estados que no proporcionan un nivel adecuado de protección entre empresas del mismo grupo cuando se hubiesen adoptado normas internas vinculantes en que consten las necesarias garantías de respecto a la normativa de protección de datos.

[96] www.agpd.es/Canal_Documentacion/InformesJuridicos.

El Director de la Agencia está obligado a dictar y notificar la resolución expresa en un plazo de tres meses, pasado el cual, se entiende autorizada la transferencia internacional de datos. Por tanto, el Reglamento incorpora la curiosa paradoja de prohibir las comunicaciones de datos personales, por ejemplo, dentro de la misma ciudad o el mismo país si no se garantizan las medidas de seguridad y, sin embargo, permite la transferencia a Singapur, con total ausencia de garantías para el titular de los datos .

La Audiencia Nacional en su Sentencia de 11 de enero de 2002[97] ratificó la sanción impuesta por la Agencia de Protección de Datos a una entidad por utilizar los datos de un cliente que expresamente había solicitado que no se le enviase publicidad de la entidad recurrente. Esta entidad argumentó que los datos solicitados se obtuvieron de los ficheros de tres empresas pertenecientes a su grupo, que junto con otras sociedades se fusionaron y cambiaron su denominación social a nombre de la entidad recurrente. La Audiencia Nacional manifiesta que la entidad recurrente interpretó que el solicitante se refería a la publicidad de la empresa con la que el solicitante había firmado el contrato pero no a las entidades vinculadas. Si dicha entidad integra el dato en un fichero de grupo no se puede entender que la posterior revocación del consentimiento afecte sólo a la entidad que firmó el contrato con el solicitante y no a las demás entidades integradas en el grupo y que tienen acceso al fichero porque las formas de organización de las empresas no pueden suponer una disminución de los derechos del titular de los datos.

La interpretación debe ser la contraria: “la revocación del consentimiento es referida al uso del dato en el fichero, lo que implica que el dato ha de tener un tratamiento homogéneo en el fichero y por ello que todas las entidades del grupo con acceso al fichero quedan vinculadas del consentimiento y a la forma autorizada del tratamiento del dato”.

Por lo tanto, para proceder a la cesión de datos del solicitante se debería haber obtenido su consentimiento informado en el que se detallara el cambio de denominación del grupo y la posibilidad de que sus datos fueran utilizados por el resto de las empresas del nuevo grupo.

En conclusión, son tres los requisitos necesarios para que el titular de un fichero pueda cederlos o comunicarlos a un tercero[98] (o a empresas de su grupo):

1. consentimiento previo del afectado,
2. que la cesión se relacione con el cumplimiento de los fines del cedente,
3. que la cesión se relacione también con los fines del cesionario.

[97] Núm. Rec. 432/2000.

[98] Sentencia de la Sala Tercera del Tribunal Supremo, de 31 de octubre de 2000 (núm. rec. 519/1994).

En el mismo sentido cabe destacar la Sentencia de la Audiencia Nacional de 22 de junio de 2005[99] en relación a la cesión de datos entre empresas del mismo grupo para la promoción, captación y seguimiento de su cartera de clientes. Se alega que la comunicación se realiza al amparo del artículo 12 de la LOPD que lo permite cuando se trata de una prestación de servicios; sin embargo, no puede admitirse que sea tal puesto que UFM se apodera de los datos de los clientes de UFD y los utiliza para los fines propios relacionados con su propia actividad comercial, incluso hasta el punto de que cede dichos datos a otras entidades diferentes y a efectos de la prestación de seguros. Una cosa es, a efectos civiles, la habilitación para actuar en nombre de otro, y otra cuestión es que con el pretexto de esa habilitación se traten datos personales, lo cual se ha de hacer observando los requisitos que exige la legislación de protección de datos.

En este caso *no hay prestación de servicios* en el sentido del artículo 12 de la LOPD, que permite que un tercero pueda tratar los datos de carácter personal por cuenta o encargo de otro, sino que estamos ante una auténtica cesión de datos a tercero. *En el momento que UFM utiliza los datos cedidos en provecho propio,* conservando los archivos y usándolos después para el envío de publicidad y la captación de clientes, comunicándolos, incluso a terceros, *se convierte en titular y responsable del tratamiento*.

Otro ejemplo dentro del sector asegurador nos lo ofrece la Sentencia de la Audiencia Nacional de 20 de mayo de 2005 en la que se sanciona a una empresa reaseguradora por infracción del artículo 11 de la LOPD y a una segunda empresa que valora la situación de enfermedad por infracción del deber de consentimiento del artículo 6 de la Ley. La Sala consideró que la relación jurídica entre la empresa aseguradora y reaseguradota no podía considerarse incluida en el artículo 12 de la LOPD al no haber suscrito entre las mismas un contrato por escrito donde se recogieran los requisitos previstos en el citado artículo.

Por tanto, la cesión de datos de un asegurado por su empresa aseguradora a otra con la que tiene contratado un reaseguro, no tiene cabida en los artículos 11 y 12 de la LOPD, por lo que en el caso anterior se precisa el consentimiento del interesado.

8.4. La comunicación de la cesión de datos

La comunicación de la cesión de datos del interesado aparece recogida en el artículo 27 de la LOPD en los siguientes términos:

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando,

[99] Núm. rec. 744/2003.

asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por Ley.

También es preciso tener en cuenta otros dos artículos de la LOPD. En concreto el artículo 15.1 y el 16.4 de la Ley. El primero, relativo al derecho de acceso, establece la obligación de comunicar al afectado, en el ejercicio del derecho de acceso, las comunicaciones que se hayan realizado de sus datos o que se prevea realizar.

En este sentido 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.

Por su parte, el artículo 16.4 de la Ley se refiere al derecho de rectificación y cancelación y dispone que:

> *Si los datos rectificados o cancelados no hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se haya comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación*.

Con todo, del análisis de la casuística de la Agencia de Protección de Datos resulta sorprendente las escasas ocasiones en que ésta ha exigido el cumplimiento de la citada obligación. Una de estas ocasiones se produjo en la sanción por falta grave a una entidad bancaria por incumplimiento del artículo 27 en atención a los siguientes hechos: la entidad bancaria cedió a otra entidad bancaria un contrato de préstamo en virtud de Escritura Pública de Cesión de Crédito y Tansmisiones de Activos. En esa escritura pública se establecía que la notificación al deudor de la cesión y el cambio de titularidad registral será asumida por la entidad cedente. No obstante no hay constancia de que se haya realizado dicha notificación siendo ésta preceptiva en virtud del artículo 27 de la LOPD.

Ante el recurso presentado por la entidad bancaria, la Audiencia Nacional, en su Sentencia de 21 de septiembre de 2005[100] se pronunció en contra de la Agencia de Protección de Datos al considerar que la cesión del crédito mercantil y su puesta en conocimiento, a efectos mercantiles, así como la información o comunicación a efectos de la LOPD, responden a normas jurídicas con finalidades y consecuencias distintas. Por lo que la conducta

[100] Núm. Rec. 697/2003.

imputada a la entidad bancaria no tiene encuadre en el tipo descrito en el artículo 27.

Sin embargo, en otras ocasiones la Audiencia Nacional ha ratificado el criterio de la Agencia. En concreto ese mismo año resuelve el recurso nº 843/2003 por el que confirma la sanción impuesta al cesionario (Banco F) al no acreditar el consentimiento del afectado, prestatario en el contrato de préstamo en que se subrogaba, en los términos del artículo 6.1 de la LOPD. En este caso no cabe aplicar ninguna de las excepciones del artículo 6.2 (no es necesario el consentimiento cuando los datos de carácter personal se recojan por las partes de un contrato y sean necesarios para su cumplimiento o mantenimiento) puesto que los datos personales de un negocio bancario concreto (en este caso contrato de préstamo) no se refieren a las partes del otro contrato, relativo a la transmisión de parte del negocio bancario de una entidad de crédito a otra en virtud de la referida cesión de créditos.

8.5. Datos disociados

El último apartado del artículo 11 de la LOPD establece que no será aplicable todo lo previsto en el mismo respecto a la comunicación de datos si previamente se efectúa un procedimiento de disociación.

El procedimiento de disociación consiste en todo tratamiento de datos personales, de modo que la información que se obtenga no pueda asociarse a una persona determinada o determinable (artículo 3, f) LOPD); sin embargo, para que exista disociación no es necesario que la identificación se haya producido sino que es suficiente con que esta se permita o sea posible.

Mediante el procedimiento de disociación se elimina la conexión entre el dato y la persona, se "despersonaliza" el dato impidiendo su identificación constituyendo, de este modo, una barrera protectora de la intimidad del afectado.

Por el contrario, para que exista un dato de carácter personal no es imprescindible una total correspondencia entre el dato y la persona, sino que es suficiente con que pueda realizarse esa identificación sin que ello conlleve esfuerzos desproporcionados, como se desprende del artículo 3 en sus apartados a) y f) y así lo ha corroborado la Audiencia Nacional en su Sentencia de 8 de marzo de 2002[101].

En este caso la Sala analizó la denuncia de un Comité de empresa por la realización de llamadas telefónicas a sus empleados por parte de una agencia encuestadora al que la empresa había facilitado los datos. La empresa

[101] Núm. Rec. 948/2000.

recurrente alega que los datos personales fueron sometidos a un procedimiento de disociación previo a su comunicación; sin embargo la Audiencia los consideró como auténticos datos personales al contener información sobre personas identificables ya que con la edad, sexo, destino, cargo y teléfono de los empleados, es posible sin grandes esfuerzos la identificación de las personas a las que se refieren esos datos.

9. PRESTACIÓN DE SERVICIOS

La prestación de servicios se recoge en la LOPD bajo la expresión "Acceso a los datos por cuenta de terceros". El artículo 12 señala que:

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la *prestación de un servicio* al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras empresas.
   En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley, que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice con incumplimiento de las estipulaciones del contrato, será considerado también responsable del tratamiento respondiendo de las infracciones en que hubiera incurrido personalmente.

El prestador de servicios aparece recogido en el artículo 3, g) de la LOPD bajo la expresión encargado del tratamiento, tal y como aparece en la Directiva 95/46 de Protección de Datos, y que se refiere a la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Por tanto, la LOPD califica jurídicamente la prestación de servicios como diferente de la cesión de datos sin que sea necesario, en este caso, el consentimiento del afectado. La regulación del encargado del tratamiento

constituye una excepción extraordinaria al artículo 11.1 (comunicación) lo que justifica su interpretación restrictiva.

De ahí que la propia Ley imponga un conjunto de requisitos materiales que deben cumplirse para garantizar los derechos de los titulares de los datos, hasta el punto que su incumplimiento llevaría a tipificar la actuación de cesión y de tratamiento ilícito de datos. Cuando se contrate con un tercero la realización de una prestación de servicios deberán tenerse en cuenta los siguientes extremos:

1. El contrato debe celebrarse por escrito[102], donde quede perfectamente detallada, la necesidad, el objeto, el ámbito, en el que se va a desarrollar la prestación de los servicios solicitada por el responsable del tratamiento.
2. Dar las instrucciones necesarias para la realización del servicio de la manera más concreta y delimitada posible.
3. Establecer en el contrato los fines concretos para los que serán tratados los datos. Establecer expresamente que el prestador de servicios no debe comunicar los datos a terceros, ni siquiera para su conservación.
4. Fijar las medidas de seguridad necesarias que el prestador de servicios está obligado a cumplir.
5. Delimitar el tiempo de ejecución en que la prestación de servicios se considere finalizada.
6. Asegurarse del cumplimiento de la obligación por parte del prestador de servicios en lo que se refiere a la devolución o destrucción de los datos o soportes a los que se permite el acceso, concretando si se van a destruir o devolver los datos, y en su caso, la fecha en la que se llevará a cabo cualquiera de estas medidas.
7. Guardar secreto profesional durante la prestación de los servicios, así como una vez finalizados.
8. Comunicar y hacer cumplir a sus empleados, incluidos, en su caso, las empresas de trabajo temporal, las obligaciones establecidas en el contrato y, en concreto, las relativas al deber de secreto y las medidas de seguridad.

Insistimos que en toda prestación de servicios resulta relevante que el poder de disposición de los datos personales no sea transmitido a un tercero puesto que en este caso estaríamos ante una cesión o comunicación de datos ya sea temporal o definitiva. Ello impide la posibilidad de proceder a una subcontratación lo que se justifica en el riesgo que supone para el interesado una cadena de prestación de servicios en la que se difuminara el control de la

[102] La importancia del carácter escrito de estos contratos ha sido puesta de manifiesto en diferentes sentencias de nuestros tribunales. A modo de ejemplo podemos citar la Sentencia de la Audiencia Nacional núm. 6201/2000, de 15 de noviembre (núm. Rec. 732/2000) o más recientemente la Sentencia de 18 de enero de 2006, del mismo Tribunal (núm. Rec. 225/2004) por la que se impone una multa de 60.101,21 euros a la empresa responsable del fichero y de 60.121,21 a la empresa prestadora del servicio, al no recogerse en el contrato referencia alguna a la LOPD ni a sus exigencia para el tratamiento de datos por tercero.

localización y el alcance del tratamiento de los datos hasta vaciar de contenido el derecho a la autodeterminación informativa.

En consecuencia, si el responsable del fichero o del tratamiento desea la prestación de servicios por parte de varias entidades deberá contratar dichos servicios con cada una de ellas. Por tanto, para que se pueda aceptar la subcontratación del tratamiento derivado del artículo 12 de la LOPD, deben cumplirse los siguientes requisitos que, además deberán figurar en el contrato[103]:

- Que los servicios a subcontratar se hayan previsto expresamente en el contrato originario celebrado entre el prestador y prestatario del servicio,
- Que el contenido preciso del servicio subcontratado conste en el contrato originario.
- Que el responsable del tratamiento establezca las instrucciones mediante las cuales el subcontratista tratará los datos.
- Que en el contrato originario se establezcan las medidas de seguridad a adoptar por el subcontratista.

Una novedad importante que introduce el Reglamento 1720/2007 es la conveniencia de incluir en el contrato una cláusula en el sentido del artículo 26 autorizando a atender las solicitudes de acceso, rectificación y cancelación al encargado del tratamiento o bien que se pueda solicitar al responsable del fichero (por parte del encargado) la remisión de la solicitud cumplimentada en el plazo de diez días.

10. OBLIGACIONES DEL RESPONSABLE DEL FICHERO O DEL TRATAMIENTO

Sobre el responsable del fichero recae el cumplimiento de todas las obligaciones que se han ido analizando en este Capítulo y que se reducen a dos: información y consentimiento, que, a su vez, constituyen derechos para el titular de los datos, de los que parten los demás previstos en la Ley: forma de recogida de los datos, tratamiento de datos y cesiones.

En relación al consentimiento en las relaciones on-line la entidad aseguradora responsable del tratamiento de los datos debe:

1. Facilitar y promover la consulta anónima de sitios comerciales sin solicitar a los usuarios que se identifiquen mediante su nombre, apellidos, dirección electrónica u otros datos.

[103] Informe 582/2004 de la Agencia de Protección de Datos, disponible en la página *web* de la Agencia Española de Protección de Datos:
www.agpd.es/Canal_Documentacion/InformesJuridicos.

2. Cuando sea necesario establecer un vínculo con el usuario sin que sea necesario su identificación completa, aceptar y proponer el uso de todo tipo de seudónimos, incluso para determinadas transacciones, por ejemplo utilización de certificaciones con seudónimos para firmas electrónicas.

3. Concretar el período de almacenamiento para los datos recogidos.

4. emprender las acciones necesarias para garantizar la seguridad de los datos no sólo en la recogida, sino en el tratamiento y la transmisión.

5. Cuando participe un encargado de tratamiento, por ejemplo para alojar un sitio web, debe firmarse un contrato en el que se exija a este encargado que garantice las medidas de seguridad necesarias al nivel de protección de los datos.

6. Al transferir datos a terceros países se debe notificar este extremo a la Agencia de Protección de Datos e incluir el número de registro de la notificación en el sitio, preferentemente bajo el apartado dedicado a la protección de datos.

7. En caso de transferir datos a países terceros que no garanticen un nivel de protección adecuado, el responsable del tratamiento debe garantizar que la transferencia de datos sólo se produce cuando se cumplen las excepciones previstas en la LOPD, y en cualquier caso informar al cliente de las garantías acogidas para asegurar la legalidad de la transferencia.

Por lo que se refiere a la cancelación de datos, el Informe de la Agencia de Protección de datos nº 283/2004 concluye que si bien no es posible la aplicación al encargado del tratamiento de los dispuesto en el artículo 16.3 (cancelación), cabría la posibilidad de que en el propio instrumento contractual en el que se funda la relación entre el responsable y el encargado se hiciese constar expresamente que las partes no considerarán cumplida la prestación a los efectos del artículo 12 de la LOPD hasta el momento en que el responsable del tratamiento manifieste expresamente su conformidad con la actividad desarrollada por el encargado del tratamiento, para lo que concederá un plazo máximo que también figurará en el contrato.

11. LA RESPONSABILIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

La responsabilidad en el tratamiento de los datos personales recae en el responsable del fichero dado que sus atribuciones coinciden con los límites del mismo, respondiendo, por tanto de los accesos no autorizados, de las pérdidas accidentales, de la destrucción o de la utilización fraudulenta o

contaminación por virus, siempre y cuando se demuestre que se le puede imputar el hecho que ha provocado el daño.

La Directiva 95/46/CE[104] presta una mayor atención a este principio, aunque sin calificarlo como tal. Así, reconoce el derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido (art. 23.1), y prevé la posibilidad de eximirle parcial o totalmente de la misma si se demuestra que no se le puede imputar el hecho productor del daño (art. 23.2). Por otro lado, la norma comunitaria se ocupa de la responsabilidad de la transferencia de datos dentro de la red[105]. En este sentido, si bien es cierto que la transmisión de datos reside en la propia naturaleza del fichero automatizado, el uso de las nuevas tecnologías facilita su acceso y, por tanto, la responsabilidad del encargado del fichero se extiende también a este ámbito.

En cuanto a la responsabilidad del encargado del fichero, se deduce del art. 9 LOPD[106] y expresamente se recoge en el art. 43, puesto que a él compete, con los matices analizados anteriormente, cumplir y hacer cumplir las medidas necesarias para garantizar el fichero y por tanto cualquier comportamiento que no se ajuste a este planteamiento permitirá exigir su responsabilidad.

[104] *Vid.*también la Directiva 2000/31/CE, relativa a los aspectos jurídicos de la Sociedad de la Información, en particular el comercio electrónico.

[105] Art. 17. "*Seguridad del tratamiento*. 1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados," (negrita mío) **" en particular cuando el tratamiento incluya la transmisión de datos dentro de una red**, y contra cualquier otro tratamiento ilícito de datos personales".

[106] *Vid.* también Ley 34/2002, de Servicios de la Sociedad de la Información y comercio electrónico.

Capítulo IV
LA IMPORTANCIA PARA EL SECTOR ASEGURADOR DE LA IDENTIDAD DE LAS PARTES EN EL ENTORNO DIGITAL

SUMARIO: 1. LA IDENTIDAD DEL CLIENTE EN LAS TRANSACCIONES COMERCIALES EN LA RED. 2. EL PRINCIPIO DE SEGURIDAD. 3. OBJETIVOS DE SEGURIDAD EN LAS COMUNICACIONES ELECTRÓNICAS DEL SECTOR ASEGURADOR.- 4. MEDIDAS DE SEGURIDAD APLICABLES A LOS FICHEROS Y TRATAMIENTOS. 4.1.- Categorías de medidas. 4.2.- Medidas concretas de seguridad.- A. Medidas generales y de nivel básico.- B. Medidas de nivel medio.- C. Medidas de seguridad intermedia.- D. Medidas de nivel alto.- 5. TÉCNICAS DE GARANTÍA DE LA SEGURIDAD EN LA RED. 5.1.- La firma digital. 5.2.- Los certificados digitales. 5.3.- La autenticación.

1. LA IDENTIDAD DEL CLIENTE EN LAS TRANSACCIONES COMERCIALES EN LA RED

En este apartado nos ocupamos de los problemas que surgen a la hora de identificar clientes en los supuestos relacionados con el comercio electrónico del sector asegurador dada la importancia de este tipo de relaciones y el interés que se presta a cuestiones como la confidencialidad, el no repudio y la seguridad.

Indudablemente la trascendencia a nivel mundial que el comercio electrónico tiene ofrece oportunidades desconocidas hasta hace diez años por las empresas y permite la promoción de aquéllas con menos medios. De este modo, las transacciones electrónicas mejoran la eficacia y efectividad de las empresas al poder ofrecer y vender sus productos en todo el mundo y ello con independencia de su tamaño o volumen de negocio, si bien desde el prisma de la privacidad, la consecución de los objetivos de las empresas puede arrastrar importantes lesiones para la protección de los usuarios.

No cabe duda que los riesgos principales que se derivan de estas transacciones electrónicas se conectan con el uso secundario no autorizado de los datos personales, pero también con las quiebras a la confidencialidad e incluso con la potencialidad de suplantar identidades. En este sentido, se está desarrollando una nueva forma de comercio que añade un peligro más a la privacidad del ciudadano. Nos referimos al comercio electrónico móvil que utiliza teléfonos móviles y conexiones a páginas web a través del *protocolo WAP* (protocolo de aplicación inalámbrica), lo que genera nuevos datos que ayudan a completar los perfiles que del consumidor se pueden elaborar[107].

[107] A modo de ejemplo, podemos hacer mención al proyecto conjunto desarrollado por Yahoo! Y CellPoint Systemas AB para comercializar un localizador personal usando teléfonos móviles. El sistema, denominado “Find-A-Friend”, permite la localización de personas gracias

Internet utiliza protocolos conocidos por todos y destinados a compartir información pues esta idea fue la que gestó la Red de Redes, de ahí que cierta pericia técnica en el uso de herramientas de programación configure el elemento intrínseco que permite suplantar personalidades o bien interceptar y desvelar los datos personales que circulan en la Red. Un ejemplo de estas tecnologías invasivas de la intimidad son los programas conocidos como *sniffers* que *olfatean* secuencias de dígitos que se parezcan a los de las tarjetas de crédito con el fin de conseguir los datos completos del titular de una tarjeta y realizar transacciones fraudulentas en la Red[108].

Otras prácticas muy extendidas son las del *phising* o el *pharming*. La primera es una técnica por la que los estafadores se hacen con los datos del usuario que les interesa a través de correos electrónicos en los que suplantan la identidad de un banco u organismo público. Para ello suelen solicitar las cuentas bancarias y las claves de acceso con el pretexto de actualizar las bases de datos o de hacer una devolución de la Agencia Tributaria.

A través del *pharming*, técnica más difícil de detectar, se infecta el ordenador del usuario con un virus *troyano* que redirige la página web que se visita (por regla general de una entidad bancaria) a la fraudulenta creada por el estafador con el objetivo de recabar datos confidenciales[109].

Frente a ello es aconsejable prestar especial atención a las redes P2P que constituyen una de las mayores fuentes de virus, no contestar a los mensajes de correo electrónico o *sms* que soliciten datos (sea cual sea su origen) y comprar en comercios electrónicos que utilicen servidores seguros

---

a la red GSM de este tipo de teléfonos, aunque requiere el previo consentimiento del interesado. Mas detalles de esta tecnología en: http://www.cellpt.com/v2/000504.htm.

[108] Este tipo de riesgos aconsejan contar con sistemas de seguridad informática que permitan conexiones seguras como las del tipo SSL, que consisten en el uso de sistemas de encriptación de datos como los que ofrece la firma digital, de las que se tratará más adelante en este trabajo, en el apartado dedicado al DNI electrónico. Otro sistema de seguridad informática lo proporcionan las intranets y otras redes como la VPN (virtual private networks) que establecen diálogos *tunelizados* entre máquinas que se reconocen recíprocamente. Vid. SUÑÉ LLINÁS, ob. cit., p. 7.

[109] Una de las últimas redes desmanteladas en España en febrero de 2008 en la denominada *Operación Ulises* consiguió estafar en Internet más de tres millones de euros. Parte de la red se dedicaba a realizar ventas o subastas de productos que nunca llegaban al comprador utilizando conocidas páginas de compraventa o creando sus propias páginas falsas. El otro grupo se dedicaba a efectuar transferencias bancarias de cuentas ajenas, sin consentimiento. La desaparición de las barreras físicas permite que los delincuentes se organicen desde distintos lugares, sin conocerse y sin coste alguno. Así, una de las peculiaridades de estos delitos es la diversidad de nacionalidades implicadas en el mismo. En la Operación Ulises de entre los 76 detenidos, 47 eran españoles y el resto ucranianos (5), rumanos (4), rusos (2), marroquíes (2), 1 holandés, 1 suizo, 1 venezolano, 1 alemán, 1 uruguayo, 1brasileño, 1 armenio, 1 jamaicano, 1 camerunés, 1 argentino y 1 moldavo. Además la pena asociada a estos delitos no es muy elevada en los países de nuestro entorno y resulta inversamente proporcional al número de potenciales víctimas.

acreditados, desconfiando, en cualquier caso, de los precios "excesivamente bajos".

Por ello también en el ámbito de la identidad son aplicables todas las normas jurídicas existentes sobre protección de datos y, como norma de base, la Directiva general sobre Protección de Datos, en el marco de la UE, lo que afecta a todas las empresas que aún no estando establecidas en este territorio, ni utilizando equipos localizados en la UE, negocien electrónicamente con destinatarios situados en alguno de los países miembros, incluso cuando los responsables del tratamiento se encuentren fuera de la Comunidad (en virtud del art. 4 de la Directiva general y de la Directiva 2000/31/CE, de 8 de junio, sobre el Comercio Electrónico,[110]).

A las transacciones comerciales y a las comunicaciones en la Red les son aplicables los principios relativos a la legitimidad del tratamiento (arts. 5 a 7 Directiva 95/46/CE y art. 4 Ley 15/1999, de Protección de Datos de Carácter Personal), así como los derechos de información clara y fácilmente accesible para el consumidor directamente en la pantalla (art. 10 Directiva 95/46/CE y art. 5 LPD, en relación con la Recomendación de 17 de mayo de 2001[111] y art. 18 RD 1720/2007), los derechos de acceso y oposición (art. 6 y 12 de la Directiva 95/46/CE y 15, 16 y 17 LPD, arts. 23-30 RD 1720/2007) y las obligaciones del responsable del tratamiento desde la óptica de la confidencialidad y la seguridad (art. 16 y 17 Directiva 95/46/CE, arts. 4 y 5 Directiva 2002/58/CE y arts. 9 y 10 LPD, arts. 79 a 87 RD 1720/2007).

Con todo, interesa poner de relieve que en el marco de las transacciones comerciales electrónicas la recogida legítima de datos personales sin el consentimiento del interesado se reconoce tanto en la Directiva general (art. 7, letra b), como en la transposición nacional de esta norma (art. 6.2 LPD) y en el Reglamento 1720/2007 de desarrollo de la LOPD, sobre la base de una relación negocial, tanto contractual como precontractual. Si bien es necesario advertir que cualquier otro dato, incluidos los datos invisibles, que no sean necesarios para realizar la transacción, necesitan el consentimiento inequívoco del interesado o del responsable del tratamiento, o bien la concurrencia de obligaciones jurídicas o un interés vital del interesado.

En este sentido, la Instrucción nº 2/1995, de 4 de mayo, de la APD, específica aún más este extremo en el caso de datos recabados como consecuencia de la contratación de un seguro de vida. La obtención de datos personales a través de cuestionarios u otros impresos debe realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. Incide en el principio de proporcionalidad de manera que cuando el contrato

[110] Art.4 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[111] Recomendación del Grupo de Trabajo del art. 29, sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, WP 43.

se celebre de forma conjunta con la concesión de un préstamo hipotecario o personal, las entidades bancarias no pueden recabar en ningún caso datos relativos a la salud del solicitante. Existen en nuestro país varias sanciones contra empresas del sector asegurador que han incumplido el trámite de solicitar el consentimiento del cliente: como la Resolución 927/2005 de la APD contra una gran aseguradora por no cancelar datos de un cliente y emitir una póliza sin consentimiento o la Resolución de 28 de octubre de 2005 contra la Compañía ARAG, Compañía Internacional de Seguros y Reaseguros.

Por otro lado, la protección de los derechos del cliente en línea se refuerza, en términos generales, con la obligación de facilitar al destinatario las condiciones generales del contrato para que éste pueda almacenarlas y reproducirlas (art. 10 Directiva 2000/31/CE) y de este modo, garantizar que no se modifican posteriormente una vez que le han sido mostradas y que ha aceptado el contrato.

Otra cuestión importante en relación a la protección de los derechos del cliente es la nueva dimensión que toma el derecho de acceso en este tipo de transferencias. En efecto, el derecho del titular de los datos personales no se agota con la información básica que sobre él se pueda obtener sino que se extiende a la información derivada; esto es, aquellos perfiles elaborados a partir de datos combinados de diferente procedencia, que deben estar a disposición del interesado, como se especifica en el art. 12 Directiva 95/46/CE.

Por su parte, la aprobación de la ley 26/2006 de mediación de los Seguros Privados, ha venido a culminar el proceso de aumento de las garantías de los asegurados al trasladar al ámbito de los mediadores los requerimientos de la Ley Orgánica de Protección de Datos. A los mediadores se les exige un deber de información mucho más amplio que el recogido en la LOPD, puesto que en artículo 42.1 f) se dispone que antes de celebrar un contrato de seguro, el mediador de seguros deberá, como mínimo, proporcionar al cliente información acerca del "tratamiento de sus datos de carácter personal, de conformidad con lo establecido en la LOPD. De modo que deberá conservar el soporte en el que conste el cumplimiento del deber de informar para lo que podrá utilizar medios informáticos o telemáticos, por ejemplo puede escanear la documentación en soporte papel, siempre que pueda garantizar que no ha habido alteración del original. Los principales retos son, por tanto, concienciar al sector que se está ante un Derecho Fundamental y el Deber de Información.

Por último, no debemos olvidar la importancia que cobra en este ámbito la confidencialidad de la transacción y de ahí que al final del Capítulo se haga alusión a la tecnología de la encriptación y a los certificados electrónicos como posibles soluciones técnicas para garantizar la integridad de los mensajes. También en este sentido se analiza en el Capítulo del trabajo dedicado a la prueba electrónica la nueva herramienta que proporciona el DNI electrónico.

2. PRINCIPIO DE SEGURIDAD

La seguridad aparece elevada a rango de principio desde su formulación en el Convenio 108 (art. 7), en su esfuerzo por delimitar un "núcleo irreductible" de la protección de datos. Hasta ese momento fue considerada como una de las tres soluciones que definían el sistema protector de los datos[112]: la solución *tecnológica*, la solución *jurídica* y la solución *deontológica*[113].

Corresponde al responsable del tratamiento[114] adoptar las medidas técnicas y organizativas adecuadas a los riesgos del tratamiento tales como pérdida accidental o la destrucción[115], la modificación, el uso y el acceso sin la correspondiente autorización. Se trata de una cláusula general incluida en términos muy similares en todos los textos multilaterales, si bien la OCDE[116] perfila los riesgos y diferencia los *naturales* (pérdida accidental o destrucción por siniestro) de los *humanos* (acceso no autorizado, utilización fraudulenta o contaminación por virus informáticos).

Por su parte la Directiva comunitaria añade el tratamiento que incluya transmisión de datos dentro de una red (art. 17.1).
A pesar de todo, ningún texto multilateral define qué debe entenderse por "medidas de seguridad" por lo que son las legislaciones nacionales las encargadas de desarrollar este término, como veremos a continuación al estudiar el caso de España.
De ahí que un sistema de seguridad constituya una herramienta inestimable para garantizar la identidad del cliente. En la configuración del sistema de seguridad que garantice el tratamiento de los datos incluidos en cada fichero y su transferencia deben tenerse muy presentes tres variables claras. En primer

---

[112] TRUJOL, A y VILLANUEVA ECHEVARRÍA, R.: *"Derecho a la intimidad e informática",* en Información Jurídica, nº 318, julio-septiembre, 1973.

[113] La solución deontológica hacia referencia al deber de secreto. Se consideraba que en los primeros momentos de evolución de la tecnología, el personal de los centros de proceso de datos era depositario de un "saber oculto" y que el uso de los datos personales por dichos trabajadores no debía ser objeto de control externo, lo que justificaba los posibles abusos en el trato de los datos personales. A medida que el uso de la informática se va generalizando, se produjo un cambio sustancial en la fisonomía del sistema protector de los datos personales. Así, las leyes de primera generación fueron incluyendo preceptos relativos a la seguridad y al deber de secreto del personal encargado de su proceso. Vid. HEREDERO HIGUERAS, M, ob, cit, p. 111 y ss.

[114] La LOPD mantiene la misma redacción que el art. 9 de la LORTAD (*Seguridad de los datos)*, incorporando ahora la figura del encargado del tratamiento y no sólo la del responsable del fichero, como garantes de la seguridad de los datos.

[115] Paradójicamente la ley española no incluye entre los supuestos la destrucción, si bien el RD 994/99 al desarrollar el art. 9.1 de la LOPD corrige este punto al regular las diversas medidas de seguridad que han de aplicarse a la información contenida en los ficheros de datos personales.

[116] Equivalente al art. 7 del Convenio 108.

lugar, se debe valorar su vulnerabilidad. El concepto de vulnerabilidad tiene, al menos, tres acepciones. Se puede, por un lado, pensar en la facilidad de acceso al fichero en general; pero también cabe utilizar este término para aludir al índice de probabilidad de acceder, a través de ese fichero, al resto de la organización a la que pertenece, y la necesidad de limitar ese acceso; incluso cabe una tercera interpretación de la vulnerabilidad en el sentido de considerar que las dificultades de almacenamiento a largo plazo de los ficheros debiliten las barreras de acceso.

En segundo lugar, las medidas de seguridad que se adopten deben ser las idóneas; esto es las que se adapten adecuadamente a las funciones concretas del fichero en proporción a los riesgos potenciales o ciertos.

Por último, se deben utilizar los sistemas y técnicas de seguridad informáticas que se deriven del estado actual de conocimiento en este campo[117].

En el caso de nuestro país, el legislador ha acudido a la vía reglamentaria para regular las condiciones de seguridad de los ficheros. La fórmula de la remisión reglamentaria, característico del sistema español, utilizada para determinar los requisitos y condiciones que deban reunir los ficheros (art. 9.3 LOPD) modifica el alcance de las funciones del responsable del tratamiento tal y como figura en la Directiva comunitaria (y en el propio art. 9.1 LOPD). En efecto, la norma de la UE responsabiliza directamente (al igual que la ley española) al encargado del tratamiento de la adopción de las medidas; sin embargo, la ley española traslada esta competencia al Gobierno mediante habilitación reglamentaria. Haciendo uso de ella el RD 994/99[118] y el RD 195/2000[119] desarrollaron el art. 9.3 LOPD y regularon las diversas medidas de seguridad (de nivel básico, medio y alto) en función de la naturaleza de la información y de la necesidad de garantizar la confidencialidad e integridad de los datos personales contenidos en ficheros automatizados. De esta manera, el nivel inferior se aplicará a todos los ficheros; el nivel medio se reserva a una amplia gama de supuestos como son: aquellos ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, a la Hacienda Pública, servicios financieros, el censo promocional[120]

[117]Art. 17.1, párrafo 2º de la Directiva comunitaria: " Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse".

[118] Real Decreto 999/99, 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. BOE 151/1999, de 25 de junio de 1999.

[119] Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el RD 994/99, de 11 de junio. BOE 49, de 26 de febrero de 2000.

[120] Art. 28 LOPD.

o a grupos profesionales (estos dos últimos en los términos del art. 3, *j)* LOPD). Por otro lado, el Real Decreto 994/99 incluía entre los supuestos a los que se les aplicaban medidas de seguridad de nivel alto a los ficheros con datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual, así aquellos datos recabados con fines policiales sin consentimiento de las personas afectadas.

Por lo que se refiere a las medidas concretas de seguridad aplicables, el RD 994/99 las diferenciaba en función de los niveles de seguridad descritos en los arts. 3 y 4 de la norma. Así, para todos los ficheros se debe elaborar un *documento de seguridad* que incluya, como mínimo: el ámbito de aplicación del documento, las medidas, las normas y los procedimientos así como las reglas y estándares necesarios para garantizar el nivel básico de seguridad, las funciones y obligaciones del personal, la estructura del fichero y el sistema de información de que se trate, el procedimiento de notificación, el tratamiento y la respuesta ante incidencias, y , por último los procedimientos de realización de copias y recuperación de datos (art. 8 RD 994/99).

Para los ficheros a los que se les aplican las medidas de seguridad de nivel medio, se exige además que el *documento de seguridad* contenga: la identificación del responsable de seguridad[121], los controles periódicos que se deban realizar[122] y las medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado (art. 15 RD 994/99). Frente a la solución del legislador español las distintas leyes de los países de nuestro entorno se limitan a imponer al responsable del tratamiento la obligación de adoptar este tipo de medidas[123]. Todos estos esfuerzos permiten garantizar la seguridad del tratamiento automatizado de datos personales en ficheros informáticos y, por tanto, resultan básicos para iniciar una segunda fase como es la del tráfico de los mismos y asegurar, en nuestro caso concreto, las transferencias transnacionales de datos personales.

Por su parte, la aprobación del Reglamento 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal ha venido a modificar la panorámica anterior sobretodo en lo que se refiere a los datos que se incluyen en cada nivel (art. 81).

---

[121] La figura del responsable de seguridad se ocupará de coordinar y controlar las medidas incluidas en el *documento de seguridad* y sus funciones son diferentes a aquellas atribuidas al responsable del fichero (art. 16 de este RD).

[122] En este sentido, el art. 17 de este RD establece la obligación de realizar una auditoría, al menos, cada dos años sobre los sistemas de información e instalaciones de tratamientos de datos. Estos informes serán posteriormente analizados por el responsable de seguridad que los elevará al responsable del fichero para que, en su caso adopte las medidas correctoras necesarias.

[123] HEREDERO HIGUERAS, ob, cit, p.113.

De este modo, algunos datos que antes tenían asociadas medidas de seguridad alta han visto modificado su nivel de modo que únicamente se exige para ellos medidas de seguridad básica. En este supuesto se encuentran:

1. *los ficheros* de datos de ideología, afiliación sindical, religión creencias, origen racial o vida sexual en dos casos:

   a) Cuando la única finalidad sea la **transferencia dineraria** a entidades de los que los asociados sean asociados o miembros y
   b) Cuando se trate de ficheros o tratamientos **no** automatizados en los que de forma **accidental o accesoria** se contengan datos que no guarden relación con su finalidad.

2. *Datos de salud referentes exclusivamente a*:

   a) **grado de discapacidad** del afectado,
   b) simple **declaración de la condición de discapacidad o invalidez** del afectado

y todo ello con motivo del **cumplimiento de deberes públicos**. Con ello el legislador concede mayor agilidad a las medidas de seguridad exigibles a cada nivel puesto, que, efectivamente los contenidos anteriores aparecían revestidos en la regulación anterior de unas salvaguardas excesivas que ralentizaban la efectividad de las mismas.

3. OBJETIVOS DE SEGURIDAD EN LAS COMUNICACIONES ELECTRÓNICAS DEL SECTOR ASEGURADOR

En las comunicaciones electrónicas el problema de la seguridad se agrava sobre todo en lo que afecta a los servicios de la sociedad de la información y se traduce en nuevos riesgos para las personas frente al tratamiento de datos de carácter personal y frente a la identidad del posible cliente. Así, pese a las indudables ventajas de las comunicaciones electrónicas, se plantean dudas relativas la eficacia y validez de la contratación electrónica, al momento de perfeccionamiento del contrato o a la ley aplicable, a lo que hay que añadir los riesgos derivados directamente de los sistemas electrónicos como: la alteración de los datos, su utilización fraudulenta, el no reconocimiento de envíos o recepciones, etc. Todo ello ha hecho necesario articular mecanismos que aseguren la confianza de usuarios y aseguradoras en la red no sólo desde el punto de vista comercial sino también jurídico.

Desde la perspectiva jurídica se identifican como elementos a asegurar los siguientes: a) que el mensaje haya sido enviado por la persona que dice que lo envía; b) que no haya sido modificado en su trayecto y, c) que el emisor no

pueda negar su envío ni el receptor que lo ha recibido. Para lograr estos objetivos es necesario acudir a soluciones técnicas que lo garanticen, por lo que, desde el punto de vista técnico se habla de: autenticación (solución técnica que asegura la identidad de la persona que ha enviado el mensaje), integridad (procedimiento técnico que permite garantizar que el mensaje no ha sido modificado), confidencialidad (protege el mensaje de usos no autorizados) y no rechazo (técnica que demuestra que se ha realizado la operación).

En el Convenio 108 (art. 7) se apuntaba ya la obligación de tomar medidas específicas para proteger los datos personales registrados en ficheros automatizados y evitar la destrucción accidental o no autorizada, la pérdida, y el acceso, modificación o difusión no consentidos.

En los últimos años una de las cuestiones que más han preocupado en relación a las comunicaciones electrónicas es la de la confianza de los usuarios en la seguridad de las comunicaciones. No cabe duda que la seguridad absoluta constituye una utopía confirmada por el día a día; sin embargo, si es posible fijar mecanismos que confieran cierta garantía de una transmisión segura. Al mismo tiempo hay que insistir en la importancia de coordinar las políticas de seguridad a nivel internacional a fin de conseguir su total aceptación.

Por su parte la Directiva general de Protección de Datos, en su art. 17, presta especial atención al “transporte de datos dentro de una red”, y obliga al responsable del tratamiento a aplicar medidas técnicas y de organización adecuadas para proteger este tipo de datos.

En España, la exigencia comunitaria se cumplió con la aprobación del Real Decreto 994/1999, de 11 de junio, Reglamento de Seguridad**,** aplicable tanto a los ficheros públicos como privados. Este Reglamento no especifica medidas especiales en función del entorno tecnológico en que se actúe, pero sí aclara que el nivel de seguridad que se garantice no puede descender por el hecho de que se acceda a los datos a través de una red de telecomunicaciones (art. 5), por lo que una interpretación extensiva permite incluir en el ámbito de aplicación de la norma al sector de Internet.

Ello es consecuencia de la libertad que otorgan los textos multilaterales en relación a las "medidas de seguridad" que no definen su contenido. De este modo, a la hora de establecer un sistema de seguridad que garantice el tratamiento de los datos incluidos en cada fichero los Estados deben tener muy presentes tres variables claras: vulnerabilidad, idoneidad y estado de la ciencia.

Así, el RD 1720/2007 diferencia en el artículo 81 tres niveles de seguridad en función de los niveles de seguridad descritos en el artículo 81 de la norma y exige la elaboración de un *documento de seguridad* para todos ellos.

Dada la importancia que la seguridad tiene para el sector asegurador tanto desde el punto de vista organizativo, como de gestión e inversión, el impacto del deber de seguridad exige un cuidado rigor en la atribución de los niveles de seguridad. En este sentido, la aplicación del Reglamento 195/2000 reveló una serie de puntos débiles que han venido a subsanarse en el nuevo Reglamento 1720/2007 en el sentido de delimitar con mayor rigor el contenido y las obligaciones relacionadas con el documento de seguridad, incluyendo medidas complementarias que clarifican el marco de actuación del responsable del fichero o del tratamiento.

En cualquier caso, las medidas de seguridad exigibles para los accesos a datos personales a través de la red de telecomunicaciones debe garantizar un nivel de seguridad equivalente a los accesos locales y en caso de que esos datos se almacenen en dispositivos portátiles o se traten fuera de los locales de la entidad aseguradora se exige una autorización previa del responsable del fichero o tratamiento (mediador del seguro) que debe garantizar el nivel de seguridad correspondiente al tipo de fichero que se trate, lo que, en todo caso debe constar en el documento de seguridad.

4. MEDIDAS DE SEGURIDAD APLICABLES A LOS FICHEROS Y TRATAMIENTOS

Corresponde al responsable del tratamiento[124] adoptar las medidas técnicas y organizativas adecuadas a los riesgos del tratamiento tales como la pérdida accidental o la destrucción[125], la modificación, el uso y el acceso a los datos sin la correspondiente autorización. En la práctica, la implantación de las medidas de seguridad en los sistemas de información ha demostrado que exige esfuerzos más desde el punto de vista organizativo que económico. Si bien, también es cierto que una parte importante en la implementación de medidas técnicas recae en el fabricante del software que debe no sólo conocer la normativa de seguridad sino actuar diligentemente en la venta de herramientas que cumplan la normativa en protección de datos, dado que la preparación del software que cumpla con ella depende del fabricante.

La seguridad es un principio general que garantiza la legitimidad del tratamiento de datos personales. Por lo que una interpretación *a contrario* supondría que no resulta legítimo ninguna de las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la

[124] La LOPD mantiene la misma redacción que el art. 9 de la LORTAD (*Seguridad de los datos)*, incorporando ahora la figura del encargado del tratamiento y no sólo la del responsable del fichero, como garantes de la seguridad de los datos.

[125] Paradójicamente la ley española no incluye entre los supuestos la destrucción, si bien el RD 994/99 al desarrollar el art. 9.1 de la LOPD corrige este punto al regular las diversas medidas de seguridad que han de aplicarse a la información contenida en los ficheros de datos personales.

recogida de datos, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como cualquier cesión de datos que resulte de comunicaciones, consultas, interconexiones o transferencias, en las que no se hayan respetado las medidas de seguridad previstas.

Por tanto, la seguridad se configura no sólo como principio sino como condición previa al tratamiento.

4.1. Categorías de medidas

Las medidas de seguridad que se han de implementar en el ámbito de las empresas aseguradoras y concretamente en los centros de tratamiento, locales, equipos, sistemas, programas y personas que intervienen en el tratamiento de datos personales se estructuran en cinco categorías:

1. Las medidas para tratar cualquier dato de carácter personal que configuran el nivel básico.

2. Medidas para tratar datos que revelen la ideología, afiliación sindical, religión y creencias o que hagan referencia al origen racial, a la salud y a la vida sexual de las personas, así como aquéllas que se recojan para fines policiales sin consentimiento de las personas afectadas. Todas ellas incorporan medidas de seguridad de nivel alto, con las peculiaridades reseñadas en el apartado dos de este Capítulo.

3. Medidas que deben adoptarse para llevar a cabo tratamientos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los relativos a la solvencia patrimonial y crédito de las personas, o al cumplimiento de sus obligaciones dinerarias[126].En estos casos las medidas de seguridad a establecer se sitúan en el nivel medio.

Dentro de esta categoría, se debe destacar que la doctrina de la AEPD ha concretado el alcance de las expresiones Hacienda Pública y servicios financieros, en el siguiente sentido:

- Datos de la Hacienda Pública. *Dicha expresión, en principio hace referencia a los ficheros cuya titularidad corresponda a la Hacienda Pública, debiendo entenderse como aplicable a aquellos ficheros cuyo responsable sea una Administración Pública que ostente potestades en materia tributaria; esto es aquellos ficheros cuyo responsable sea la Agencia Estatal de la Administración Tributaria, los que correspondan a las Comunidades Autónomas en materia de tributos que les hayan sido*

[126] En estos dos últimos casos, respecto a los tratamientos realizados en el marco del art. 29 LOPD, prestación de servicios de información sobre solvencia patrimonial y crédito y el uso de estas bases de datos.

cedidos o aquellos padrones fiscales, correspondientes a los tributos locales, de los que son responsables las Haciendas Locales.

- Servicios Financieros. En esta expresión la AEPD incluye una amplia gama de servicios como son: las actividades de intermediación financiera, intermediación monetaria, actividades relacionadas con el Banco Central, Bancos, Cajas y Cooperativas, actividades de arrendamiento financiero, las desarrolladas por Sociedades de crédito hipotecario, entidades de financiación, Sociedades mediadoras en el mercado de dinero y el Instituto de Crédito Oficial.

También quedan incluidas en esta expresión los servicios financieros relacionados con la Administración de mercados financieros, las actividades llevadas a cabo por sociedades de valores, sociedades de garantía recíproca y reafianzamiento, sociedades de tasación, casas de cambio, fondos de garantía de depósito y sus sociedades gestoras.

Por lo que se refiere al sector asegurador, y teniendo en cuenta la Clasificación Nacional de Actividades Económica, la AEPD incluye dentro de los servicios de intermediación financiera:

- los relacionados con los seguros de vida, incluidos los que se realicen por entidades de previsión social,
- los planes de pensiones,
- los seguros de daños y el reaseguro (ramo no vida),
- las actividades desarrolladas por agentes y corredores de seguros e intermediarios de seguros.

4. Las medidas de seguridad para tratar los datos personales que permitan obtener una evaluación de la personalidad del individuo se sitúan en un nivel intermedio entre el nivel básico y medio.

5. Por ultimo, y con independencia del nivel de seguridad, el Reglamento de seguridad se refiere a una serie de medidas que han de tenerse en cuenta para realizar cualquier tratamiento de datos de carácter personal (condiciones de acceso a través de redes de comunicaciones, régimen de trabajo fuera de los locales donde se encuentra el fichero y tratamiento de ficheros temporales).

4.2. Medidas concretas de seguridad

Por lo que se refiere a las medidas concretas de seguridad son aplicables los RD 994/99 y 1720/2007, que establecen los contenidos mínimos y diferencian las medidas en función de los niveles de seguridad. De esta manera, los responsables y encargados del tratamiento o fichero podrán superar lo previsto en los Reglamentos poniendo en práctica las medidas de carácter

técnico y organizativo que garanticen un nivel de seguridad adecuado en relación con los riesgos del tratamiento y la naturaleza de los datos, teniendo en cuenta el estado de la ciencia y el coste de su implementación.

A. Medidas generales y de nivel básico

Para todos los ficheros se elaborará un *documento de seguridad* que incluirá:

- El ámbito de aplicación del documento especificando los recursos que se van a proteger,
- Las medidas, normas y procedimientos así como las reglas y estándares necesarios para garantizar el nivel básico de seguridad,
- Las funciones y obligaciones del personal,
- La estructura del fichero y el sistema de información que lo trata,
- El procedimiento de notificación, gestión y respuesta ante incidencias,
- Los procedimientos de realización de copias y recuperación de datos.
- Las medidas a adoptar para el transporte de soportes y documentos, así como para su destrucción o, en su caso, reutilización de los mismos (art. 88.3 RD 1720/2007 en relación con el art. 92 de gestión de soportes).
- Establecerá la periodicidad, nunca superior al año, con la que deben cambiarse las contraseñas, que, además, se almacenarán de forma ininteligible (art. 93.4 RD 1720/2007).

En relación a la realización de copias de respaldo y recuperación de datos la doctrina de la AEPD las sitúa en la base para hacer efectivo el derecho de acceso a la información como consecuencia de un hecho que suponga la interrupción no voluntaria a esos accesos (por causas naturales o por deficiencias del sistema).

La copia de respaldo define el procedimiento que permite una eventual recuperación o reconstrucción de la información al contar con una copia fiel del conjunto de datos preexistentes al momento de producirse el fallo (art.94 RD 1720/2007).

Otro requisito incorporado por el nuevo Reglamento es la periodicidad en la realización de las copias de respaldo. Así, cada semana como mínimo se realizarán copias de respaldo, salvo que no se hayan actualizado los datos. Además el responsable del fichero tiene la obligación de verificar cada seis meses el correcto funcionamiento de los procedimientos de realización de copias de respaldo y recuperación de datos.

Por su parte, la eficacia del procedimiento de recuperación estriba en la capacidad de reubicar los datos y volver a disponer de la estructura en la que se localizaba la información.

Por tanto, ambos procedimientos están íntimamente relacionados y se complementan siendo claves para restituir al sistema al momento inmediatamente anterior a la producción del fallo.

La importancia de estos procesos está recogida en el Reglamento 994/1999 con carácter temporal y material. De este modo, frente a la redacción general del Reglamento de 1999 en el que se hace alusión a las copias de respaldo sin especificar cada cuanto deben realizarse, la redacción del año 2007 exige elaborar copias al menos semanalmente, salvo que en dicho período no se produzca ninguna actualización.

Desde el punto de vista material se hace responsable al encargado del tratamiento de la adecuada implementación de los mismos, hasta el punto de obligar a la verificación de su correcta definición y funcionamiento concretando los procedimientos con el suficiente grado de detalle, lo que, en muchos casos, supone la realización de pruebas previas para comprobar su operatividad.

Por tanto el documento debe mantenerse actualizado continuamente y revisarse en el momento que se produzcan cambios sustanciales en el sistema de información o en su organización.

Por lo que se refiere a las funciones y obligaciones de las personas que tienen acceso a los datos de carácter personal y a los sistemas de información:

- El responsable del fichero debe adoptar las medidas necesarias para que el personal tenga conocimiento de las normas de seguridad que tengan que ver con el desarrollo de sus funciones y las consecuencias en caso de incumplimiento.
- Las funciones y obligaciones de los usuarios o los perfiles de usuarios [127]
- Las personas que tengan un acceso autorizado al sistema de información, que se enumerarán con carácter independiente, deben reflejarse en una relación actualizada estableciéndose procedimientos de identificación y autenticación para dicho acceso.
- Cuando el mecanismo de autenticación se base en contraseñas, el procedimiento de asignación, distribución y almacenamiento debe garantizar el principio de confidencialidad e integridad. Las contraseñas se modificarán periódicamente según lo previsto en el documento de seguridad y se almacenarán de forma ininteligible.
- El acceso a la información propiamente dicha también debe controlarse por el responsable del fichero o persona en la que se delegue y los usuarios sólo deben tener acceso a aquellos datos y recursos necesarios

[127] La redacción de 1999 se refería a personal, habiéndose producido una ampliación del ámbito subjetivo en el RD 1720/2007, en el que no sólo se prevé la enumeración de las personas que puedan tener acceso a los datos sino la inclusión de "perfiles de usuarios", lo que abre el campo de los posibles usuarios que pueden acceder al fichero.

para el ejercicio de sus funciones fijándose mecanismos que eviten que el usuario pueda acceder a datos o recursos diferentes a los autorizados.
- Únicamente el personal autorizado en el documento de seguridad puede conceder, alterar o anular el acceso autorizado a datos y recursos.

El Reglamento 1720/2007 viene a dar solución a otro gran interrogante que se planteaba a menudo cuando se producían accesos a ficheros por personas no vinculadas laboralmente al responsable del fichero. A partir del 19 de abril de 2008 estas personas quedarán sometidas a las mismas condiciones y obligaciones de seguridad del personal propio.

En caso de que se produjera alguna incidencia debe existir un procedimiento de notificación y gestión, así como un registro en el que se haga constar: el tipo de incidencia, el momento en que se ha producido (o en el que se ha detectado), la persona que realiza la notificación, a quien se comunica y los efectos derivados de la incidencia y las medidas correctoras aplicadas (art. 90).

Además para poder tratar datos de carácter personal es necesario adoptar las siguientes medidas técnicas para todos los niveles de seguridad:

a) Cuando el acceso a datos de este tipo se realice a través de redes de comunicaciones se deberá garantizar un nivel de seguridad equivalente al correspondiente a los accesos que se produzcan en modo local.
b) Cuando el tratamiento de los datos se realice fuera de los locales donde está ubicado el fichero, debe autorizarse expresamente por el responsable del fichero **o encontrarse debidamente autorizados en el documento de seguridad**, y garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
c) Cuando vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal se adoptarán previamente **medidas de destrucción o borrado** dirigidas a evitar el acceso o recuperación de la información (art. 92.4 RD 1720/2007).
d) Para aquellos soportes que contengan datos de carácter personal que la organización considere especialmente sensibles, la identificación de los mismos podrá realizarse mediante un **sistema de etiquetado** que permita su localización a las personas autorizadas y lo dificulta para el resto (art.92.5 RD 1720/2007).
e) Los ficheros temporales cumplirán el nivel de seguridad que corresponda de acuerdo al tipo de datos que contengan y deberán ser borrados cuando dejen de ser necesarios para el fin para el que se crearon.

B. Medidas de nivel medio

Mayor interés presenta para el sector asegurador las medidas previstas por nuestro legislador para el tratamiento de datos personales relativos a la solvencia patrimonial y al crédito de personal, así como al cumplimiento o

incumplimiento de obligaciones dinerarias. Todos llevan asociados medidas de seguridad de nivel medio, por lo que, con carácter previo al tratamiento se deben cumplir los siguientes requisitos:

1. El *documento de seguridad* debe contener: además de lo previsto para el nivel básico, la identificación del responsable de seguridad[128], los controles periódicos que se deban realizar[129] y las medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado (art. 15 RD 994/99). Frente a la solución del legislador español las distintas leyes de los países de nuestro entorno se limitan a imponer al responsable del tratamiento la obligación de adoptar este tipo de medidas con carácter general sin pormenorizarlas. Todos estos esfuerzos permitirán garantizar la seguridad del tratamiento automatizado de datos personales en ficheros informáticos.

2. Debe establecerse un sistema de control de acceso físico a las instalaciones donde se localicen los sistemas de información que garantice que sólo el personal autorizado en el documento de seguridad tiene acceso a esos lugares.

3. Para acceder al sistema de información la solución que se implante debe poder garantizar de forma inequívoca y personalizada la identidad del usuario que pretenda acceder y comprobar que está autorizado. Además, se debe limitar los intentos de acceso reiterado no autorizado.

4. En el registro de incidencias, debe reflejarse el número de procedimientos de recuperación realizados indicando, además:

   - la persona que ejecutó el proceso,
   - los datos restaurados,
   - los datos que, en su caso, han sido necesarios grabar manualmente en el proceso de recuperación[130].

5. Nombrar a una o varias personas como responsables de la coordinación y control de las medidas incluidas en el documento de seguridad y que analicen los informes de auditoría. Este responsable no precisa reunir

[128] La figura del responsable de seguridad se ocupará de coordinar y controlar las medidas incluidas en el *documento de seguridad* y sus funciones son diferentes a aquellas atribuidas al responsable del fichero (art. 16 del Reglamento de Seguridad).

[129] En este sentido, el art. 17 del Reglamento de Seguridad establece la obligación de realizar una auditoría, al menos, cada dos años sobre los sistemas de información e instalaciones de tratamientos de datos. Estos informes serán posteriormente analizados por el responsable de seguridad que los elevará al responsable del fichero para que, en su caso adopte las medidas correctoras necesarias.

[130] Es necesaria la autorización por escrito del responsable del fichero para la ejecución de los procesos de recuperación de datos, si bien el Reglamento 1720/2007 amplía esta competencia a las personas que ejerzan esta función por delegación, lo que viene a legitimar una práctica habitual hasta el momento.

requisitos especiales más que los derivados de los suficientes conocimientos técnicos en la materia, por lo que, puede desarrollar esta función el mismo responsable del fichero o la persona designada por éste.

6. El responsable de seguridad debe adoptar las medidas necesarias para impedir que un soporte que vaya a ser desechado o reutilizado pueda recuperarse posteriormente, con carácter previo a su baja en el inventario. A este respecto, La Sentencia de la Audiencia Nacional de 7 de febrero de 2003 es muy clara sobre el alcance de esta obligación señalando que es insuficiente con acreditar que se adoptan una serie de medidas, pues es también responsable de que las mismas se cumplan y ejecuten con rigor. Hasta el punto que si un tercero posee documentación interna de una entidad "ello es debido necesariamente a un funcionamiento anómalo de sus medidas de seguridad".

7. Debe crearse un registro de entrada y salida de soportes informáticos en el que quede reflejado:

   a. Registro de entrada: tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, persona responsable de la recepción (debidamente autorizada).
   b. Registro de salida: tipo de soporte, fecha y hora, destinatario, número de soportes, tipo de información que contienen, forma de envío, persona responsable de la entrega (debidamente autorizada).

   En caso de que los soportes salgan fuera del local donde se encuentren por causas asociadas al mantenimiento se deben adoptar las medidas necesarias para evitar que se pueda producir una recuperación indebida de la información almacenada.

8. Realizar una auditoria, interna o externa, sobre los sistemas de información que permita conocer el grado de cumplimiento del Reglamento de Seguridad, al menos cada dos años.

C. Medidas de seguridad intermedia

Para aquellos tratamientos de datos personales que permitan obtener una evaluación de la personalidad del individuo deben adoptarse, junto a las medidas de seguridad básica, algunas de las medidas previstas para el nivel medio como son:

a) Auditoría bienal de los sistemas de información
b) Control de acceso físico
c) Identificar y autenticar del usuario que intente acceder al sistema de información y comprobar su autorización
d) Gestión los soportes
e) Medidas para el desechado o reutilización de soportes

D. Medidas de nivel alto

Las medidas más restrictivas se reservan para los ficheros que llevan aparejados medidas de seguridad alta como son los datos relativos a la salud que por su actividad maneja el sector asegurador. En estos casos, con carácter previo al tratamiento, deben implementarse, además de las establecidas con carácter general para cualquier tipo de tratamiento y todas las enumeradas para el nivel básico y medio, las siguientes:

a) La copia de los procedimientos de recuperación de datos y de la copia de respaldo debe conservarse en un lugar diferente a aquél en que se encuentran los equipos informáticos que tratan la información, cumpliendo todas las medidas de seguridad que se exigen para almacenar este tipo de información.

b) Debe crearse un registro de cada acceso a la información en el que se recoja, como mínimo: la identificación del usuario, fecha y hora en que se realizó, fichero al que se accede, tipo de acceso y si se ha autorizado o no. Estos datos deben conservarse dos años como mínimo y el responsable de seguridad será el encargado de revisar periódicamente los accesos registrados y elaborar un informe donde detalle las revisiones realizadas y los problemas detectados al menos cada mes.

c) Cuando se transmitan datos a través de redes de telecomunicaciones deben cifrarse los datos o utilizar cualquier mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

d) Cuando la transmisión se realice mediante la distribución de soportes, los datos contenidos en ellos deberá cifrarse o protegerse mediante cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante el transporte.

Al respecto de las dos últimas medidas la duda que se plantea es si el cifrado de la información se aplica sólo para el caso de que la información salga de las dependencias de la empresa o se aplica también a aquélla que se transmite en el interior de la misma entidad.

En este supuesto habría que concretar aquellas entidades que cuentan con varias sedes físicas de aquellas otras que sólo tienen un establecimiento. En el segundo caso, la propia eficacia y efectividad del trabajo diario aconsejaría que no se realizara esa encriptación siempre y cuando se garantizara en todo momento el deber de custodia y la confidencialidad (intranet).

Cosa distinta sería que para la transmisión del fichero se utilizasen redes públicas de telecomunicaciones en cuyo caso si debe cifrarse el fichero para garantizar la salvaguarda del contenido, como puede ser la solución “WINZIP v9 sr2” o superior con cifrado con el algoritmo AES 256.

La misma solución cabría aplicar a los supuestos de entidades con más de un establecimiento. En este caso suelen diferenciarse dos situaciones:

- En la comunicación entre oficinas se utilizan redes privadas cifradas.

- Para el resto de comunicaciones se utiliza un anillo. Esta solución consiste en una línea punto a punto contratada con proveedores externos que garantizan la confidencialidad e integridad de los datos que se transmiten.

Otra duda que plantea la transmisión es qué ha de entenderse por redes de telecomunicaciones. En este sentido, la Directiva 97/66/CE, de 15 de diciembre, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones y la propia Ley General de Telecomunicaciones las define como: "*los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales de señales entre puntos de terminación definidos mediante cable, o medios ópticos o de otra índole*".

Esta definición viene a reforzar la solución apuntada más arriba, de manera que cuando la transmisión se realice entre establecimientos de la misma empresa utilizando de una red de telecomunicaciones no perteneciente a la misma, la información habrá de cifrarse.

El Reglamento 1720/2007 especifica el cifrado de las comunicaciones cuando se utiliza la red pública de telecomunicaciones al transmitir datos de carácter personal que lleven asociados medidas de seguridad de nivel alto. De este modo, la transmisión que se efectúe a través de "redes públicas o redes inalámbricas de comunicaciones electrónicas" se realizará cifrando dichos datos o utilizando cualquier mecanismo que garantice que la información no sea inteligible ni pueda manipularse por terceros (art. 104).

Por lo tanto, *a sensu contrario*, cabe interpretarse que no se incurre en ilegalidad alguna cuando la transmisión se realiza utilizando redes privadas; sin embargo, la norma se rebela más estricta en el caso de las redes inalámbricas de comunicaciones para las que exige, al margen de su carácter público o privado, el cifrado de los datos.

Junto con todas estas exigencias, la práctica aconseja que en lo referente a los datos de salud se enumeren con claridad qué ficheros deben incluir medidas de nivel alto, como sería el caso de aquéllos que contienen datos de salud, y esta es la opción acogida por el Reglamento 1720/2007de desarrollo de la LOPD.

Por el contrario, bastaría utilizar el nivel básico cuando los datos tengan como única finalidad realizar una transferencia dineraria, incluso si existen retenciones a sindicatos, o bien se trate de ficheros o tratamientos no

automatizados en los que de una manera accesoria puedan incluirse este tipo de datos sin que tengan relación con su finalidad.

Asimismo cuando los ficheros incluyan datos relativos a la salud, relacionados exclusivamente con el grado de discapacidad o invalidez del titular, y con motivo del cumplimiento de deberes públicos es suficiente incorporar medidas de seguridad de nivel básico.

La duda en relación a la inclusión o no en las medidas de este nivel de las bajas por enfermedad queda también despejada en el Reglamento dado que las normas laborales incluyen la baja por enfermedad entre la declaración de la condición de invalidez.

En aquellos supuestos en que en los sistemas de información haya ficheros o tratamientos a los que se dé una finalidad o uso concreto, o cuya naturaleza requiera medidas de seguridad específicas no incluidas en el sistema principal de medidas, cabe la segregación y la configuración de medidas de seguridad. Medidas acordes con el tipo de datos y el destino que se les vaya a dar, siempre y cuando puedan delimitarse los datos afectados y los usuarios con acceso a los mismos; siempre y cuando todos estos extremos se hagan constar en el documento de seguridad.

5. TÉCNICAS DE GARANTÍA DE LA SEGURIDAD EN LA RED

Junto a las conexiones seguras del tipo del protocolo SSL, SET[131] o a las redes seguras VPN, la articulación de las técnicas de seguridad llevó en una primera fase a la utilización de las técnicas criptográficas y de firma electrónica, si bien han comenzado a implantarse en el mercado otras tecnologías que refuerzan las opciones del usuario a la hora de garantizar sus datos personales en la red.
De este modo, se exponen en este apartado las soluciones técnicas y jurídicas que existen hasta el momento. En concreto, se enuncia la firma digital desde un punto de vista conceptual con el objeto de dejar constancia de su utilización como herramienta para garantizar la identidad de las partes, si bien su estudio detallado se ha trasladado al Capítulo VI, dedicado a los medios de prueba electrónica.

La técnica de encriptación tiene su origen en la Segunda Guerra Mundial con fines exclusivamente de defensa militar. Actualmente se distingue entre su

[131] Secure Electronic Transaction, desarrollado por VISA y MasterCard desde 1995. Este protocolo ofrece la autenticación de todas las partes implicadas en la conexión, confidencialidad e integridad, por lo que garantizan la seguridad de la transacción; sin embargo, la complejidad de sus requisitos tecnológicos ha hecho que se encuentre implantada en un número inferior de sitios inferior al previsto en un primer momento. Para más información sobre este protocolo y el protocolo SSL vid. DAVARA & DAVARA, ob, cit, p. 469.

aplicación para la firma digital y para asegurar la confidencialidad de la información transmitida.

Encriptar un documento o una firma significa aplicar un algoritmo matemático que usando cierta variable, denominada clave de encriptación o clave criptográfica, transforme los datos de manera que sean ininteligibles para aquél que los reciba, siempre y cuando no cuente con la clave necesaria para reconstruir esos datos cifrados. Actualmente existen dos sistemas de encriptación de datos: el de clave simétrica (DES)[132] y el de clave asimétrica (RSA)[133].

A nivel europeo, en 1992 se creó un Comité sobre temas relacionados con la seguridad de la información (SOG-IS), cuyo objetivo era asesorar a la Comisión en este terreno. Continuando con esta línea la Comisión está impulsando varios proyectos dirigidos a la creación de licencias de empresas que aseguren el uso de la criptografía a nivel europeo, lo que se conoce como TTP (Trusted Third Parties).

De un alcance más amplio es el Acuerdo Wassenar sobre control a la exportación de armas y mercancías de uso dual de 19 de diciembre de 1995, firmado por 28 países, en su mayoría miembros de la OTAN. También la OCDE se ha ocupado de la criptografía destacando como objeto de estudio: la confianza en los métodos criptográficos, la elección entre distintos métodos criptográficos, la elección entre los métodos a disposición del usuario, las tendencias del mercado en el desarrollo de sistemas criptográficos, los estándares criptográficos, la responsabilidad que debe recaer sobre la empresas de criptografía, la protección de la vida privada y de los datos personales, la interceptación lícita de la comunicación y la necesidad de cooperación a nivel internacional.

---

[132] En este caso, emisor y receptor usan la misma clave para cifrar y descifrar los datos. Esta clave debe ser secreta para impedir el acceso no autorizado. De ahí que la seguridad en el uso de este sistema se encuentre en la protección que las partes hagan de la clave puesto que si se difunde el mensaje cifrado puede ser conocido por cualquiera en detrimento de su confidencialidad y pérdida de eficacia de la encriptación con clave simétrica. Martínez Nadal, Apolonia: Comercio Electrónico, Firma Digital y Autoridades de Certificación. Editorial Civitas. Madrid, 1998, pág.44.

[133] El mecanismo de cifrado asimétrico utiliza dos claves asociadas: una pública y otra privada. Cada parte tiene una clave privada que sólo ella conoce y que debe mantener en secreto y una clave pública que puede ser conocida por todos. De esta manera si el emisor quiere mandar un mensaje confidencial al receptor codifica el mensaje con la clave pública de receptor y éste procederá a descodificarlo utilizando su propia clave privada, recuperando así el mensaje original, puesto que el receptor es el único que posee su clave privada, queda garantizada de este modo la confidencialidad de lo transferido. Martínez Nadal, Apolonia: Comercio Electrónico, Firma Digital y Autoridades de Certificación. 2ª Edición. Editorial Civitas. Colección: “Estudios de Derecho Mercantil”. Madrid, 2000.

En la Unión Europea, el Reglamento del Consejo sobre mercancías de uso dual, de 19 de diciembre de 1994, establece un régimen común de control de la exportación de los productos de uso dual. Algunos productos criptográficos no pueden exportarse fuera de la Unión sin autorización previa. Con carácter transitorio los países de la UE pueden limitar la circulación de estos productos a otros países de la Unión.

En los Estados miembros la política sobre regulación de la criptografía varia de unos a otros. En Francia, por ejemplo, existe una regulación muy restrictiva dado que equipara la criptografía al material bélico, y requiere autorización expresa del Primer Ministro para su exportación, salvo en el caso que se trate de criptografía que garantice sólo la autenticación. Asimismo prohibe el uso de este material si no se ha registrado el algoritmo.

El Reino Unido cuenta con una legislación específica que prohibe el uso comercial de criptografía si no se tiene la autorización precisa (sistema TTP)[134]. Asimismo se prohíbe la comercialización de criptografía que se ofrece a los usuarios en este país a través de Internet.

Alemania o los países nórdicos no tienen restricciones para el uso de la criptografía, si bien en Alemania una ley obliga a las compañías de telecomunicaciones a fijar mecanismos que garanticen la interceptación legal de las comunicaciones.

En España, la Ley General de Telecomunicaciones[135], menciona las técnicas de cifrado remitiendo su regulación al desarrollo reglamentario posterior. Más tarde, la Ley de Firma electrónica, aprobada por Real Decreto-Ley 14/1999, de 17 de septiembre, regula el uso de la firma electrónica y la prestación de servicios de certificación[136].

Sin duda es en Estados Unidos donde se encuentra el mayor número de usuarios de criptografía y es allí donde está más desarrollado el debate.

---

[134] Informe:" Licensing of Trusted Third Parties for the Provision of Encryption Services", http://www.dti.gov.uk/pubs.

[135] Ley 11/1998, de 24 de abril, General de Telecomunicaciones (BOE núm. 99, de 25 de abril; rect. BOE núm. 162, de 8 de julio) y Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones (BOE núm. 213, de 5 de septiembre).

[136] En este mismo sentido: Orden de 21 de febrero de 2000, por el que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica; Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el art. 81 de la Ley 66/1997, de 30 de diciembre, en materia de prestación de servicios de seguridad en las comunicaciones de las administraciones públicas a través de técnicas y medios electrónicos, informáticos y telemáticos, con las administraciones públicas; Borrador de Anteproyecto de Ley de Firma electrónica, de 26 de julio de 2002.

Llama la atención la prohibición casi total de exportación de material criptográfico fuerte, asimilándose para su exportación con el comercio de armas, lo que ha provocado que otros países con legislaciones más permisivas, como Alemania, Suiza o Bélgica, obtengan escasos beneficios en este creciente mercado. De entre los proyectos concretos desarrollados en Estados Unidos vamos a detenernos en el Proyecto Clipper, en el Sistema TTP y en el Programa PGP.

5.1. La firma digital

Junto a las iniciativas técnicas existen otros sistemas que proporcionan una garantía adicional para el usuario en relación a la protección de sus datos personales y a la no alteración como es el caso de la *firma digital*. De este modo el usuario puede guardar la firma electrónica de las condiciones en que ha facilitado sus datos de manera que si son destinados a finalidades distintas pueda hacer valer sus derechos. Esta solución permite garantizar no sólo la integridad de los datos personales facilitados sino la transferencia en sí de los mismos. En una primera aproximación podríamos definir la firma electrónica como un conjunto de datos electrónicos utilizados como medio para vincular al autor del documento o autenticar su contenido; sin embargo, resulta insuficiente puesto que incluiríamos en el mismo ámbito técnicas tan poco seguras como la firma manual digitalizada.

La solución de la firma electrónica se recoge en el caso europeo, en la Directiva 1999/93/CE, de 13 de diciembre, dirigida muy especialmente a los proveedores de servicios de certificación y a los organismos públicos competentes, por la que se establece un marco comunitario para la firma electrónica.

En España, la aprobación del Real Decreto-Ley 14/1999, de 17 de septiembre, permite reconocer efectos jurídicos a la firma electrónica avanzada (o firma digital). De este modo, el art. 3 establece que: *" La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales, Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado con arreglo a lo establecido en el artículo 21".* Además, continúa el artículo citado que: *"A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica".*

Esta definición introduce el término avanzada que implica tanto la identificación del signatario como la creación de medios que éste conserve bajo su control, lo que le permite detectar cualquier modificación posterior que puedan realizar terceros, con lo que se está reforzando la protección de los datos del interesado. La definición de firma electrónica avanzada coincide con una clase particular de firma electrónica: la firma digital, que se crea utilizando una tecnología específica: la criptografía asimétrica o de clave pública. En la actualidad las firmas digitales son las únicas firmas electrónicas seguras. El hecho de que la ley española no se refiera directamente a ella se debe al interés por abarcar el mayor número de firmas electrónicas posibles, dejando abierta la puerta a nuevos desarrollos tecnológicos aún por crear.

5.2. Los certificados digitales

Asimismo y con el fin de evitar el tan temido suplante de personalidad en un medio en el que las partes no tienen por que estar presentes en el mismo lugar al mismo tiempo e incluso puede que no lleguen nunca a conocerse físicamente, resulta muy aconsejable la utilización de *certificados digitales* que autentiquen a las partes que participan en la transferencia, incidiéndose en la conveniencia de almacenar esos certificados en tarjetas inteligentes, como el DNI electrónico que ya utilizan más de 500.000 personas en nuestro país, obteniéndose, de este modo, un mayor grado de seguridad.

Otro aspecto importante en relación a este tipo de certificados es el derivado del principio de sujeción de los servicios relacionados con la firma digital a la Directiva 95/46, puesto que con ello se evita que los certificados puedan considerarse datos de acceso público, lo que, de otro modo, limitaría en gran medida la aplicación de la legislación de protección de datos personales a la firma digital.

Por otro lado, la aplicación de la legislación sobre protección de datos personales a los certificados digitales resulta de especial interés por cuanto en ellos pueden figurar muchos datos al margen de los esenciales para identificar al sujeto -nombre y apellidos-, como: poderes de representación, incapacidad parcial del titular o datos del proveedor de servicios de certificación, entre otros.

Qué duda cabe que todo este elenco de posibilidades debe completarse con medidas de seguridad técnica que se deben adoptar para garantizar los niveles adecuados por parte de los responsables de ficheros o de tratamientos. En el caso español, el Reglamento de Seguridad (Real Decreto 1720/2007, de 21 de diciembre) establece que se ha de prestar especial atención al art. 4.4 respecto al nivel básico incrementado cuando: *"...los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo"* en cuyo caso se *"deberán garantizar medidas de*

nivel medio[137]*",* dado que si se llevan a cabo procesos de selección de perfiles, de *datawarehouse* o de *datamining* existe un alto nivel de probabilidades de que esa actividad entre dentro del ámbito de aplicación del artículo citado.

Por lo que se refiere al sector asegurador la Ley de Mediación del Seguro Privado resuelve la cuestión de la responsabilidad del tratamiento distinguiendo la condición de responsable y de encargado en cada una de las figuras de mediación de seguros y reaseguros. Así, se consideran encargados del tratamiento a: los agentes exclusivos y vinculados, operadores de bancaseguros exclusivos y vinculados y los auxiliares externos. Por el contrario, sólo los corredores de seguros y reaseguros son considerados como responsables del tratamiento. De todas maneras, habrá que estar al caso concreto, puesto que la APD sancionó a una correduría de seguros por ceder datos de carácter personal de un cliente sin su consentimiento a una aseguradora. Los hechos fueron los siguientes: una persona suscribió una póliza de Hogar, anual renovable, a través de una correduría. La aseguradora resolvió el contrato con la correduría, comunicándoselo a la otra entidad. Esta celebra la póliza directamente con la entidad. Paralelamente, la correduría envió una carta al cliente ofreciéndole una cobertura lo más similar posible en garantías y precio, salvo que indicase lo contrario. Al no contestar el cliente, la correduría contrató una nueva póliza con otra entidad a la que facilitó los datos para la domiciliación de los recibos. Ante estos hechos la APD consideró que había existido una extralimitación de las funciones de la correduría puesto que la falta de respuesta, nunca puede sustituir al consentimiento del interesado.

En relación al consentimiento, la Directiva precisa que los datos que se obtengan para el tratamiento de datos personales con el fin de proporcionar un servicio concreto de valor añadido estará en función de los datos que deban tratarse, el tipo se servicio, y que (tanto desde un punto de vista técnico, de procedimiento y de contrato) pueda distinguirse a la persona que utiliza el servicio de comunicaciones electrónicas de la persona física o jurídica que ha suscrito el contrato.

La Directiva trata también otros temas relacionados con la intimidad como es el peligro de las facturas desglosadas. Con el fin de proteger la intimidad del usuario de los servicios de comunicaciones electrónicas contempla la utilización de alternativas que permitan el acceso anónimo o estrictamente privado a los

[137] El nuevo Reglamento de Seguridad reubica y amplía el artículo 4 y lo sitúa en el Capítulo VIII, dedicado a las medidas de seguridad en el tratamiento de datos de carácter personal. El nuevo artículo 79 desglosa los ficheros a los que se han de aplicar los diferentes niveles de seguridad y se refiere a aquellos que permitan hacer perfiles de la personalidad del individuo atribuyéndoles asimismo, niveles medios de protección y simplificando la redacción anterior.

De este modo, se da una mayor coherencia al texto reuniendo en el mismo capítulo los niveles de seguridad a aplicar a cada tipo de ficheros y terminando con la dispersión que el Reglamento del 99 incluía al recoger en diferentes partes de la norma las particularidades que hacían variar los niveles de seguridad a aplicar a los ficheros y provocaba una cierta inseguridad jurídica.

servicios de comunicaciones electrónicas disponibles al público (ej. tarjetas de llamada, tarjetas de crédito o facturas que omitan algunas de las cifras del número de llamada).

La Directiva insiste en la necesidad de proteger la intimidad y los datos personales del usuario de estos servicios con independencia de la tecnología utilizada, puesto que en caso contrario, se podría obtener el efecto perverso de no proteger la privacidad.

Por esta razón, la UE propone por primera vez y haciéndose eco de las voces que, principalmente en Estados Unidos, abogan por un mayor control sobre los fabricantes de equipos, por la imposición de medidas exigibles para aquellos equipos utilizados en los servicios de comunicaciones electrónicas de modo que fabriquen sus productos incorporando salvaguardias para garantizar la protección de datos personales y la intimidad del usuario y del abonado[138].

5.3. La autenticación

Otras herramientas que se utilizan para proteger los datos personales en la Red y garantizar la identidad del usuario son los servicios de autenticación en línea, el software que garantiza el anonimato, los filtros de correo electrónico y los informediarios.

Los *servidores proxy* constituyen una de las soluciones de *autenticación on-line.* Son servidores intermediarios entre el usuario de Internet y la Red y mejoran considerablemente el funcionamiento de Internet por lo que su uso por los proveedores de acceso es cada vez mayor. Esta solución permite al usuario delegar en un tercero la autenticación en línea. Junto a este sistema existen otros tres: transferir esta función al browser (navegador) en el pc, utilizar protocolos especiales o suscribir un contrato para formar parte de un "círculo de confianza".

La solución que desarrollan los *servidores proxy* resulta muy interesante para organizaciones grandes puesto que no es necesario que cada miembro tenga su propia dirección IP, dado que no se accede directamente a Internet y se puede utilizar desde diferentes ordenadores. Otra de las ventajas es que el servidor proxy no transmite, en principio la dirección IP del usuario[139] al sitio web que se

[138] Directiva 1999/5/CE, del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad. Esta Directiva garantiza la introducción de características técnicas en los equipos de comunicaciones electrónicas, incluido el soporte lógico, con el fin de armonizar la protección de datos.

[139] Algunos servidores proxy incluyen en la cabecera HTTP la dirección TCP-IP para la que trabajan con lo que este tipo de servidores no pueden incluirse entre las técnicas para asegurar la privacidad o el anonimato en Red, pero si como herramienta para agilizar el tráfico.

descarga y puede filtrar "los charloteos del navegador" y suprimir, cambiar o almacenar *cookies.*

Desde el punto de vista del usuario individual, éste debe registrar su password en el servidor proxy por cada sitio que visite depositando su confianza en que no se revelará su identidad por el servidor proxy. Se trata de un servicio gratuito que se financia por otros medios como la publicidad[140].

La utilización de la herramienta browser (motor de búsqueda) permite que el usuario prescinda de teclear su password cada vez que quiera conectarse y elimina el riesgo de olvidos. Sin embargo, cuando hacemos uso de estos robots, a través de los que seleccionamos la información de Internet (Google o Altavista, entre otros) el control recae exclusivamente en el usuario, desde el punto de vista de la protección de datos, y es éste el que debe comprobar que su "pin" está a salvo de ataques.

Otro factor que conviene no olvidar es el hecho de que las empresas de venta directa financian muchos de los motores de búsqueda lo que añade nuevas dificultades a la protección de los datos personales[141]

Otras empresas ofrecen un servicio de autenticación en línea utilizando un protocolo de autenticación específico como la *.NET Passport de Microsoft* o el modelo circular de *Liberty Alliance*. Su sistema se ancla en tres ejes: el usuario, el proveedor del servicio y el proveedor de la autenticación.

En el caso de Microsoft utiliza un único servidor de autenticación que incorpora dos grupos de información: la relativa a la identidad del sujeto y la comprobación de la misma y, por otro lado, otras informaciones de perfiles[142]. En cambio el modelo que propone Liberty Alliance tiene un carácter circular. El usuario puede unir su cuenta a dos proveedores de servicios. Una vez que se ha dado de alta en ellos (entra en el círculo) uno de los proveedores de servicios aceptará la actuación del segundo proveedor de servicios como prestador del servicio de autenticación[143].

---

[140] *Working Document on on-line authentication services, adopted on 29 january 2003,* en http://europa.eu.int/comm/internal_market/en/dataprot/index.htm.

[141] SUÑÉ LLINÁS, E, ob. cit., p.7.

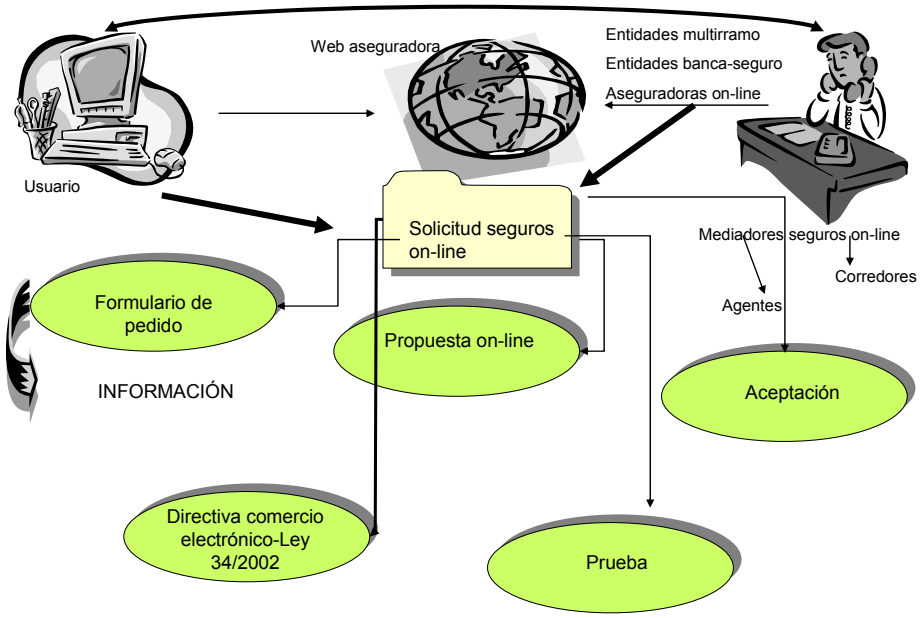
[142] La versión de .NET Passport separa claramente la creación de la cuenta .NET Passport de los datos que se almacenan en la Información sobre perfiles.

[143]En este sentido, la UE ha estudiado estos protocolos especiales y ha encontrado importantes lagunas en relación a la protección de datos en las transferencias electrónicas a terceros países en los sistemas de autenticación en línea a la luz de la Recomendación 2/2001, sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea.Aprobada el 17 de mayo de 2001, en:
http://www.europa.eu.int/comm/internal_market/en/media/dataprote/wpdocs43.htm.

Capítulo V
LA CONTRATACIÓN DE SEGUROS ON-LINE

SUMARIO: 1. CUADRO. 2. OBLIGACIONES DE LAS ASEGURADORAS COMO PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMAICIÓN. 2.1-.Obligaciones estáticas. 2.2.- Obligaciones dinámicas. 3. SOLICITUD DEL SEGURO *ON-LINE*: RECOGIDA DE DATOS. 4. PROPUESTA *ON-LINE* DEL SEGURO. 5. PERFECCIÓN DEL CONTRATO DE SEGURO *ON-LINE*. 5.1.- La aceptación.- 5.2.- La prueba. 5.3.- Momento de perfección. 6. EL VALOR DE LA PÓLIZA. 7. CUADRO COMPARATIVO DE LA DIRECTIVA SOBRE COMERCIO ELECTRÓNICO Y LA LEY 34/2002, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL COMERCIO ELECTRÓNICO.

1. CUADRO



El presente Capítulo profundiza en los aspectos jurídicos de la contratación de seguros on-line. Venimos viendo a lo largo de este trabajo cómo las entidades aseguradoras continúan concluyendo sus contratos utilizando los cauces tradicionales, si bien la tendencia se orienta hacia una mayor utilización de las nuevas tecnologías. El porcentaje de aseguradoras que opera completamente on-line no supera el 34 %, si bien la inmensa mayoría utiliza la web como canal de comunicación de la imagen corporativa. En el ámbito de la contratación on-line la estrategia es una mayor atención a la web como canal de trabajo para la mediación y por tanto con una orientación más profesional que hacia el consumidor final.

La captación de datos personales de los potenciales clientes se lleva a cabo a través de la cumplimentación de formularios voluntarios, y no siempre revestidos de todos los requisitos legales desde el punto de vista de la LOPD, para, posteriormente, enviar una comunicación (a través de correo electrónico) en la que se informa al destinatario de la oferta y se le invita a que se dirija a cualquier oficina comercial para firmar el contrato.

La posibilidad de contratar on-line es reducida limitándose a un 33,3% de y este porcentaje se reduce hasta el 22,2% en los casos de tramitación de siniestros u otros servicios con asistencia, reparación, etc. En la mayoría de los casos, se utiliza un sistema mixto que lleva a la perfección del contrato off-line. No obstante, el objeto de esta investigación se centra en el negocio jurídico on-line, por lo que delimitaremos el estudio a los aspectos jurídicos de la contratación en este entorno.

De otro lado, no conviene olvidar que la protección de datos personales en la contratación on-line y la identidad del usuario constituyen uno de los caballos de batalla que frena este tipo de negocios, de ahí que en los Capítulos anteriores se hayan profundizado en esta problemática, dedicando ahora nuestro interés a los elementos del contrato tales como: presencia no física de las partes, elementos esenciales del contrato, perfección del contrato y el valor de la póliza contratada on-line.

2. OBLIGACIONES DE LAS ASEGURADORAS COMO PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

Uno de los aspectos a tener en cuenta a la hora de la contratación electrónica son las obligaciones derivadas de la presencia en Internet de la empresa aseguradora. En este sentido, podemos distinguir entre las obligaciones estáticas y las dinámicas.

Obligaciones estáticas

Dentro de las primeras, se encuentran las generales de todos los prestadores de servicios; esto es, que cualquier compañía aseguradora presente en Internet y prestadora de servicios debe cumplir. La LSSI-CE[144] exige:

1. Comunicar el nombre o nombres de dominio de Internet que le correspondan al registro público en el que figure inscrita, para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con objeto de poder vincular su establecimiento físico o su "localización en la red". De este modo, el nombre de dominio cumple una función de identificador comercial de la entidad aseguradora.
   En el supuesto de prestadores de servicios que ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet, deben solicitar la anotación en el registro público en el que figuren inscritos de, al menos, uno de ellos.

2. Proporcionar información de manera continuada, fácil, directa y gratuita en relación a:

   a) nombre o denominación social.
   b) Residencia o domicilio, o bien la dirección de uno de sus establecimientos permanentes en España.
   c) Dirección de correo electrónico.
   d) Otros datos para establecer una comunicación efectiva y directa.
   e) Datos sobre la inscripción del nombre de dominio en el registro correspondiente.
   f) En el caso de autorización administrativa, datos sobre la misma y sobre el órgano supervisor.
   g) Si ejerce una profesión regulada:
      - Datos del Colegio profesional al que pertenezca y número de colegiado.
      - Título académico oficial o profesional con el que cuente.
      - Estado de la Unión Europea o del EEE en que se expidió el título y, la homologación, en su caso.
      - Normas profesionales aplicables al ejercicio de su profesión.
   h) Número de identificación fiscal.
   i) Precio del producto o servicio, indicando si se incluyen o no impuestos y gastos de envío.
   j) Código de conducta al que se encuentran adheridos y cómo consultarlos electrónicamente.

   La entidad aseguradora debe cumplir con todos estos requisitos desde el momento en que incluye la información en su página o sitio de Internet.

[144] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.

3. la entidad aseguradora tiene la obligación de facilitar al Ministerio de Industria, Turismos y Comercio, así como a los demás órganos previstos en la LSSI-CE (art. 36) la información y colaboración necesarias para el ejercicio de sus funciones.
   Entre ellas se incluye la de permitir el acceso a sus instalaciones y consultar cualquier información relevante para la actividad de control.
4. Cuando se realicen comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, la entidad aseguradora debe tener presente que está prohibido su envío salvo en los tres casos siguientes:
   a) que hayan sido previamente solicitadas por el receptor,
   b) que hayan sido expresamente autorizadas,
   c) que existe una relación contractual previa, si:
      - la entidad ha obtenido los datos de contacto del cliente de forma lícita y
      - los emplea para el envío de comunicaciones comerciales relacionados con los productos y servicios aseguradores que ofrece la empresa y que sean similares a los que inicialmente fueron objeto de contratación por el cliente.

En cualquier caso, las comunicaciones publicitarias que se realicen por vía electrónica deberán mostrar claramente en el asunto la palabra “publicidad” e indicar el nombre de la persona física o jurídica en cuyo nombre se realizan.

Obligaciones dinámicas

El segundo gran grupo de obligaciones se exige a las entidades aseguradoras que contratan electrónicamente o tienen una presencia más dinámica en la red. En este caso, junto a las obligaciones enumeradas más arriba se exigen una serie de requisitos añadidos como son:

a) Obligación de informar con carácter previo de los trámites que deben seguirse para celebrar el contrato.
b) Informar al cliente si va a archivar o no el documento electrónico en el que se formaliza el contrato y si éste va a ser accesible o no para el titular de los mismos.
c) Los medios técnicos que facilita al cliente para identificar y corregir errores en los datos.
d) Poner a disposición del cliente las condiciones generales del contrato de manera que puedan ser almacenadas e impresas por el destinatario.
   Este requisito no se exige en el caso de que ambas partes tengan la condición de empresa, cuando así lo hayan acordado, o en el caso de que el contrato se haya celebrado exclusivamente por correo electrónico o comunicación electrónica equivalente.

e) El plazo de validez de la oferta o propuesta de contratación vía electrónica, serán válidas durante el tiempo que fije el oferente, en caso contrario, será
f) válida durante el tiempo que permanezcan accesibles al destinatario, salvo lo dispuesto en la legislación sobre seguros.

3. SOLICITUD DEL SEGURO ON-LINE: RECOGIDA DE DATOS

La contratación electrónica es aquella que se celebra a distancia o sin que las partes estén simultáneamente presentes, enviándose en origen y siendo recibida en destino por equipos electrónicos de tratamiento y almacenaje de datos, y que además son en su totalidad transmitidos y recibidos por medio de cable, radio, medios ópticos o por otros medios electromagnéticos.

La regulación de la figura del contrato electrónico recogida en el anexo h) de la LSSI-CE no aparece contemplada como modelo nuevo de contrato sino que se trata de un negocio jurídico definido teniendo en cuenta la forma o el medio a través del cual se celebra y perfecciona.

En este modelo lo decisivo no es el contenido ni el documento o soporte del contrato sino el medio electrónico en el que el contrato surge y se desarrolla. Si el contrato se celebra utilizando una infraestructura de telecomunicaciones se estará ante un contrato electrónico ya se refiera a bienes o servicios, tenga un carácter oneroso o gratuito, tenga naturaleza civil o mercantil, sea cual sea la norma que rija los derechos y obligaciones de las partes y, se refleje o no en soporte electrónico.

Se trata, por tanto, de un contrato en el que la especificidad del medio lleva aparejada la alteración tanto de algunos elementos que intervienen en la formación del contrato como de los efectos del mismo, lo que permitiría hablar de nuevas modalidades atendiendo al medio digital en el que se celebran y perfeccionan.

Por otro lado, la forma en que tanto la *oferta* como la *aceptación* se transmiten resulta esencial para la catalogación del mismo. En este sentido, la LSSI es más precisa que la Directiva comunitaria de comercio electrónico puesto que ésta se refiere con carácter genérico a la celebración del contrato mientras que la ley española utiliza los términos *oferta* y *aceptación*.

En cualquier caso, el momento de perfeccionamiento del contrato es el que determina la calificación como electrónico en el caso de que las declaraciones de voluntad de las partes se manifiesten y transmitan a través del medio electrónico.

En este sentido, la propia LSSI-CE excluye de su ámbito de aplicación los negocios jurídicos que utilizan mecanismos electrónicos en su fase de

negociación, elaboración, ejecución, registro y prueba, pero que no se perfeccionan de forma electrónica sino mediante la presencia física de las partes o a través de otros medios de contratación a distancia. De modo que la LSSI sólo se aplica a los contratos celebrados en línea o sobre el tramo telemático en los contratos mixtos o contratos "on/off-line".

La LSSI-CE no exige, a diferencia de la Directiva 97/7/CE o la Directiva 2002/65/CE, que el contrato electrónico se celebre sin presencia física de las partes ni con la presencia simultánea de las mismas, ni siquiera prevé el empleo de técnicas de comunicación a distancia; sin embargo, esto se deduce de la definición de servicios de la sociedad de la información, incluida en el anexo a: "servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario".

Con ello, la ley opta por el criterio técnico (cualquier comunicación a distancia), acorde con la Ley 47/2002, de 19 de diciembre, de contratos a distancia, que considera como ventas a distancia: las celebradas sin la presencia física simultánea del comprador y del vendedor, siempre que su oferta y aceptación se realicen de forma exclusiva a través de una técnica cualquiera de comunicación a distancia organizada por el vendedor.

Al definir el contrato electrónico la LSSI incluye a "todo contrato" con lo que en sus aspectos generales se rigen por el Código Civil y de Comercio, así como por las restantes normas civiles y mercantiles sobre comercio.

Una de las deficiencias de la actual Ley de la Sociedad de la Información es la falta de distinción entre los contratos celebrados en Internet y los demás contratos electrónicos.

Asimismo se echa en falta una clarificación de la naturaleza de los contratos en tiempo real o alguna referencia a las consecuencias jurídicas de los contratos electrónicos "seguros" frente al resto.

4. PROPUESTA ON-LINE DEL SEGURO

Una vez que el tomador del seguro solicita la celebración del contrato, el asegurador hace una oferta que contiene los elementos esenciales para su conclusión. Esta declaración es una declaración de voluntad unilateral en la que el oferente propone la celebración de un contrato a otra persona y, además, concreta los requisitos del mismo, de manera que, si el destinatario los acepta, se entiende por tomado el contrato.

El Código Civil se refiere al momento en que se perfeccionan los contratos y lo hace coincidir con el consentimiento (artículo 1258). Desde ese instante las partes quedan obligadas al cumplimiento de lo expresamente pactado y a las

consecuencias que según su naturaleza, sean conformes a la buena fe y a la ley. Más adelante, el Código Civil concreta el alcance del artículo 1258 recogiendo la única referencia expresa y directa de la oferta. De este modo, reconoce que el consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que van a constituir el objeto del contrato.

Por tanto, una propuesta de celebrar un contrato constituye una oferta si es suficientemente precisa e indica la intención del asegurador de quedar obligado en caso de aceptación.

La proposición del seguro debe contener las condiciones y elementos esenciales del contrato (objeto, interés asegurado, clase, duración, cuantía de las prestaciones y definición del riesgo) y las condiciones generales del contrato.

La proposición del seguro ha de contener además la firma del asegurador y debe dirigirse y entregarse al peticionario.

La proposición del seguro que contiene la oferta del contrato de seguro vincula al asegurador durante el plazo de quince días trascurrido el cual (o más amplio a voluntad de la entidad aseguradora) la oferta pierde sus efectos jurídicos salvo que el asegurador quiera prorrogarla de manera expresa o tácita.

En el caso de la contratación electrónica de un seguro, existe una equivalencia funcional de la propuesta electrónica del seguro si se dan las siguientes condiciones:

- Que la propuesta esté firmada electrónicamente por la aseguradora, siempre y cuando se utilicen métodos fiables de identificación y de aceptación que figura en el mensaje de datos.
  Para ello la Ley de Contrato de Seguros exige que los mensajes de datos que forman el contrato electrónico de seguro y las comunicaciones que resulten del mismo, garanticen la integridad del mensaje, la autenticidad y su no alteración (Disposición Adicional 2ª); esto es, que la propuesta (mensaje de datos) sea firmado por la aseguradora con firma electrónica avanzada o reconocida.

- Que la información del mensaje de datos que contiene la propuesta electrónica del contrato de seguro es accesible para su ulterior consulta[145].

[145] Disposición Adicional Primera de la Ley de Contratos de Seguros: *"Siempre que esta ley exija que el contrato de seguro o cualquier otra información relacionada con el mismo conste por escrito, este requisito se entenderá cumplido si el contrato o la información se contienen en papel u otro soporte duradero que permita guardar, recuperar fácilmente y reproducir sin cambios el contrato o la información".* Este precepto se ha considerado por muchos como innecesario en una ley de contenido tan concreto puesto que la equivalencia funcional ya

En cualquier caso, no es suficiente en el proceso de contratación electrónica del seguro que en la página *web* se indique la posibilidad de obtener la propuesta solicitándola por e-mail, sino que el cliente debe tener acceso directo a la propuesta del contrato antes de aceptar.

Esta interpretación se extrae de la propia LSSI y CE (art.27.4) que exige que, con carácter previo al inicio del procedimiento de contratación, "*el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario*"[146].

En relación a los supuestos de partes que se hallan en lugares físicos distintos, *hay consentimiento cuando el oferente conoce la aceptación o desde que habiéndosela remitido el aceptante no puede ignorarla sin faltar a la buena fe.* En tal caso, el contrato se presume celebrado en el lugar en que se hizo la oferta.

En cuanto a los contratos celebrados mediante dispositivos automáticos, en el contrato se entiende que hay consentimiento desde el momento en que se manifiesta la aceptación.

Otro aspecto importante a tener en cuenta es el lugar de celebración del contrato. En este sentido, la LSSI y CE se inclina por defender los intereses del consumidor y fija como tal el lugar de residencia habitual del consumidor para los contratos celebrados por vía electrónica.

En cambio, los contratos electrónicos entre empresarios o profesionales se presumen celebrados en el lugar en que esté establecido el prestador de servicios.

5. PERFECCIÓN DEL CONTRATO DE SEGURO ON-LINE

5.1. La aceptación

Con la aceptación se emite una declaración de voluntad unilateral del tomador del seguro dirigida al asegurador en la que se manifiesta la conformidad y cuya concurrencia implica la perfección del contrato.

En el caso de la aceptación telemática debe cumplirse los siguientes requisitos:

---

aparece recogida en la LSSI y CE en relación a cualquier declaración de voluntad electrónica asociada a cualquier contrato.

[146] En este sentido también se pronuncia la Directiva 2000/31/CE de Comercio Electrónico, en su artículo 103: *"las condiciones generales de los contratos facilitadas al destinatario deben estar disponibles de tal manera que éste pueda almacenarlas y reproducirlas".*

1. Correspondencia exacta entre la oferta y la aceptación. La intención de contratar debe ser clara y coincidir con los términos establecidos en la oferta.
2. Definitiva. Se excluye la aceptación condicional y con reservas.
3. Dentro del plazo. Se debe producir antes que se haya revocado la oferta o que haya trascurrido el plazo establecido en la oferta.

La aceptación del tomador puede hacerse de forma expresa o tácita. La aceptación se realiza de forma expresa con la firma de la proposición telemática enviada al asegurador, si bien sólo el mensaje de datos producido por medios telemáticos y asociado a una firma electrónica reconocida puede reconocerse como elemento de un contrato electrónico de seguro. En este sentido, la ley de firma electrónica únicamente admite como firma con valor jurídico la firma electrónica avanzada.

No obstante, la aceptación del seguro también puede realizarse a través de una declaración tácita de voluntad que se produce con el pago de la prima incluida en la proposición.

En este sentido la Disposición Adicional Tercera de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro dispone que:

> *Los contratos de seguros celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico cuando concurran el consentimiento y los demás requisitos necesarios para su valides. En cuanto a su validez, prueba de celebración y obligaciones derivadas del mismo se sujetarán a la normativa específica del contrato de seguro y a la legislación sobre servicios de la sociedad de la información y de comercio electrónico.*

5.2. La prueba

Respecto de la prueba del contrato y partiendo de la libertad de forma que rige en nuestro ordenamiento jurídico, en la contratación de seguros vía electrónica, cobra especial relevancia el momento de la aceptación hasta el punto de poder diferenciar entre los medios de prueba de la aceptación electrónica, en sí, y la prueba de la información contenida en el proceso de contratación.

En cualquier caso, la carga de la prueba recae en la compañía aseguradora.

1. La aceptación electrónica

Confirmar la aceptación permite demostrar la certeza de la recepción.

Nuestro marco legal va más allá tipificando los medios de confirmar la recepción que son el acuse de recibo y la confirmación propiamente dicha, si bien ambos presentan el problema de no garantizar la inalterabilidad del mensaje sino sólo la recepción por el destinatario.

La LSSI-CE refuerza, por tanto, la posición del tomador del seguro exigiendo al oferente confirmar la recepción de la aceptación en los siguientes términos:

a) envío de acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente, a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o
b) confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

El acuse de recibo es un mensaje electrónico por el que el emisor declara la recepción del mensaje electrónico remitido por el destinatario. La aseguradora enviará al aceptante el mensaje electrónico que acredite la llegada y recepción de la aceptación del contrato.

Asimismo el acuse de recibo puede incluir los requisitos técnicos del mensaje recibido, en concreto, la sintaxis informática o la legibilidad el mensaje. En este caso se garantiza no sólo que el cliente ha recibido el mensaje sino que ha accedido al mismo, puesto que el sistema informático del destinatario hace legible el mensaje.

El otro medio de prueba que acredita que el cliente ha recibido la aceptación del contrato es la confirmación del mensaje, mediante la remisión por duplicado del mensaje electrónico a efectos de confirmar al emisor la recepción. De esta manera la aseguradora puede comprobar el contenido del mensaje de aceptación que envió, el origen del mensaje, la fecha, etc. Además, existe la posibilidad técnica de ampliar la confirmación de la recepción no sólo a una declaración sino al contenido de la misma.

La LSSI y CE impone multas de 30.001 a 150.000 euros por lo que califica de infracciones graves[147] en caso de incumplimiento habitual de la obligación de confirmar la recepción de una aceptación cuando expresamente no se haya

[147] Artículo 38.4, f: "*Son infracciones leves: el incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado por un consumidor salvo que constituya infracción grave*". Por la comisión de infracciones leves la multa pude ascender hasta 30.000 euros (artículo 39 c).

Este tipo de infracciones se convierten automáticamente en graves cuando se incumple de manera habitual la obligación de confirmar la recepción, salvo que se hubiese pactado lo contrario.

pactado su exclusión, en el caso de que ambas partes sean personas jurídicas y, en cualquier caso, cuando una de las partes sea un consumidor (artículo 38.3 d)

Por tanto, la carga de la prueba recae siempre en la aseguradora en virtud de la LSSI si bien no es necesario confirmar la aceptación de una oferta cuando:

a) ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o
b) cuando el contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.

Se entiende que la aseguradora ha recibido la aceptación y su confirmación cuando pueda tener constancia de ello. En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico o en el dispositivo utilizado para la recepción de comunicaciones.

2. La prueba del contrato

Por lo que se refiere a la información propiamente dicha del contrato, el RD 1828/1999, abre la posibilidad de registrar los datos correspondientes a las condiciones generales de contratación en la página web del Registro de Condiciones Generales de Contratación utilizando una firma electrónica avanzada, si bien el RD 1906/1999, de protección de los consumidores excluye expresamente de su ámbito de aplicación a los seguros y reaseguros (artículo 1), sin perjuicio de que quede constancia documental de la contratación efectuada en registros magnéticos o informáticos. A falta de ésta, se enviará inmediatamente al cliente justificación escrita de la contratación efectuada, donde constarán los términos de la misma.

La obligación de acreditar esta información alcanza a los siguientes extremos (RD 1906/1999):

- existencia y contenido de la información previa de las cláusulas del contrato,
- remisión de la información previa y justificación documental,
- entrega de las condiciones generales,
- renuncia expresa del derecho de resolución,
- correspondencia entre la información, la entrega y la justificación documental y el momento de sus respectivos envíos.

El Registro de Condiciones Generales de la contratación permite dar publicidad jurídica a las condiciones generales de la contratación. En él se

inscribirán obligatoriamente la Sentencias que declaren nulas por abusivas las cláusulas de un contrato. De esta manera ni los Notarios podrán autorizar contratos que las incluyan ni los Registradores podrán inscribir cláusulas abusivas.

Este Registro fue creado con el objeto de facilitar el ejercicio de acciones colectivas y el desarrollo uniforme de la actividad judicial en relación a la declaración o no como abusivas de las cláusulas utilizadas por los empresarios o profesionales en los contratos.

Con carácter general, la Ley de Condiciones Generales de Contratación establece el carácter voluntario de la inscripción del clausurado mediante el depósito de los modelos contractuales en los que se utilicen condiciones generales, si bien, por vía reglamentaria cabe exigir el depósito obligatorio en sectores específicos.

El objetivo es doble. Por un lado, se persigue conseguir una mayor transparencia en el tráfico jurídico que consolide la confianza del consumidor y, por otro, se refuerza la seguridad jurídica en la contratación privada.

El RD 1906/1999 admite el registro cualquier documento independientemente del soporte siempre que quede garantizada la autenticación de las partes, la integridad de su contenido y el momento de su emisión y recepción.

En el supuesto de la contratación electrónica, es aconsejable que las partes utilicen la firma electrónica avanzada por ser ésta la única a la que nuestro ordenamiento jurídico otorga la misma validez jurídica que a la manuscrita. En cualquier caso, deberá acompañarse de la fecha y hora de la remisión y recepción.

Eso no significa que las partes no puedan utilizar la firma electrónica (digital o no), si bien hay que tener en cuenta que ésta no consigue la equiparación legal a la firma manuscrita.

Por tanto, para poder obtener la presunción legal por la que la firma electrónica tenga el mismo valor jurídico que la firma manuscrita y demostrar así, sin mayores requisitos la autenticación e integridad de los documentos del contrato, la firma electrónica que se utilice debe reunir las siguientes características:

- que esté basada en un certificado reconocido;
- que haya sido producida por un dispositivo seguro de creación de firma; que el certificado reconocido haya sido expedido por un prestador de servicios de certificación acreditado;
- y, que el dispositivo seguro de creación de firma esté certificado.

5.3. Momento de perfección

Se apuntaba más arriba la reforma que la LSSI y CE ha introducido en el Código Civil y en el Código de Comercio unificando el criterio de determinación del momento de perfección del contrato de seguro on-line.

De este modo, la Disposición Adicional nº 48 recoge una importante modificación en virtud de la cual:

> *El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato. Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato en tal caso se presume celebrado mediante dispositivos automáticos y hay consentimiento desde que se manifiesta la aceptación.*

La redacción anterior del artículo 1262 Código Civil disponía que: *"el consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que de constituir el contrato. La aceptación hecha por carta no obliga al que hizo la oferta sino desde que llegó a su conocimiento".*

Frente a esto el Código de Comercio acogía la teoría de la emisión en su artículo 54, de manera que: "*los contratos que se contesten por correspondencia quedarán perfeccionados desde que se conteste aceptando la propuesta o las condiciones con que ésta fuere modificada*".

Con estos dos preceptos, la doctrina en torno a la perfección del contrato de seguro se debatía entre la teoría del conocimiento y la teoría de la emisión o declaración de aceptación. Una parte de la doctrina se inclinaba por la aplicación del artículo 54 del Código de Comercio, de manera que el contrato de seguro a distancia se consideraba perfeccionado desde el momento en que se contestaba aceptando la propuesta escrita del asegurador o la póliza firmada por el tomador del seguro. Por el contrario, otros autores abogaban por la aplicación del artículo 1262 del Código Civil entendiendo que el contrato de seguro se perfeccionaba cuando la aceptación llegaba a conocimiento de quien hizo la oferta.

La nueva redacción dada al Código Civil y al Código de Comercio plantea una serie de cuestiones respecto al momento de perfección del contrato electrónico de seguro. Partiendo de la base de que estamos ante un contrato a distancia que se caracteriza por la especialidad de los medios empleados para su celebración, mayoritariamente correos electrónicos o páginas web, la primera cuestión es cuándo se considera perfeccionado el contrato de seguro realizado por medios electrónicos en el caso de envío de mails cuya lectura se produce cuando el receptor visita los envíos recibidos. ¿Se puede considerar

que el mensaje de datos se entrega al destinatario cuando éste lo recupera realmente en su cuenta de correo?.

La segunda cuestión está relacionada también con el medio electrónico empleado. ¿Cuál es el momento de perfección del contrato en el caso de contratación de pólizas mediante página web?. ¿Habrá de entenderse que la perfección se produce cuado la aceptación llega a la web de la aseguradora?.

Todas estas cuestiones encuentran cobertura en la LSSI y CE que entiende que se ha recibido la aceptación y su confirmación cuando las partes a las que se dirijan puedan tener constancia de ello (artículo 28.2). Para ello se estará al momento de recepción del acuse de recibo de la aceptación; esto es: se presume que el destinatario tiene la referida constancia desde el momento en que haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico o en el dispositivo utilizado para la recepción de comunicaciones.

De este modo, la perfección del contrato de seguro por correo electrónico se produce con la concurrencia de la oferta y la aceptación cuando la empresa aseguradora tiene en su poder la aceptación de la otra parte y no puede desconocerla sin faltar a la buena fe. Por tanto, la recepción del mensaje se produce cuando las partes puedan tener acceso al mismo lo que, desde el punto de vista técnico, tiene lugar en el momento en que los datos entran en el servidor del destinatario.

En cuanto a la perfección del contrato celebrado vía página web ésta se produce en el momento en que el tomador del seguro manifiesta su aceptación utilizando el mecanismo dispuesto en la página por la aseguradora. Desde ese momento el cliente no podrá ignorar la aceptación sin faltar a la buena fe. Técnicamente el destinatario de la aceptación realizada en una página web puede tener constancia de ésta en el momento en que el mensaje de datos es recibido por el dispositivo que la página emplea para la recepción de comunicaciones. Por tanto, a tenor de lo establecido en la LSSI-CE el destinatario debe poder tener constancia de la recepción de la aceptación y se entiende que la tiene desde el momento en que el mensaje está a disposición de la aseguradora (accesibilidad).

6. EL VALOR DE LA PÓLIZA

En materia de contratación la regla general es la no obligatoriedad de la forma escrita, si bien este principio quiebra en determinados supuestos como ocurre en el caso de los seguros. De este modo, el artículo 5 de la LCS exige la formalización por escrito del contrato de seguro como medio de prueba del mismo en los siguientes términos: "*el asegurador está obligado a entregar al tomador del seguro la póliza o, al menos el documento de cobertura*

provisional". El documento escrito cumple, por tanto, una función probatoria de las condiciones generales y específicas del contrato.

La cuestión es cómo trasladar esta obligación al entorno digital de la conclusión de contratos de seguros en Internet. La equivalencia funcional contenida en la LSSI-CE[148] permite equiparar la entrega del documento en papel con la puesta a disposición del cliente de la póliza por medios telemáticos, si bien delimita claramente las condiciones para que esto se produzca que pasan porque el tomador del seguro pueda almacenarla y reproducirla sin introducir cambios.

Esta equivalencia se recoge expresamente en la normativa aseguradora de la siguiente manera: "*Siempre que esta ley exija que el contrato de seguro o cualquier otra información relacionada con el mismo conste por escrito, este requisito se entenderá cumplido si el contrato o la información se contiene en papel u otro soporte duradero que permita guardar, recuperar fácilmente y reproducir sin cambios el contrato o la información".*[149]

Por último, el legislador en lugar de abogar por la alteridad de pólizas (descarga o entrega en papel) simplificando así el proceso, ha optado por reforzar la protección del tomador del seguro duplicando las formas de disponer de la póliza. De manera que, junto con aquélla que puede descargar e imprimir, el asegurado puede además solicitar de la compañía aseguradora, en cualquier momento, la póliza en papel y aún más, se le reconoce el derecho a modificar, incluso una vez aceptada la póliza, las técnicas a distancia utilizadas (artículo 60 de la ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión del Seguros Privados).

7. RESUMEN COMPARATIVO DE LA DIRECTIVA SOBRE COMERCIO ELECTRÓNICO Y LA LEY 34/2002, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL COMERCIO ELECTRÓNICO

En este apartado se expone gráficamente lo analizado a lo largo del Capítulo con intención de destacar los aspectos más conflictivos que se han tratado y las soluciones propuestas por el legislador.

En este sentido, el cuadro refleja el detalle con que nuestra legislación ha acogido la norma comunitaria que regula la contratación en Internet y que, por

[148] Artículos 23.3, 24 y 27.4 relativos a las condiciones generales del contrato electrónico.

[149] Disposición Adicional Primera de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro. Y en el mismo sentido, la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de Seguros Privados (art. 65.2 a), define el concepto de soporte duradero como todo instrumento que permita almacenar información que pueda recuperarse fácilmente y que se mantenga durante el período de tiempo necesario que permita alcanzar los fines para los que se recabó la información, pudiendo, además, reproducirla sin cambios.

analogía, se aplica al sector seguros. De este modo, se puede acceder rápidamente a cuestiones básicas que suelen constituir preguntas frecuentes en la contratación electrónica.

En la Unión Europea las Directivas no tienen un efecto directo como ocurre con los Reglamentos, que son de aplicación directa en todos los Estados miembros desde el momento de su entrada en vigor con la publicación oficial. Las Directivas comunitarias, por el contrario, deben ser traspuestas al ordenamiento interno de los Estados en el plazo que se marque en la propia norma y, sólo transcurrido ese período, comenzarán a tener efecto en los términos establecidos en la propia Directiva.

Por otro lado, los distintos Tratados Comunitarios y la práctica diaria refrendada por la doctrina comunitaria aconsejaron la aplicación del principio de subsidiariedad en virtud del cual las normas comunitarias se limitan a establecer el marco de referencia trasladando a los Estados miembros la obligación de adoptar el contenido y orientando la aplicación de las normas comunitarias hacia las necesidades y realidades de sus destinatarios nacionales.

Partiendo de lo anterior y el carácter difuminado de las fronteras en el entorno de la contratación electrónica, las normas jurídicas sobre la materia tienen en cuenta no sólo el entorno en que se desarrollará la relación sino también la protección de los intereses de los usuarios nacionales. De ahí que la LSSI y CE preste especial atención a la definición de los actores y servicios y a los prestadores incluidos en su ámbito.

Otro aspecto importante que se ha tratado en este capítulo es el de los efectos y validez jurídica del contrato celebrado vía electrónica, así como el valor de la prueba que permite garantizar que ambas partes convienen en obligarse.

En tercer lugar, se compara la redacción de las obligaciones previas y posteriores a la celebración del contrato, donde, de nuevo, la ley española concreta el alcance de la europea.

Por último, el momento y lugar de celebración del contrato, al margen de la importante reforma del Código Civil y del Código de Comercio que la ley ha exigido, aparecen expresamente recogidos en la LSSI y CE de manera que la primera marcará el inicio de los efectos del contrato y el segundo el derecho aplicable.

CONTRATACIÓN DE SEGUROS ON-LINE		
	Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)	**Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico**
Servicios de la sociedad de la información	Servicios en el sentido de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE.	Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. Son servicios de la sociedad de la información la contratación de bienes y servicios por vía electrónica.
Prestador de servicios de la sociedad de la información	Cualquier persona física o jurídica que suministre un servicio de la sociedad de la información	Persona física o jurídica que proporciona un servicio en la sociedad de la información.
Ley aplicable	Libertad de las partes para elegir la legislación aplicable a su contrato	La determinación de la ley aplicable a los contratos electrónicos de seguros se realiza sobre la base del Derecho Internacional Privado español, teniendo en cuenta lo establecido en los artículos 2 y 3.

CONTRATACIÓN DE SEGUROS ON-LINE		
	Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)	**Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico**
Ámbito de aplicación	Se aproximarán entre sí las disposiciones nacionales aplicables a los servicios de la sociedad de la información para contribuir: - al buen funcionamiento del mercado interior - al establecimiento de los prestadores de servicios - a las comunicaciones comerciales - a poscontratos por vía electrónica - a la responsabilidad de los intermediarios - a los códigos de conducta, a los acuerdos extrajudiciales para la solución relitigios - a los recursos judiciales y - a la cooperación entre Estados miembros	Es de aplicación a las entidades aseguradoras que presten servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellas. Se presume que la entidad aseguradora está establecida en España cuando ella o alguna de sus sucursales se encuentre inscrita en el Registro Mercantil o en otro Registro Público español en el que fuera necesaria la inscripción para la adquisición de la personalidad jurídica. Prestadoras residentes o domiciliadas en otro Estado miembro que ofrezcan sus servicios a través de establecimiento permanente situado en España. Entidades aseguradoras establecidas en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo respecto a los siguientes servicios (salvo que la norma reguladora de la materia específica no sea de aplicación la ley del país en que resida o esté establecido el destinatario del servicio): - Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios. - Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores

Ámbito de aplicación		- Régimen de elección por las partes contratantes de la legislación aplicable al contrato. Aseguradoras no pertenecientes a la Unión Europea o Espacio Económico Europeo (EEE): - A los prestadores establecidos fuera de la Unión Europea o que no pertenezcan al EEE le será de aplicación lo previsto en los artículos 7.2 y 8 de esta ley respecto a la libre prestación de servicios y a su restricción. - Si los prestadores dirigen sus servicios específicamente al territorio español quedarán sujetos a las previsiones de esta ley.
Exclusiones	Los Estados miembros podrán disponer la no celebración por vía electrónica de los contratos incluidos en alguno de estos supuestos: a.Los contratos de creación o transferencia de derechos en materia inmobiliaria, con la excepción de los derechos de arrendamiento. b.Los contratos que requieran por ley la intervención de los tribunales, las autoridades públicas o profesionales que ejerzan una función pública. c.Los contratos de crédito y caución y las garantías presentadas por personas que actúan por motivos ajenos a su actividad económica, negocio o profesión. d. Los contratos de Derecho de Familia o de Sucesiones.	No podrán celebrarse por vía electrónica los contratos, negocios o actos jurídicos relativos al Derecho de Familia y sucesiones.

CONTRATACIÓN DE SEGUROS ON-LINE		
	Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)	**Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico**
Efectos y validez jurídica	Los Estados miembros velarán porque su legislación permita la celebración de contratos por vía electrónica garantizando que el régimen jurídico aplicable al contrato no entorpezca la utilización real de los contratos por vía electrónica ni conduzca a privar de efecto y de validez jurídica a este tipo de contratos por el sólo motivo del mecanismo electrónico utilizado en su celebración	Los contratos celebrados por vía electrónica producirán todos los efectos previstos en el Ordenamiento jurídicos cuando concurran el consentimiento, objeto y causa, necesarios para su validez. Los contratos electrónicos de seguros se regirán por el Código Civil, el de Comercio y por la Ley de Contratos de Seguros, la Ley de Ordenación del Seguro Privado, resto de la normativa específica en materia de contratos, por las normas de protección de los consumidores y usuarios así como las de ordenación de la actividad comercial. Para que sea válida la celebración de contratos de seguros vía electrónica no es necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos. Los contratos de seguros celebrados por vía electrónica tienen el mismo valor jurídico que los formalizados en cualquier otro soporte documental a efectos de las obligaciones que resulten de ellos. Cuando en el contrato se exigiera la forma documental pública para la eficacia y validez del contrato se estará a lo dispuesto en la legislación de seguros en lo relacionado a la intervención de órganos jurisdiccionales, registradores de la propiedad y mercantiles o autoridades públicas.

Prueba	Las condiciones generales de contratación deben facilitarse al destinatario y estar disponible de manera que puedan almacenarse y reproducirse. El prestador del servicio debe acusar recibo del pedido del destinatario sin demora indebida y por vía electrónica. Se considera que se ha recibido el pedido y el acuse de recibo cuando las partes a las que se dirigen puedan tener acceso a los mismos.	La prueba de la celebración de un contrato de seguros *on-line* y de las obligaciones derivadas de él se rige por las reglas generales del Ordenamiento jurídico, por lo tanto la carga de la prueba recae sobre la entidad aseguradora. Se rige también por lo dispuesto sobre el valor de los documentos electrónicos en las normas procesales, Y por lo previsto en la Ley de firma electrónica (art. 3).
Momento de celebración del contrato	No previsto en la Directiva	Tomador: en el contrato de seguro celebrado vía electrónica se entenderá prestado el consentimiento en el momento en que el destinatario de la oferta de contratación emite su aceptación. Entidad aseguradora: hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe.
Lugar de celebración	Se determina en función del lugar de establecimiento del prestador de servicios entre personas jurídicas. Cuando se trata de una sociedad que proporciona servicios mediante un sitio Internet, dicho lugar de establecimiento no se encuentra allí donde está la tecnología que mantiene el sitio sino en el lugar donde se desarrolla la actividad económica. En caso de que existan varios establecimientos de un mismo prestador de servicios se tomará como referencia aquél en que el prestador tenga su centro de actividades en relación con esa servicio en particular.	Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual. Los contratos electrónicos entre entidades aseguradoras, entre estas y otras empresas o profesionales se presumen celebrados en el lugar en que esté establecido el prestador de servicios.

CONTRATACIÓN DE SEGUROS ON-LINE		
	Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)	**Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico**
Obligaciones previas	Los Estados miembros garantizarán, excepto cuando las partes que no sean consumidores así lo acuerden, que el prestador de servicios facilite al menos la siguiente información de manera clara, comprensible e inequívoca y antes de que el destinatario del servicio efectúe un pedido: a) los diferentes pasos técnicos que deben darse para celebrar el contrato, b) si el prestador de servicios va a registrar o no el contrato celebrado, y si éste va a ser accesible, c) los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido, d) las lenguas ofrecidas para la celebración del contrato.	Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente , el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de informar de manera clara, comprensible e inequívoca y antes de que el destinatario del seguro inicie el procedimiento de contratación, sobre los siguientes extremos: a) los distintos trámites que deben seguirse para celebrar el contrato, b) si la aseguradora va a archivar el documento electrónico formalizador del contrato y si éste va a ser accesible, c) los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y d) la lengua o lenguas en que, a elección del consumidor podrá formalizarse el contrato. La entidad aseguradora no tendrá la obligación de facilitar dicha información cuando: a) ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

Obligaciones previas	Los Estados miembros garantizarán que, excepto cuando las partes que no son consumidores así lo acuerden, el prestador de servicios indique los códigos de conducta correspondientes a los que se acoja y facilite información sobre la manera de consultar electrónicamente dichos códigos. Lo anterior no será de aplicación a los contratos celebrados exclusivamente mediante intercambio de correo electrónico u otra comunicación individual equivalente. Las condiciones generales de los contratos facilitados al destinatario deben estar disponibles de tal manera que éste pueda almacenarlas y reproducirlas.	b) el contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente. Las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período de quince días o, en su defecto, si no se amplía el plazo por la aseguradora, durante el tiempo que permanezcan accesibles al tomador del seguro. Con carácter previo al inicio del procedimiento de contratación, la entidad aseguradora deberá poner a disposición del destinatario las condiciones generales a que, en su caso deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.
Información posterior	Los Estados miembros garantizarán que, excepto cuando las partes que no son consumidores así lo acuerden, en los casos en que el destinatario de un servicio efectúe su pedido por vía electrónica, se aplicarán los principios siguientes: - El prestador de servicios debe acusar recibo del pedido del destinatario sin demora indebida y por vía electrónica. - Se considera que se han recibido el pedido y el acuse de recibo cuando las partes a las que se dirigen puedan tener acceso a los mismos.	La entidad aseguradora está obligada a confirmar la recepción de la aceptación al tomador por alguno de los siguientes medios: a) el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente, a la dirección que el aceptante haya señalado, en el plazo de veinticuatro horas siguientes a la recepción de la aceptación, o b) la confirmación por un medio equivalente al utilizado en el procedimiento de contratación de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

Información posterior	**Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)** Los Estados miembros garantizarán que, excepto cuando así lo acuerden las partes que no son consumidores, el prestadores del servicio ponga a disposición del destinatario del servicio los medios técnicos adecuados, eficaces, accesibles que le permitan identificar y corregir los errores de introducción de datos antes de realizar el pedido. No es necesario que el prestador del servicio acuse recibo de la recepción del pedido realizada por el destinatario en los contratos celebrados exclusivamente por intercambio de correo electrónico u otra comunicación individual equivalente.	**Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico** En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, ya deba dirigirse ésta al propio prestador o a otro destinatario del seguro, dicha aseguradora facilitará el cumplimiento de la obligación poniendo a su disposición alguno de los medios indicados en este apartado. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello. En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia, desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones, No será necesario confirmar la recepción de la aceptación de una oferta cuando: a) ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o b) el contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente

Capítulo VI
MEDIOS DE PRUEBA ELECTRÓNICA

SUMARIO: 1. EL ARTÍCULO 5 LCS Y LA LSSI-CE. 2. EL DOCUMENTO ELECTRÓNICO. 3. LA FIRMA ELECTRÓNICA. 3.1.- Clases de firma electrónica. 3.2.- La regulación legal de la firma electrónica. 4. EL DNI ELECTRÓNICO. 4.1.- Regulación legal. 4.2.- Descripción del DNIe. 4.3.- Los certificados electrónicos en el DNIe. 4.4.- La Autoridad de Validación. 4.5.- Seguridad. 4.6.- Aplicación de firma. 4.7.- Conclusiones.

1. ARTÍCULO 5 DE LA LEY DE CONTRATOS DE SEGURO y la LSSI-CE

En este apartado se analiza el artículo 5 de la Ley de Contrato de Seguro desde la óptica de la prueba electrónica como fase final del proceso de contratación on-line.

La Ley 50/1980, de 8 de octubre, de Contrato de Seguro, fue pionera en la legislación sectorial de protección de los consumidores, adelantándose casi cuatro años a la Ley General para la Defensa de los Consumidores y Usuarios (Ley 26/1984, de 19 de julio) y en casi veinte a la Ley sobre Condiciones Generales de la Contratación (Ley 7/1998, de 13 de abril) de la que quedó excluido el contrato de seguro.

El artículo 5 de la ley establece que "el contrato de seguro y sus modificaciones o adiciones deberán ser formalizadas por escrito. El asegurador está obligado a entregar al tomador del seguro la póliza o, al menos, el documento de cobertura provisional". En aquellas "modalidades de seguro en que por disposiciones especiales no se exija la emisión de la póliza el asegurador estará obligado a entregar el documento que en ellas se establezca".

A pesar de esta redacción no se sabe muy bien cuáles son las consecuencias jurídicas del incumplimiento por el asegurador de tales requisitos, dado que el contrato de seguro no es un contrato formal, como así lo ha declarado reiteradamente la jurisprudencia, y la consecuencia de su incumplimiento no es la nulidad, sino que todo dependerá de la omisión en concreto.

Otra de las cuestiones de debate reside en el concepto mismo de póliza puesto que la propia LCS en distintos preceptos se refiere a la póliza y a los documentos complementarios como cosas distintas (arts. 3, 5. 8, etc) si bien no está muy claro qué debe considerarse póliza. Lo único que parece claro es el concepto de "contrato de seguro" que, desde un punto de vista formal, debe considerarse como el conjunto de documentos: proposición del seguro, póliza,

documentos complementarios) en el que se contienen sus elementos fundamentales y las obligaciones y derechos de las partes.

De lo que no cabe duda es de que en la contratación electrónica de productos aseguradores el cliente debe recibir en su ordenador, y poder editar, el documento que acredite que ha suscrito el contrato, independientemente de que el contrato definitivo lo reciba por correo ordinario y éste comience a surtir efectos a partir del momento en que la póliza firmada llegue a la entidad aseguradora.

En este sentido, recordemos que la LSSI-CE establece que una vez realizada la contratación la entidad aseguradora debe confirmar a los clientes la recepción a través de:

a) un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente.
b) un medio equivalente al utilizado en el procedimiento de contratación.

Además la LSSI-CE exige el cumplimiento de dos requisitos más:

c) Proporcionar al destinatario información con carácter posterior a la celebración del contrato:

   - De la recepción de su aceptación mediante el envío del acuse de recibo, o medio de comunicación equivalente, a la dirección facilitada por el cliente, en el plazo de las veinticuatro horas siguientes desde que recibió la aceptación, o medio equivalente utilizado en el procedimiento de contratación, siempre que la confirmación pueda ser archivada por el destinatario.
   - En el caso de que la obligación de confirmar recaiga en el cliente, la aseguradora deberá facilitar su cumplimiento proporcionando al destinatario alguno de los medios señalados anteriormente.

d) Se considera que hay aceptación y confirmación cuando ambas partes de la conexión tengan constancia de ello, si bien cuando para esa confirmación se utilice acuse de recibo se presume que el destinatario tiene constancia de ello desde el momento en que el mensaje se almacenó en el servidor correspondiente a su cuenta de correo electrónico.

Existen dos casos en que no es necesario confirmar la recepción de la aceptación:

1. Cuando así lo acuerdan ambas partes, y ninguno tiene la consideración de consumidor,
2. cuando el contrato se ha celebrado exclusivamente a través del intercambio de correo electrónico o comunicación electrónica

equivalente, salvo que se haya utilizado este mecanismo con el fin de esquivar el cumplimiento de la obligación de confirmar la recepción.

2. EL DOCUMENTO ELECTRÓNICO

El desarrollo del comercio electrónico ha supuesto un profundo cambio en las transacciones, comunicaciones, entregas y servicios. De ahí que una de las necesidades sea fijar medidas de seguridad técnica y jurídica. En este momento nos vamos a centrar en las segundas y, concretamente en la seguridad de los documentos electrónicos que circulan por la gran Red. En este sentido, lo primero que hay que tener presente es que el documento papel deja paso en este nuevo contexto al documento electrónico y, unido a ello, desaparecen las firmas manuscritas tradicionales para ser reemplazadas por las firmas electrónicas.

El régimen jurídico de la prueba de la celebración de contratos de seguros vía electrónica y las obligaciones que de ellos se derivan están sujetos a las reglas generales de contratación y a lo establecido en la legislación sobre firma electrónica que se analiza en el siguiente epígrafe.

Se pueden diferenciar tres clases de documentos electrónicos:

1. *Printout*: documento en papel generado por medios informáticos; esto es, la versión impresa del documento recogido en soporte informático.
2. *Input*: documento informático que se encuentra en soporte de información electrónico creado con datos almacenados en la memoria de un ordenador.
3. *EDI (Electronic Data Interchange)*: soporte de información electrónico generado mediante el intercambio de mensajes con una determinada estructura y utilizando normas de intercambio informáticas (intercambio normalizado de datos).

Estos tres tipos se agrupan normalmente en los dos primeros, distinguiéndose entre:

- el documento en *soporte papel* cuyo contenido se ha generado por medios electrónicos y
- el documento en *soporte electrónico* cuyo contenido se haya generado por medios electrónicos.

En los dos casos, el contenido del documento se puede transmitir de dos maneras:

1. Utilizando un periférico (impresora) a través de la comunicación de la unidad central de proceso (ordenador) y el periférico.
2. Utilizando una vía de comunicación distinta a los elementos periféricos del ordenador.

Ambos documentos se utilizan en la actividad diaria del sector asegurador. Pensemos en la contratación de un seguro de accidente a través de Internet. El cliente rellena los formularios y los imprime quedando el original registrado en soporte informático. A esta operación se añaden otras en cadena como el pago de la prima mediante tarjetas de crédito o transferencia bancaria que va conformando la validez de la forma electrónica de la operación y su admisibilidad en juicio como prueba.

Para poder utilizar estos documentos debe garantizarse la fiabilidad de los contenidos y la seguridad de su almacenamiento, por lo que los sistemas informáticos de las entidades aseguradoras tienen que ofrecer medidas de seguridad y de control, tanto técnicas como jurídicas, que garanticen la confidencialidad de la información y la protección frente a los accesos no autorizados.

De ahí la importancia del desarrollo reglamentario de la LOPD y la especial dedicación que a él se presta en este trabajo.

Entre las medidas a utilizar las técnicas criptográficas que se aplican al documento en soporte electrónico lo hacen más seguro e inaccesible a su alteración en mayor medidas que los documentos en soporte papel.

Otra de las medidas que se pueden utilizar entre las partes es pactar con un tercero el archivo en soporte informático de las declaraciones que se desarrollen en vía electrónica y que integran el contrato electrónico, dejando constancia de la fecha y hora en que tuvieron lugar.

El tercero de confianza archivará las declaraciones por un período no inferior a cinco años, si bien su actuación en ningún caso podrá sustituir a la de los fedatarios públicos.

Todo lo dicho respecto a los documentos en soporte electrónico debe aplicarse a los documentos en soporte papel, que precisan medidas para garantizar la no modificación de contenidos (firma o marcas de control), si bien las diferentes formas de falsificación y alteración fraudulenta que existen hasta el momento revisten un perfeccionamiento elevado.

3. LA FIRMA ELECTRÓNICA

En este apartado se analiza en profundidad la firma electrónica como medio de prueba electrónica, completando, de este modo, su función de garante de la identidad de las partes, al que se ha hecho referencia en el Capítulo IV de este trabajo.

Una firma electrónica es un conjunto de datos electrónicos utilizados como medio para vincular al autor del documento o autenticar su contenido. Sin embargo, esta definición resulta insuficiente puesto que incluiría técnicas tan poco seguras como la firma manual digitalizada.

El Real Decreto-ley 14/99, de firma electrónica, completa esta definición (art. 2, *b)* introduciendo un nuevo concepto: el de *firma electrónica avanzada,* que define como aquella firma electrónica que permite identificar al signatario y que se crea por medios que éste conserva bajo su exclusivo control, de forma que esté vinculada sólo a él, lo que le permite detectar cualquier modificación posterior realizada por terceros.

De esta definición se extrae que los requisitos exigidos a una firma electrónica para que resulte más segura son de dos tipos: requisitos de autenticación del autor y requisitos de integridad del documento. El primero de los requisitos se consigue con la triple exigencia de: identificación del signatario, creación de firma bajo su exclusivo control y vinculación única al autor. El requisito de la integridad se recoge en la última parte de la definición que establece que la vinculación a los datos haga posible detectar cualquier modificación de los mismos.

Con esta distinción, la ley española, siguiendo el parámetro comunitario, ha creado diferentes tipos de firmas electrónicas, en función del nivel de seguridad que ofrecen, o dicho de otro modo, en función de su calidad, lo que, sin duda, es importante a efectos de un posterior reconocimiento legal de las mismas (el art. 3 de la ley sólo reconoce efectos jurídicos a la firma electrónica avanzada).

La definición de firma electrónica avanzada coincide con una clase particular de firma electrónica como es la *firma digital*, que se crea utilizando una tecnología específica: la criptografía asimétrica o de clave pública. Actualmente las firmas digitales son las únicas firmas electrónicas seguras. El hecho de que la ley española no se refiera directamente a ella se debe al interés por abarcar todas las firmas electrónicas posibles, dejando abiertas las puertas a nuevos desarrollos tecnológicos aún por crear.

3.1. Clases de firma electrónica

La firma electrónica sustituye, como hemos visto, a la firma manuscrita en las comunicaciones electrónicas. La identificación de la firma manuscrita se realizaba y se realiza mediante la simple comprobación de la autenticidad de la misma, puesto que se considera que cada persona tiene su propia firma diferente a la de los demás, única y difícil de reproducir, y cuyas tres funciones principales son:

a) Identificar al autor y asociar a esa persona con el contenido del documento.
b) Declarar que se está conforme con el contenido.
c) Probar que el documento es auténtico y no ha sido alterado, para lo que se utilizan, además, técnicas complementarias como el sellado o la certificación del documento.

Estas funciones también se pueden cumplir utilizando la firma electrónica e incluso aparecen otras nuevas como: la integridad, la confidencialidad y el no rechazo del documento.

En cuanto a la forma, en la firma manuscrita se puede utilizar el nombre completo del autor, iniciales, seudónimo, sello, rúbrica o simple raya cruzada, puesto que lo importante no es el símbolo sino la intención del firmante de responsabilizarse del contenido del documento. No hay normas legales que se refieran a cómo ha de firmarse, incluso nuestro derecho reconoce la facultad de los contratantes de definir el signo que van a utilizar para sus relaciones. En cambio, en la firma electrónica, y concretamente en la firma digital, los requisitos de forma son muy específicos, dependiendo de ello la eficacia jurídica de la firma.

Utilizando el criterio de la forma se puede distinguir entre los siguientes tipos de firmas electrónicas:

A. De tecnología indefinida

Son aquellas que no ofrecen garantías ni sobre la autenticidad de la firma ni sobre la integridad del documento al que aparecen anexadas. Reciben el nombre de *firma manual digitalizada.* Esta técnica consiste en insertar la imagen leída con un escáner de la firma manuscrita (nombre o símbolo que lo identifique) del autor al final del documento electrónico.

Esta firma se caracteriza por su escasa seguridad y valor probatorio.

B. De tecnología definida

Esta tecnología es la criptográfica que se aplica tanto para crear y verificar firmas electrónicas como para asegurar la integridad y confidencialidad de los documentos. Consiste en transformar los datos con el fin de hacerlos indescifrables para aquel que no es el receptor autorizado. Actualmente existen dos sistemas de encriptación de firmas electrónica:

- *Firma en forma digital de clave simétrica*: el autor de la firma y el receptor del documento electrónico utilizan la misma clave para cifrar y descifrar el mensaje.

- Firma *en forma digital de clave asimétrica* (o *firma digital* propiamente dicha): es la técnica más utilizada y segura. Usa un algoritmo que crea dos claves diferentes y relacionadas: una pública, que se utiliza para cifrar la firma, y otra privada para descifrarla y verificarla, de manera que sólo el verdadero destinatario podrá comprobar la firma del emisor del documento.

3.2. La regulación legal de la firma electrónica

Los antecedentes españoles del Real Decreto-ley 14/99 se encuentran, principalmente en el ámbito de las Administraciones Públicas. En efecto, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se refiere (art. 45) a la apertura de la Administración hacia la tecnología. En desarrollo de este precepto, se aprueba el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de la tecnología por parte de la Administración General del Estado.

El Real Decreto-ley sobre firma electrónica es de aplicación en todo el territorio español y regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación de servicios de certificación, si bien la ley hace dos precisiones:

1. Sus disposiciones no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos.

2. Las previsiones sobre la prestación de servicios de certificación no sustituyen a las que corresponde realizar a los fedatarios públicos (notarios y corredores de comercio) cuya función es distinta (examen de la capacidad de las partes, asesoramiento legal, actuación en declaraciones unilaterales de voluntad y bilaterales, como los contratos…). Existen intentos de crear la figura del cibernotario, sin embargo, la distinta naturaleza de la función notarial en los sistemas latinos y anglosajones lo han impedido hasta el momento.

En relación a los elementos de creación y verificación de firma electrónica, la Ley española ha incorporado en este punto la previsiones de la Directiva comunitaria sobre firma electrónica, y así, se refiere a los siguientes elementos:

1. Datos de creación de firma. Son aquellos datos (códigos o claves criptográficas privadas) que el signatario utiliza para crear la firma.
2. Datos de verificación de firma. Son aquellos datos (códigos o claves criptográficas públicas) que se utilizan para comprobar la identidad del firmante.

3. Dispositivo de creación y verificación de firma. Elementos informáticos (programas o aparatos informáticos) que sirven para aplicar los datos de creación y verificación de firma.

La Ley exige para los dispositivos de creación de firma el cumplimiento de ciertos requisitos de calidad, lo que es trascendental a la hora de reconocer efectos jurídicos a esa firma; sin embargo, como veremos a continuación, se confunde el término dispositivo con el de datos, y de la lectura del articulado se desprende que los requisitos hacen alusión más a la seguridad de los datos (tres primeros apartados) en la creación de firma electrónica que a los dispositivos (último apartado).

De este modo los requisitos necesarios son:

a. Asegurar que los datos utilizados para la creación de la firma puedan producirse sólo una vez y garantizar, razonablemente, su secreto.
b. Seguridad razonable de que los datos utilizados para la generación de firma no pueden obtenerse por deducción y que la firma está protegida contra la falsificación mediante la tecnología existente.
c. Protección fiable por el signatario de los datos de creación de firma contra la utilización por otros.
d. El dispositivo seguro de creación de firma no debe alterar los datos o el documento ni impedir que éstos se muestren al signatario durante del proceso de firma.

En cuanto a las normas técnicas de calidad deben publicarse en el DOCE y en el BOE.

Por lo que se refiere a los efectos jurídicos de la firma electrónica la ley española acoge una regla general y otra especial para el reconocimiento de efectos jurídicos a la firma electrónica y su equiparación con la firma manuscrita.

La regla general reconoce efectos jurídicos a cualquier firma electrónica y prohíbe su exclusión como prueba en juicio por el mero hecho de presentarse en forma electrónica. Esto quiere decir que se debe respetar la libertad de las partes, tal y como establece el Código Civil, en las firmas de este carácter que se utilicen exclusivamente en relaciones basadas en acuerdos voluntarios de Derecho privado.

La regla especial exige una serie de requisitos añadidos para el reconocimiento de efectos jurídicos a la firma electrónica avanzada (firma digital). En este caso, dicha firma debe:

a) estar basada en un certificado reconocido (concepto que estudiaremos en el siguiente tema),
b) haber sido producida por un dispositivo seguro de creación de firma.

El problema que plantea la regla especial es la demostración de esos requisitos puesto que serán necesarios complejos informes técnicos, y aún así puede resultar difícil la prueba.

Para eliminar el escollo de la acreditación del cumplimiento de esos requisitos la Ley introduce una presunción reconociendo que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados, cuando el certificado reconocido en que se basa haya sido emitido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma se encuentre certificado. No obstante, aunque en un principio parece resuelto el problema la realidad es muy distinta puesto que tanto el concepto de servicios de certificación acreditados como el de dispositivo seguro de creación de firma deben desarrollarse por Real Decreto.

A pesar de que la Ley de firma electrónica apuesta por la seguridad de las comunicaciones al regular sistemas que permiten garantizar la autenticidad de la firma electrónica y la integridad de los documentos electrónicos; sin embargo, no impone ninguna exigencia para el reconocimiento de efectos legales y para su admisión como prueba en juicio de las firmas electrónicas menos seguras (como la firma manual digitalizada) y sí a las calificadas hoy por hoy como más seguras: las firmas digitales.

Por tanto, parece poder concluirse que no cumple con su objetivo de garantizar la validez de los efectos jurídicos de la firma electrónica en general, puesto que, en último caso, queda a la libre decisión de los jueces la aceptación o no como prueba en juicio de las firmas electrónicas menos seguras y a la aprobación de una norma de desarrollo.

Por su parte, la Ley 59/2003, de 19 de diciembre, de firma electrónica introduce como novedad la regulación del documento nacional de identidad electrónico y lo considera como un certificado electrónico reconocido con vocación de generalizar el uso de instrumentos seguros de comunicación electrónica con el mismo nivel de integridad y autenticidad que las que hasta el momento se reconocen a las comunicaciones por medios físicos.

La LFE fija el marco normativo del nuevo DNI electrónico y destaca como características del mismo: la acreditación de la identidad del titular en cualquier procedimiento administrativo y la posibilidad de firmar electrónicamente los documentos.

En este sentido, el art. 15.2 LFE expone que: Todas las personas físicas o jurídicas públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónicos en él incluidos. La importancia de esta novedad hace necesario dedicar un apartado diferente a su estudio.

4. EL DNI ELECTRÓNICO

Regulación legal

La sociedad de la información exige la generalización de mecanismos que refuercen la confianza de los ciudadanos en las comunicaciones electrónicas. En respuesta a esta necesidad la UE ha aprobado varias Directivas y en España la Ley de Firma Electrónica y el Real Decreto sobre el Documento Electrónico, RD 1553/2005, de 23 de diciembre, regula la expedición del documento nacional de identidad (BOE, nº 307, de 24 de diciembre de 2005) y desarrolla en este punto la Ley 59/2003, de 19 de diciembre de Firma Electrónica.

Con ello se están creando nuevos instrumentos que acreditan la identidad de las partes que intervienen en la comunicación y se asegura tanto la procedencia como la integridad de los mensajes, lo que constituye una de las grandes preocupaciones de la contratación de seguros en Internet para las compañías aseguradoras.

Las particularidades del DNI electrónico se recogen el Real Decreto 1553/2005, de 23 de diciembre, y adapta el tradicional documento de identidad a la nueva sociedad interconectada con el fin de poder realizar gestiones telemáticas asegurando la identidad de los participantes. Para su estudio vamos a apoyarnos también en la Guía de Referencia Básica del DNI electrónico, de la Comisión Técnica de Apoyo a la Implantación en su versión de 2007.

La identidad personal adquiere, por tanto, una nueva dimensión cuando trata de utilizarse en contextos no presenciales y, a pesar de su carácter físico, lo que se persigue es fijar mecanismos y procedimientos electrónicos para verificar esos nuevos entornos. Curiosamente una de las funciones que el DNI electrónico está llamada a cumplir es la de crear confianza en el ciudadano y dinamizar la Sociedad de la Información.

En España la utilización del DNI está presente en la mayoría de las relaciones comerciales y administrativas y es el único que se utiliza con carácter generalizado en todo el territorio nacional y de uso obligado para la expedición de documentos como el pasaporte, el NIF, el permiso de conducir, la tarjeta de la Seguridad Social...

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica, se refiere por primera vez al DNIe atribuyéndole nuevos efectos y utilidades. Se crea así un documento que certifica la identidad del ciudadano no sólo en el mundo físico sino también en las transacciones telemáticas, lo que permite firmar todo tipo de documentos electrónicos. De este modo, la firma electrónica que

se efectúe mediante el DNI electrónico tendrá efectos equivalentes a la firma manuscrita.

Este documento es aceptado por todas las Administraciones Pública y Entidades de Derecho Público dependientes o vinculadas de algún modo a las mismas. Como ejemplo puede hacerse alusión a la presentación de la Declaración de la renta, solicitud de empadronamiento, reclamación del derecho de pensión o alta en el registro de nacimientos.

Descripción del DNIe

El DNIe contiene información del ciudadano, a través de certificados relativos a la autenticación y firma, así como claves primadas asociadas, que se generan e introducen en el proceso de expedición del documento.

Mediante el certificado de autenticación el titular del documento podrá certificar su identidad frente a terceros. Además, la firma electrónica avanzada que incorpora el DNIe permitirá realizar y firmar compromisos de manera electrónica, utilizando los instrumentos de firma incorporados en él.

En concreto la firma electrónica avanzada permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados y que se crea por medios que el titular mantiene bajo su control. El funcionamiento de esta firma, basado en clave pública, se desarrolla de la siguiente manera:

- Cada parte tiene un par de claves. Una se utiliza para cifrar y la otra para descifrar.

- Cada parte mantiene una de las claves en secreto (clave privada) y pone a disposición la otra (clave pública). A la hora de emitir el mensaje se genera un resumen del mensaje (“hash”) formado por un conjunto de datos fijos que no varía en función del tamaño original.

- El emisor cifra ese resumen con la clave privada y lo envía.

- El receptor descifra el mensaje utilizando la clave pública del emisor obteniendo de este modo el resumen que creó el emisor.

Si ambos resúmenes coinciden se valida la firma puesto que quedan verificados los requisitos de autenticidad e integridad, además del no repudio, porque el emisor no puede negar que ha realizado el envío puesto que el mensaje lleva su firma.

En el anverso de la tarjeta aparecen los apellidos del titular, su nombre, sexo, nacionalidad, fecha de nacimiento, número de la tarjeta (IDESP) y fecha de fin de la validez.

Fuente: Ministerio del Interior

En el reverso de la tarjeta aparece el lugar de nacimiento, la provincia y el país, el nombre de los padres, domicilio, lugar del domicilio, provincia y país del domicilio, número de la oficina que expide el DNIe e información para lectura mecanizada de datos según la normativa OACI para documentos de viaje.

Fuente: Ministerio del Interior

El DNIe no contiene, por tanto ningún dato de tipo sanitario, fiscal o de tráfico.

El sector asegurador cuenta, a partir de ahora, con un instrumento extraordinario para desarrollar el mercado de la contratación de seguros vía telemática. Para ello es necesario que utilicen servicios basados en la identificación y en la firma electrónica, dinamizando así las relaciones con sus clientes, garantizando la máxima seguridad a sus clientes y asegurándose la identidad de los mismos.

De este modo, adquiere gran importancia el apartado 5 del artículo 1 del Real Decreto 1553/2005, respecto a la firma electrónica realizada a través del DNIe dado que los datos consignados en forma electrónica tendrán el mismo valor que la firma manuscrita en papel.

No cabe duda de la importancia de este precepto dado que se trata de un documento socialmente aceptado para la identificación y acreditación en múltiples actividades con repercusión jurídica.

Los certificados electrónicos en el DNIe

Junto a la utilización de la firma electrónica avanzada para identificar al firmante y detectar cualquier modificación posterior a la firma, otra de las ventajas que presenta el nuevo DNIe es el de su utilización en los certificados electrónicos, de manera que los prestadores de servicios de certificación que utilizan las firma electrónica avanzada identifican de este modo a cada usuario con la firma garantizando su identidad en el ámbito telemático.

En la relaciones entre ciudadanos y de estos con empresas, el nuevo DNI permite garantizar tanto la identidad de la persona que realiza la gestión como a integridad del contenido del mensaje se envía, lo que permitirá a sus titulares consultar datos de carácter personal, acceder a diferentes servicios públicos o realizar determinados trámites.

Al identificar a las partes que se conectan telemáticamente permite garantizar el máximo grado de confidencialidad y seguridad en la utilización de Internet.

El chip de la tarjeta contiene los siguientes certificados electrónicos:

1. Certificado de componente. Este certificado tiene por objeto autenticar el DNI electrónico mediante un protocolo de autenticación mutua que se define en CWA 14890.

   A través de este protocolo se crea un canal de cifrado y autenticado entre la tarjeta y los drivers. Este certificado no es accesible directamente a través de los interfaces estándar como pueden ser PKCS11 o CSP.

2. Certificado de Autenticación (Digital Signature). Este certificado garantiza electrónicamente la identidad del sujeto que va a realizar la transacción telemática. De esta manera se asegura que la comunicación electrónica se realiza con la persona que dice que es con lo que se acreditará su identidad puesto que cuenta con el certificado de identidad y con la clave privada asociada a la misma.

   El uso principal de este certificado está pensado para crear mensajes de confirmación de identidad y de acceso seguro a sistemas informáticos, lo que, a su vez, exigirá articular canales privados y confidenciales entre los prestadores de servicios y el sector asegurador.

   También puede utilizarse este certificado para garantizar un registro que facilite la expedición de certificados por parte de las entidades privadas, sin que ello lleve aparejado una gran inversión para su puesta en marcha y mantenimiento de la infraestructura de registro.

   Por el contrario el certificado de autenticación no está pensado para actuaciones que requieran no repudio de origen, por lo que los terceros aceptantes y los prestadores de servicios no tendrán una garantía del compromiso del titular del DNI con el contenido firmado.

3. Certificado de firma. Con este certificado firmaremos los documentos garantizando la integridad de los mismos y el no repudio de origen.

   Es un certificado del tipo X509v3 estándar que tiene activado el bit de no repudio y asociado a una clave pública y otra privada generadas en el interior del chip del DNI. Se expide como certificado reconocido y se crea en un dispositivo seguro de creación de firma, lo que permite su equiparación a la firma manuscrita al ser creado bajo los requisitos de firma electrónica avanzada que exige tanto la Ley 59/2003, de firma electrónica, como la Directiva 1999/93/CE, por la que se establece el marco comunitario para la firma electrónica).

La utilización del DNIe está prevista, por tanto, como medio de autenticación de identidad, dado que el titular se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo; de firma de documentos, pudiendo de esta forma demostrarse la identidad del firmante sin que éste pueda repudiarlo y de certificación de la integridad del mismo; esto es, que el documento no ha sido alterado a lo largo de la comunicación una vez que ha sido enviado.

Imaginemos un contexto en el que un sujeto sentado ante su ordenador esté interesado en conocer los productos que ofrece una compañía aseguradora para contratar un seguro de vida.

Lo más probable es que nuestro sujeto buscase, en primer lugar, las compañías que ofrecen ese servicio vía Internet. Lo que más le atraería, al margen de posibles recomendaciones o confianza en una compañía u otra, sería la facilidad en el manejo de la página.
Una vez seleccionada la compañía, el siguiente paso sería acceder a la información sobre el producto y, en tercer lugar, iniciar los trámites telemáticos para su contratación.

A partir de ese momento entraría en juego el DNIe constituyendo una herramienta capital para la captación final del cliente y para su fidelización puesto que deberá cumplimentar los trámites que requieren su consentimiento explícito y la garantía de su identidad.

En este supuesto deberían utilizarse dos tipos de certificados electrónicos por parte del cliente:

- *Digital Signature* (Certificado de Autenticación). Con este certificado se busca únicamente identificar al cliente sin que ello le vincule de ninguna manera a la suscripción del contrato y se utiliza exclusivamente para abrir canales privados y de carácter confidencial con la empresa prestadora del servicio.

  De esta manera se cierra el tunel SSL[150] a través del certificado del ciudadano/cliente y el del prestador de servicios.

- *Non repudiation* (Certificado de firma). Permite al ciudadano/cliente firmar trámites o documentos. De este modo se puede sustituir la firma manuscrita por la electrónica en las relaciones del titular de la tarjeta con

[150] La tecnología Secure Socket Layer salvaguarda los accesos a la información que circula por los protocolos de Internet HTTP, SMTP, FTP, etc, cifrando los datos de forma simétrica, de manera que el acceso a estos datos sólo será posible si se tiene la clave correcta.
Hasta la aparición masiva de *Works, spyware polimórfico* y software "mutante" con capacidad para introducirse por cualquier puerto abierto, se abrió una nueva etapa en la que filtrar sólo en Capa 3 no resultaba seguro (la Capa 3 responde a la capa de red en la que se produce el direccionamiento de la información).
Las respuestas tecnológicas han ido evolucionando en paralelo, en ocasiones de manera preactiva y en la mayoría de los casos de manera reactiva.
El protocolo funciona dentro de un tunel VPN (virtual private network). Entre las compañías que están desarrollando está tecnología Microsoft ha incorporado en su nuevo sistema operativo Vista el protocolo SSTP (Secure Socket Tunneling Protocol) que permite al cliente acceder a las redes mediante una VPN desde cualquier punto de Internet. Esta tecnología crea un tunel VPN sobre Secure-HTTO, con lo que se solventan los problemas asociados a las conexiones VPN basadas en Pts (point-to-point tunneling protocol) o en L2TP (layer 2 tunneling protocol).
Con todo, no han tardado en saltar las alarmas puesto que el nuevo sistema operativo da muchos más problemas que Windows XP, no sólo en lo que se refiere al funcionamiento ordinario del pc sino en cuanto a las comunicaciones a través de la Red, dado que el sistema ha multiplicado los mecanismos de seguridad en detrimento de la agilidad de su uso, por lo que el usuario debe confirmar cada paso que da en la Red, ralentizándose de este modo la navegación.

terceros (arts. 3.4 y 15.2 de la Ley 59/2003, de firma electrónica). El certificado responde a los parámetros del ETSI (European Telecommunications Standards Institute, Instituto Europeo de Normas de Telecomunicaciones), organización de estandarización de la industria de las telecomunicaciones de Europa (fabricantes de equipos y operadores de redes), que cuenta entre sus éxitos con el de estandarizar el sistema de telefonía móvil GSM.

El DNIe funcionaría previo establecimiento de una conexión privada con la entidad aseguradora. El canal quedaría autenticado en los dos extremos de la conexión utilizando certificados que garanticen la identidad de las partes, conforme al siguiente protocolo:

1. El ciudadano/cliente realiza una petición de conexión segura autenticada.
2. La entidad crea un mensaje autenticado y lo envía al cliente.
3. El cliente verifica la validez del certificado de servidor que se le ofrece.
4. A continuación se genera la clave de sesión y se cifra la misma con la clave pública de la empresa aseguradora.
5. Se procede a la construcción del mensaje de intercambio de claves.
6. El cliente introduce el DNI electrónico en el lector y, con el certificado electrónico de autenticación, valida el mensaje de intercambio de claves.
7. Se crea el canal privado.
8. La entidad aseguradora verifica el mensaje de establecimiento de sesión.
9. La aseguradora comprueba con la correspondiente Autoridad de Validación el estado de validez del Certificado de Autenticación del ciudadano/cliente.
10. Se establece un canal seguro, cerrándose el túnel SSL.

Todo el proceso de autenticación para generar un canal seguro precisa del uso de un certificado expedido por organismo público o entidad privada. Este certificado está asociado al servidor de la aseguradora y garantiza que el ciudadano se está conectando a dicho organismo y no a otro.

Este certificado no se podrá emitir ni por la Dirección General de la Policía ni por el Ministerio del Interior, sino que tendrá que ser garantizada por una Autoridad de Certificación distinta a las citadas en el marco de las obligaciones exigidas a los prestadores de servicios de certificación y en la Ley de Firma Electrónica.

Por lo tanto el proceso de autenticación requiere el uso de un certificado de Organismo público o entidad privada y el certificado de autenticación del ciudadano.

El ciudadano para autenticarse frente al Organismo público o la entidad privada cuenta con un certificado con capacidad de autenticación de manera que la entidad aseguradora podrá determinar la identidad del cliente para

ofrecerle un servicio personalizado. La veracidad de este certificado se acredita por la Dirección General de la Policía.

Por lo que se refiere a las partes involucradas en la fijación del canal privado, se distingue:

a) Cliente: persona física titular del DNI electrónico. Este dispositivo de firma y autenticación segura emitido por la Institución del DN y que contiene tanto el conjunto de claves privadas del ciudadano, de certificados y los elementos de seguridad para garantizar la integridad del documento frente a alteraciones.
b) Entidad proveedora de servicios.
c) Autoridad de Validación: informa sobre el estado de validez de los certificados del ciudadano.
d) La entidad aseguradora.

La cuestión a continuación es por qué se ha elegido el protocolo descrito anteriormente para crear una sesión SSL. La respuesta es que la mayoría de los servidores y clientes disponen de esta capacidad. Mediante este protocolo se pueden establecer dos tipos de canales privados:

1. Autenticación del Servidor. En este caso, sólo el servidor necesita tener un certificado, por lo que la identidad del cliente será anónima.
2. Autenticación Servidor-Cliente. Se exige que tanto el proveedor de servicios se autentique frente al cliente como que el cliente se autentique frente al servidor.

La segunda opción sería la más aconsejable dado que de esta manera ambas partes se aseguran la voluntad de compromiso en la relación. La diferencia entre una y otra estriba en que si el proveedor de servicios tiene garantía de la identidad del cliente podrá ofrecerle una información lo más ajustada posible a sus necesidades dado que se podrá utilizar el DNI electrónico para establecer reglas de acceso a la información en base a la identidad del cliente.

Otro de los aspectos que interesa señalar del uso del DNI electrónico es el de la firma de trámites. En este sentido, el procedimiento sería el siguiente:

1. La entidad certificadora enviaría el formulario para realizar el trámite.
2. El cliente cumplimenta el formulario y lo reenvía. Conviene recordar que para poder llevar a cabo todo el proceso de firma se debe contar con la aplicación informática correspondiente.[151]
3. La entidad certificadora reconstruye el formulario en formato de texto lo vuelve a enviar al cliente.

[151] En este sentido, actualmente existen dos alternativas tecnológicas de funcionalidad de firma electrónica: la funcionalidad de firma a través de la aplicación informática previamente instalada en nuestro equipo informático; o bien, que la funcionalidad esté incluida en el proceso general del prestador de servicios telemáticos.

4. El cliente verifica que el trámite se corresponde exactamente con el cumplimentado.
5. Se solicita al cliente la firma electrónica del formulario.
6. El cliente introduce su clave de acceso personal (PIN) para el certificado de Firma.
7. El DNI electrónico firma electrónicamente el formulario.
8. El ciudadano envía el formulado firmado a la entidad de certificación.
9. La entidad certificadora verifica la validez de la firma, comprobando la integridad del documento.
10. La entidad certificadora comprueba en la autoridad de validación el estado de validez del certificado de firma del cliente.

El trámite se completa con la entrega del formulario firmado con acuse de recibo por parte de la entidad receptora a la aseguradora. A pesar de que en este último paso no interviene el DNI electrónico es recomendable para reforzar la confianza del cliente sobre la correcta realización del trámite por parte de la entidad certificadora, debiendo incluirse como una herramienta más de las buenas prácticas del prestador del servicio. Para ello el recibo debe ir firmado y sellado por una Autoridad de Sellos de Tiempo (Tercera parte de confianza) que acredita el momento exacto en el que el trámite se aceptó por el prestador de servicios (entidad aseguradora) y que debe ser una entidad diferente a ese prestador y reconocida por la legislación española.

4.4. La Autoridad de Validación

Esta Autoridad se encarga de informar sobre el grado de vigencia de los certificados electrónicos[152] que hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

En la estructura utilizada para crear el DNI electrónico se han asignado las funciones de validación y de certificación a órganos diferentes con el fin de diferenciar la comprobación de la vigencia de un certificado electrónico con los datos de la identidad de su titular, en aras a la transparencia del sistema. De este modo, el Ministerio del Interior, y concretamente la Dirección General de la Policía, no tiene acceso a los datos de las comunicaciones que se realicen con los certificados que ella emite y, por su parte, las Autoridades de Validación no pueden acceder a la identidad de los titulares de los certificados electrónicos que pasan por sus manos.

Están acreditados como prestadores de Servicios de Validación para el DNI electrónico: la Fábrica Nacional de Moneda y Timbre y el Ministerio para las Administraciones Públicas. La primera presta sus servicios a ciudadanos, empresas y Administración Pública, mientras que el segundo limita sus servicios al conjunto de las Administraciones Públicas. Junto a ellas, se prevé

[152] La información sobre los certificados electrónicos no vigentes se almacena en unas listas denominadas de revocación de certificados que se conocen con el acrónimo CRL.

que la Entidad Pública Empresarial "Red.es" pueda prestar también en un futuro próximo este servicio. La validación se realiza on-line en base al protocolo (OCSP- Online Certificate Status Protocol) y está disponible de forma ininterrumpida todos los días del año.

4.5. Seguridad

Otro aspecto importante en todo este proceso es el de la seguridad técnica. El DNI electrónico incorpora como funciones de seguridad: la autenticación, la securización de mensajes, el desbloqueo y cambio de PIN, la función criptográfica, el intercambio de claves y el cifrado.

La autenticación se puede realizar de diversas maneras. Se puede centrar la atención en la autenticación de usuario, en la autenticación de la aplicación o en ambas. En el primer caso, bien a través de la autenticación del usuario mediante su PIN, bien a través de datos biométricos (aunque esta opción sólo puede utilizarse desde accesos que cuenten con un dispositivo lector de huellas).

El fin de la autenticación de la aplicación es que la entidad pueda demostrar que conoce el nombre y valor de un código secreto, para lo que se utiliza el protocolo desafío-respuesta[153]. La autenticación mutua propicia que cada parte de la relación confíe en la otra al tener que presentar ambos certificados y su verificación.

El DNI electrónico permite también crear un canal seguro entre el Terminal y la tarjeta para reforzar la seguridad de los mensajes transmitidos (securización de mensajes). Por otro lado, se permite el cambio de PIN en terminales específicamente habilitadas para ello (autorizadas por la Dirección general de la Policía) con objeto de garantizar los máximos niveles de confidencialidad y seguridad.

Para funcionalidad criptográfica se utilizan las claves RSA, el lenguaje hash y la firma electrónica. .En cuanto al intercambio de claves se utiliza para compartir claves simétricas o de sesión entre dos entidades.

4.6. Aplicación de firma

Como se viene apuntando una de las principales ventajas del DNI electrónico es la posibilidad de realizar la firma electrónica. En este sentido, el Ministerio del Interior ha desarrollado un manual de uso para su aplicación donde se describe con claridad su manejo.

[153] La aplicación pide un desafío a la tarjeta. A continuación la aplicación usa un algoritmo para ese desafío junto con el correspondiente código secreto y el nombre de la clave. La tarjeta realiza la misma operación y compara el resultado con los datos transmitidos por la aplicación. Si coinciden lo valida para posteriores operaciones.

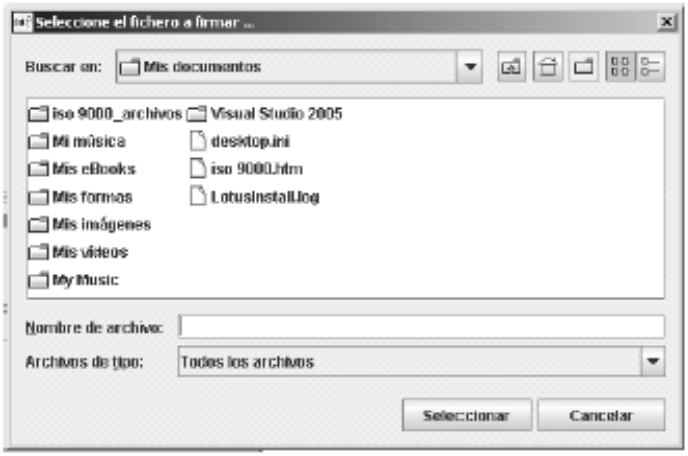
La aplicación facilita las siguientes operaciones:

- Firma de un archivo, generando un nuevo fichero de firma.
- Firma de documento adjunto, se firma el archivo generando un nuevo fichero de firma que contiene los datos firmados.
- Verificación off-line para comprobar un archivo firmado con documento adjunto. En este caso sólo se comprueba: si el certificado con el que se ha firmado está caducado o no, si el fichero firmado ha sufrido alguna modificación posterior o si el certificado de firma corresponde a una entidad de certificación de confianza.
- Verificación off-line sin documento adjunto. Se comprueba el archivo firmado. En este supuesto se verifica si el certificado está o no caducado y si ha sido modificado el fichero firmado.
- Verificación on-line. Tanto si se trata de comprobar un archivo firmado con documento adjunto como sin él, la verificación se hace off-line y la comprobación del estado del certificado vía OCSP.

El usuario es el responsable final de utilizar la firma por lo que en la creación de la misma debe cumplir los requisitos exigidos por la Ley 59/2003 de firma electrónica y la Directiva comunitaria de firma electrónica (Directiva 1999/93/CE) a fin de que sea reconocida como tal.

La firma de un documento se ha articulado para que resulte atractivo y ágil su manejo, impulsando su utilización. De este modo, la interfaz general de usuario se describe de la siguiente manera:

Esta pantalla (interfaz) permite visualizar las diferentes opciones (funcionalidades) que ofrece la aplicación (firmar, verificar, configurar y ayuda). Si solicitamos firma, se despliega otra pantalla para que seleccionemos el documento que se quiere firmar.



Una vez seleccionado el documento se nos preguntará nuestro código de acceso (PIN), tecleado el código correcto se pregunta al usuario si desea incluir o no lo firmado dentro de la firma que se ha creado. En caso afirmativo, se genera un archivo que contiene lo firmado y la firma propiamente dicha de la siguiente manera:

A continuación se nos pide autorización para proceder a realizar la operación y se nos informa sobre su resultado:

Por último se nos pide el nombre del fichero en el que queremos que se almacene el resultado.

La segunda fase es la de verificación del fichero firmado. El usuario selecciona de nuevo el fichero que ha firmado. En esta fase no se solicita el PIN del DNI electrónico puesto que para la verificación se utiliza la clave pública del firmante del documento. Tras seleccionar el fichero se nos muestra el resultado de la operación.

4.7. Conclusiones

Visto todo lo anterior los efectos y utilidades del DNIe son:

1. Crear un documento que certifique la identidad del ciudadano con el mundo físico y permita transacciones telemáticas, posibilitando la firma de documentos electrónicos que tendrán efectos equivalentes a los de una firma manuscrita, siempre que se utilicen dispositivos seguros de creación de firma.
2. Reducción del tiempo para la obtención del DNIe, al tratarse de un solo acto administrativo.
3. Agilidad e interoperabilidad con los proyectos europeos de identificación digital.
4. Incrementar la confianza en las transacciones electrónicas.
5. Aceptación del DNIe por las Administraciones Públicas y entidades vinculadas o dependientes.
6. Validez de la utilidad informática asociada a la identificación electrónica de su titular, así como para realizar la firma electrónica, tendrá un período de validez único de 30 meses (art. 12.1 RD 1553/2005).

7. Certificado de autenticación.
8. Certificado de firma electrónica reconocida.

En este proceso, la firma electrónica del DNIe permite garantizar la identidad de la persona y la integridad del contenido del mensaje, con lo que el titular del mismo podrá realizar trámites o acceder a diferentes servicios públicos o privados, con un máximo grado de confidencialidad y seguridad en Internet al hacer posible la identificación de las partes que se conectan telemáticamente.

Por otro lado, la propia Ley 59/2003, de Firma Electrónica, en su artículo 16.2 se refiere al esfuerzo que debe hacer la Administración General del Estado para emplear sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el DNIe con los distintos dispositivos y productos de firma electrónica generalmente aceptados, hasta el punto de convertirse en uno de los principales proveedores de servicios que se podrán utilizar con el DNIe, lo cual agilizará los trámites con la Administración al dejar de ser necesaria la presencia física para garantizar la identidad.

Por lo que se refiere al sector privado en general y al sector asegurador, en particular, deberán desarrollar servicios basados en la identificación y firma electrónica que dinamicen las relaciones con sus clientes y los trámites burocráticos con la Administración. De ahí que, el DNIe deba percibirse como herramienta esencial en las relaciones comerciales del sector asegurador.

En suma, podemos decir que el DNI electrónico facilitará las relaciones entre ciudadanos, agilizando además la de éstos con la Administración Pública. Al mismo tiempo, las ventajas también alcanzarán al sector asegurador en el sentido de reducir los tiempos de realización de trámites administrativos e incrementando la seguridad de las relaciones con sus clientes al garantizarse la identidad de los mismos lo que se traducirá en un incremento de la eficacia y efectividad en la prestación de servicios en el mercado asegurador.

Capítulo VII
RETOS JURÍDICOS DEL SECTOR ASEGURADOR EN INTERNET. CONCLUSIONES

1. LA IMPLANTACIÓN DE MEDIDAS TÉCNICAS Y JURÍDICAS EN EL SECTOR ASEGURADOR

La evolución de los sitios webs de las compañías aseguradoras ha sido continua en los últimos años, confirmándose la tendencia de la mayoría de las entidades a ofrecer un amplio espectro de "e-servicios" a sus clientes, proveedores y socios. De ahí que los retos jurídicos del sector deban estudiarse tomando como referencia la estrategia de presente y futuro, desarrollada y prevista por las aseguradoras.

El último barómetro del Centro de Investigaciones Sociológicas de abril de 2008 señala que el 75% de los españoles se sienten inseguros a la hora de comprar por Internet y el 71% está preocupado por el tratamiento que reciben sus datos personales, si bien, paradójicamente, el 56% pasa por alto la casilla en la que se incluye información sobre el uso que la empresa que solicita sus datos personales va a hacer de ellos.

Estos datos resultan, sin duda, inquietantes y reflejan el gran desconocimiento general del entorno de Internet y de sus mecanismos

La visión estratégica acerca del canal Internet y de sus posibilidades constituye uno de los aspectos a tener en cuenta en relación a la plena implantación en el sector.

En este sentido, factores como: la estrategia de comunicación, la captación de negocio, el desarrollo a medio plazo, el volumen de tráfico los servicios a futuro o la responsabilidad de la web, están muy presentes en la conceptualización del negocio.

De los datos del 2006 recogidos por el VII Informe del Sector Asegurador en Internet[154], debe destacarse el alto porcentaje de implantación de medidas de seguridad técnica y jurídica de las principales entidades aseguradoras de nuestro país, porcentaje que se aleja de otros servicios ofrecidos on-line y que demuestra, una vez más, en gran interés del sector por adecuar su actividad al marco de la ley y el gran esfuerzo inversor que se está realizando en este sentido.

[154] Informe Capgemini, publicado en Octubre de 2007.

Los datos más significativos de los servicios ofrecidos son:

1. Compra on-line. La compra on-line está presente en el 79% de las webs españolas.

2. E-claims. La gestión de las reclamaciones on-line o la posibilidad de gestionar las pólizas cuando el concepto "siniestro" no es aplicable, por ejemplo, en el caso de los seguros médicos, crece en su implantación y es uno de los aspectos mejor valorados siendo un servicio que ya ofrecen el 69% de las webs nacionales.

3. Servicio a mediadores. En la interacción de las entidades con sus profesionales, proveedores, socios, etc., Internet se presenta como una prioridad. De ahí que el 51% de las webs cuenten con este servicio, si bien este porcentaje es mayor si tenemos en cuenta de este servicio a través de intranets.

4. Servicios a dispositivos móviles. Se ha detectado una nueva tendencia en el uso de servicios a través de los dispositivos móviles para relacionarse con el cliente, socio o proveedor (mediadores, peritos…). De hecho el 28% de las webs analizadas utilizan servicios que se apoyan en estas tecnologías.

5. Accesibilidad. Comienza a abrirse paso la sensibilización de las entidades hacia las personas discapacitadas, de modo que el 12% de las webs aseguradoras dispone de secciones habilitadas para este sector de la población.

6. Idiomas. Todas las principales webs del sector ofrecen su información en español e inglés, si bien el 18% incorporan otros idiomas como el alemán, el portugués o el francés, aunque este porcentaje aumenta al 28% en el caso de la utilización de idiomas autonómicos.

7. Certificados de seguridad. La preocupación por garantizar la seguridad técnica y jurídica de las transacciones realizadas y los aspectos asociados a las certificaciones es continua y está presente en el 84% de las webs.

Desde el punto de vista estratégico, las webs no representan aún un canal relevante de captación de negocio y las previsiones a medio plazo no prevén una evolución importante en esta dirección.

Las entidades aseguradoras se dirigen más hacia las ofertas de valor añadido y a campañas de fidelización de que buscan que el cliente interaccione con la compañía a través de la web pero el canal básico de contratación en la mayoría de los casos sigue siendo el convencional a pesar del alto número de visitas a éstas.

Por tanto, se tiene una visión optimista de las actuales webs aseguradoras que son fáciles de usar e integradas con el resto de los canales de comunicación de las compañías.

Desde el punto de vista del negocio, el Informe de Capgemini destaca la escasa relevancia de los volúmenes de negocio captados en la red. En el 69% de los casos, estos valores no llegan al 3% del total de negocio captado por las compañías, si bien, otro 26% capta más de un 20% de su negocio en la red, por lo que no existe un término medio, aunque existe una leve tendencia a pensar que el volumen de negocio en la red se incrementará gradualmente.

Otro factor que permite evaluar el interés de las compañías aseguradoras en la red es el control de tráfico en la red. El 89% de las empresas incluidas en el Informe utilizan medios de control de tráfico, así como técnicas que permiten conocer el volumen de visitas.

Por lo que se refiere a los servicios ofrecidos on-line, la inmensa mayoría de las empresas aseguradoras considera que sus webs son principalmente un canal de comunicación de la imagen corporativa de la compañía (94,4%) y prestan mayor atención a la configuración de la web como canal de trabajo para la mediación (en un 77,8% de los casos) y los peritos (un 33,3%), por tanto tienen una orientación más profesional hacia el "business to business" (B2B) que hacia el consumidor final (B2C).

Los porcentajes de actuación on-line del consumidor final se reducen a un 33,3% para la posibilidad de contratación e incluso resultan más bajos los de tramitación de siniestros u otros servicios como asistencia, reparación, etc. (22,2%). La tendencia de futuro se dirige hacia una evolución de los servicios que ya se están ofreciendo, complementando la oferta en función de los resultados que se obtengan y consolidando el mayor aumento de servicios hacia mediadores y peritos.

Para los clientes finales la oferta de servicios aumentará en porcentaje de implantación pero seguirá basándose en la contratación y en la prestación de servicios de asistencia, comenzando a abrirse camino el uso de dispositivos móviles que por el momento sólo es tenido en cuenta por el 5,6% de las compañías.

En todo este proceso estratégico no puede olvidarse la importancia de una adecuada gestión de la web que normalmente afecta a varios departamentos de la compañía. Su actividad alcanza tanto a la gestión de los contenidos, como al mantenimiento de la infraestructura necesaria para su funcionamiento o para las tramitaciones de las transacciones comerciales. De ahí que se opte por la diversificación de responsabilidades, si bien el grueso de la misma recae en los departamentos que gestionan la imagen de la compañía, unas veces denominado marketing (7%) y otras comunicación corporativa (50%).

El departamento de tecnología es clave, lógicamente, para la gestión de la webs (27,8%) por lo que en más de la mitad de las empresas aseguradoras la responsabilidad se comparte por estos dos departamentos.

2. RETOS JURÍDICOS

Sobre la base de los resultados anteriores la seguridad jurídica del uso de las tecnologías de la información en el sector asegurador debe enmarcarse en la defensa de los derechos de los usuarios/clientes y en el cumplimiento de las obligaciones legales por parte de las compañías aseguradoras.

En este sentido, la protección jurídica se manifiesta reforzada en cuanto a la protección del individuo y deja en manos de la empresa la configuración de procedimientos de protección contra posibles fraudes, al margen de la protección conferida en el Código Civil y Mercantil.

Las recientes modificaciones introducidas por el Reglamento 1720/207, de 21 de diciembre, sin duda, ayudarán a garantizar la seguridad jurídica de las tecnologías de la Información en el sector, si bien la ampliación de la protección a los ficheros no automatizados añadirá dificultades a la hora de su aplicación.

Por otro lado, la variación de los niveles de seguridad y la exclusión del nivel alto de ficheros como los relacionados con las bajas laborales o los datos de discapacidad agilizará su uso y tratamiento. El Reglamento introduce un verdadero estatuto del encargado del tratamiento, incorporando un procedimiento voluntario para recabar el consentimiento.

El Título VII del Reglamento tiene especial importancia porque se refiere a las medidas de seguridad con la repercusión que ello tiene en la organización, gestión e inversión desde el momento que se traten datos personales. El Reglamento es particularmente riguroso en tres aspectos: en atribuir los niveles de seguridad, en la fijación de las medidas que corresponde adoptar en cada caso y en la revisión de las mismas cuando sea necesario. La época de bonanza económica comienza a retirarse por lo que las compañías de seguros que mayores garantías de protección ofrezcan conseguirán una mayor fidelización de clientes.

La información que manejan las aseguradoras tiene en muchos casos un carácter crítico dado que se trata de datos que tienen reconocido el máximo nivel de confidencialidad en la LOPD. De ahí que en los últimos años se hayan hecho verdaderos esfuerzos por acercar el entorno asegurador al de la protección de datos y claros ejemplos los encontramos en la normativa sectorial en la materia. Así, podemos hacer mención a la reciente puesta en marcha del Registro de Contratos de Seguro de Cobertura de Fallecimiento, o las referencias a la protección de datos del Texto Refundido de la Ley de

Ordenación y Supervisión de los Seguros Privados, así como de la Ley 26/2006 de Mediación de Seguros Privados.

Con la aprobación de la Ley 20/2005, de 14 de noviembre, sobre la creación del Registro de Contratos de Seguros de Cobertura de Fallecimiento, las compañías aseguradoras pasan a tener un nuevo papel como entidades informantes de los datos personales de los asegurados al fichero común. A partir de ahora, ya no son sólo responsables de su fichero de clientes, sino que se convierten en cedentes de los datos que se remiten al Registro de Contratos de Seguros de Cobertura de Fallecimiento.

El reto en este sentido es gestionar el volumen y la complejidad del trabajo que el funcionamiento de este Registro va a ocasionar y que parece apuntar la conveniencia de crear un nuevo fichero para el cumplimiento de esta función, incluido un fichero histórico.

El TRLOSSP parece haber solucionado el problema planteado por la Disposición Adicional Sexta de la LOPD en relación a la necesidad de recabar el consentimiento expreso para obtener los datos de salud. El Texto Refundido de la Ley de Ordenación y Supervisión de los Seguros Privados permite a las entidades aseguradoras crear ficheros comunes para la liquidación de siniestros y para la colaboración estadístico actuarial con la finalidad de permitir la tarificación y la selección de riesgos, así como para la elaboración de estudios de técnica aseguradora.

En cuanto al control de la actividad aseguradora por parte de la Administración General del Estado se permite la utilización de cualquier medio técnico, electrónico, informático y telemático para el desarrollo de su actividad en el marco de la LOPD, así como la emisión de documentos utilizando esas mismas técnicas.

Otro de los retos de futuro es la plena implantación de las nuevas tecnologías entre la Administración y las entidades aseguradoras mediante la tramitación de procedimientos electrónicos con soporte informático, garantizando la confidencialidad y la seguridad de los datos de carácter personal.

Por lo que se refiere la mediación del seguro privado, la Ley 26/2006, extiende a su ámbito la aplicación de la LOPD, con lo que se ha logrado clarificar aspectos esenciales relacionados con el tratamiento de datos personales en el sector asegurador, planteando dos claros retos a la mediación: la concienciación al sector de que se está ante un Derecho Fundamental y el Deber de Información. La asunción de ambos facilitará en gran medida las obligaciones derivadas de la LOPD.

Desde el punto de vista de la contratación on-line, la mayoría de las compañías aseguradoras continúan confiando en la conclusión del contrato por la vía tradicional, si bien aquéllas que operan on-line se enfrentan a partir

del 19 de abril de 2008 al reto de adaptar su operativa de trabajo a las novedades del Reglamento 1720/2007.

De este modo, en la contratación on-line se deberá tener en cuenta a partir de ahora:

1. Que el responsable del tratamiento debe solicitar el consentimiento del afectado durante el proceso de formación del contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, permitiendo, en todo caso, al interesado expresar su negativa al tratamiento o comunicación de datos.

2. Por lo que se refiere a los datos de salud se recomienda solicitar el consentimiento expreso por escrito del afectado, a pesar de que el Reglamento no especifique éste último carácter.

3. Existe un procedimiento voluntario de recogida de datos orientado a favorecer el consentimiento de forma tácita.

4. Se incluye una definición de lo que ha de entenderse por datos de carácter personal relacionados con la salud, que reproduce el artículo 45 del convenio 108 del Consejo de Europa de 1981, e incluye en su ámbito los referidos al porcentaje de discapacidad y a la información genética.

5. Los datos biométricos no aparecen recogidos en el nuevo Reglamento dentro de los datos de salud si bien una interpretación extensiva del concepto de dato personal como la acogida por la doctrina comunitaria incorpora a los mismos dentro de los de carácter persona con el objeto de proteger los derechos y libertades de los afectados, sin necesidad de que sea necesario por el momento una modificación de la norma en este sentido.

6. Se amplía el catálogo de excepciones del consentimiento no sólo a la autorización legal sino también a una norma de derecho comunitario, recordando la ausencia de consentimiento para realizar comunicaciones de datos incluso a través de medios electrónicos entre organismos, centros y servicios del Sistema Nacional de Salud.

7. En relación a la prestación de servicios, la regulación de las funciones del encargado del tratamiento debe figurar por escrito de la manera más concreta y delimitada posible y, en cualquier caso, queda prohibida la transmisión de datos personales a un tercero.

8. Se prohibe asimismo la subcontratación de servicios a un tercero salvo que este extremo esté expresamente previsto en el contrato de origen.

Otro de los aspectos que más preocupa al sector asegurador es la identidad de la otra parte de la comunicación. Hasta el momento las soluciones que existen junto con la aplicación de los diferentes niveles de seguridad son: la firma electrónica avanzada, la encriptación de documentos, los certificados electrónicos, el registro del usuario y el DNI electrónico.

Todas estas soluciones permiten garantizar la identidad de la persona y la integridad del contenido del mensaje con un máximo grado de confidencialidad y seguridad al hacer posible la identificación de las partes que se conectan telemáticamente.

El reto en este sentido para el sector asegurador es desarrollar servicios basados en la identificación y firma electrónica avanzada que dinamicen sus relaciones con los clientes y mediadores, reduciendo los tiempos de realización de trámites e incrementando la seguridad de las relaciones con sus clientes, contribuyendo a hacer disminuir los porcentajes de desconfianza a que nos referíamos al comenzar este apartado.

La seguridad jurídica absoluta es una utopía pero nuestro trabajo es demostrar que esta afirmación puede llegar a desmoronarse y prueba de ello son los indudables avances que se están acometiendo y que han sido analizados en estas líneas. El camino está marcado el siguiente paso es asfaltarlo y recorrerlo sin temor.

BIBLIOGRAFíA

LIBROS

Anuario de Derecho de las tecnologías de la Información y las Comunicaciones (TIC) 2006. DAVARA & DAVARA Asesores Jurídicos. Ed. Vodafone. Fundación España. 2007. Madrid.

Cibersociedad. Los retos sociales ante un nuevo mundo digital. JOYANES AGUILAR, L. McGraw-Hill, Madrid, 1997.

Comercio Electrónico, Firma Digital y Autoridades de Certificación. MARTÍNEZ NADAL, Apol-lonia Editorial Civitas. Colección: "Estudios de Derecho Mercantil". Madrid, 2006.

Derecho Privado de Internet. DE MIGUEL ASENSIO, Pedro A. Editorial Civitas. Madrid, 2000.

El Código y otras leyes del ciberespacio. LESSIG, L. Tauruses Digital. Madrid, 2001.

El derecho a la autodeterminación informativa. LUCAS MURILLO, Pablo Editorial Tecnos, Madrid, 1990.

El Mundo Digital. NEGROPONTE, N Ediciones B. Barcelona, 1996.

El poder de la Identidad, vol. 2 de La Era de la Información: Economía, Sociedad y Cultura. CASTELLS, M Alianza Editorial. Madrid, 1998, p. 286.

Estudio Práctico sobre la protección de datos de carácter personal. Coord. ALMUZARA, Cristina. Editorial Lex Nova. 2ª Edición, marzo 2007. Valladolid.

Factbook Comercio Electrónico. DAVARA & DAVARA Asesores Jurídicos. Aranzadi & Thomson. 2007. Navarra.

Factbook de las Tecnologías de la Información. CAPGEMINI. Aranzadi & Thomson. 2006. Navarra.

Factbook Protección de Datos Personales. ECIJA Abogados. Aranzadi & Thomson. 2003. Navarra.

La Galaxia de Internet. CASTELLS, M. Plaza & Janés Editores. Barcelona, 1ª edición, noviembre, 2001.

La Regulación de la Red. Poder y Derecho en Internet. MUÑOZ MACHADO, Santiago. Ed. Taurus, Madrid, 2000**.**

Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Comentario y textos. HEREDERO, Manuel. Editorial Tecnos. Madrid, 1996.

Los señores del aire: Telépolis y el tercer entorno. ECHEVARRÍA, Javier Editorial Destino. Madrid, 1999.

Nuevas tecnologías. Intimidad y Protección de Datos. TÉLLEZ AGUILERA, Abel. Estudio Sistemático de la Ley Orgánica 15/1999. Edisofer S.L. Madrid, 2001, p. 85 y ss.

Regulación Jurídica de los tratamientos de datos personales realizados por el sector privado en Internet. CORRIPIO GIL-DELGADO, Mª de los Reyes Agencia de Protección de Datos. Premio Protección de Datos Personales. IV Edición. Madrid, 2000.

Tratado de Derecho Informático. SUÑÉ LLINÁS, Emilio Vol. I. Servicio de Publicaciones, Facultad de Derecho. Universidad Complutense Madrid, 2ª Ed. Madrid, 2002, p. 424.

Tratamiento de Datos Especialmente Protegidos, en: Estudio Práctico sobre la Protección de Datos de Carácter Personal, ALMUZARA, C y otros. Editorial Lex Nova, Valladolid, 2007.

JORNADAS E INFORMES

Análisis de Diseño y Contenido de los Sitios Webs de las Aseguradoras. Comparativa Nacional e Internacional. 2006. ICEA.

Crecimiento del sector asegurador en Internet. Informe Consultora Tatum, marzo, 2007, disponible en la web de la Consultora.

*DNI electrónico, Guía de Referencia Básica***.** Ministerio del Interior. Comisión Técnica de Apoyo a la implantación del DNI Electrónico. Grupo de Trabajo de Comunicación y Divulgación. Versión 1.1, de 26 de junio de 2006, disponible en la web del Ministerio del Interior.

*Evolución del mercado asegurador***.** Estadística a septiembre de 2006. Informe nº 997. Noviembre, 2006. ICEA.

Informe Bangemann. BANGEMANN, presentado al Consejo Europeo de Corfú de junio de 1994 bajo el título: *"Europa y la Sociedad global de la Información"*, en: http://europa.eu.int.

Informe Grupo de Trabajo del artículo 29. Tratamiento de datos biométricos, 1 de agosto de 2003.

Insurance Core Principles and Methodology. Internacional Association of Insuresr Supervisors (2003), Basiles, disponible en: www.iaisweb.org,

*Internet y el Seguro Electrónico***.** Estadística año 2005. Informe nº 965. ICEA.

La libertad informática, un novísimo derecho fundamental. MENDIZABAL ALLENDE, Rafael. Jornadas sobre protección de la privacidad, Pamplona, 22 y 23 de junio de 2000. APD, p.15-16.

La Protección de Datos en Internet. SUÑÉ LLINÁS, Emilio. II Congreso Mundial de Derecho Informático. Madrid, 2003, en: http://www.ieid.org.

*La Sociedad de la Información en España 2006***.** Ariel. Colección Fundación Telefónica.

Las Tecnologías de la Información en el Sector Asegurador. Estadística año 2006. Informe nº 1.034, de septiembre 2007. ICEA.

Las TIC en la Sanidad del Futuro. Telefónica 2006, disponible en la web de Telefónica.

Le droit de l'informatique. LUCAS, A. PUF. Paris, 1987.

Licensing of Trusted Third Parties for the Provision of Encryption Services. INFORME GOBIERNO BRITÁNICO http://www.dti.gov.uk/pubs, 2000.

*Memoria de la Agencia Española de Protección de Datos del año 2004***,** en relación a la aplicación de la LOPD a ficheros y tratamientos no automatizados.

Memoria de la Agencia Española de Protección de Datos de año 1999.

Los riesgos derivados del comercio electrónico y del uso de la Internet y su aseguramiento. Ponencia presentada por ARTIGAS, Francisco y otros, en representación de la sección chilena de AIDA para el Congreso Iberoamericano de Derecho de Seguros. Rosario República Argentina, disponible en: Biblioteca Fundación MAPFRE.

Protección de datos de carácter personal. Antecedentes y ordenamiento europeo. HEREDERO HIGUERAS, M. Master en Derecho de las

Telecomunicaciones y de las tecnologías de la información. Curso 2000-2001. Universidad Carlos III de Madrid, no publicado.

*Semana del Seguro XIV Edición***.** Ponencias. 2007. Madrid.

Transacciones electrónicas en Internet, ACED FÉLEZ, Emilio. Jornadas sobre protección de la privacidad, Pamplona 22 y 23 de junio de 2000. APD, p. 112.
VII Informe del Sector Asegurador en Internet. Julio-septiembre 2006. Publicado en octubre 2007.

World Insurance Report. Informe Capgemini, 2007.

*Cuaderno de Protección de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid***,** en: www.apdm.es.

Informe 127/2004 AEPD, relativo a la cesión de datos sin consentimiento por corredor de seguros, en: www.agpd.es

Informe 359/2002 AEPD, relativo a la cesión de datos personales.

Informe 433/2003 de la AEPD en el que se analiza la actuación del corredor de seguros: www.agpd.es

Informes del año 19993 y 2003 de la AEPD, sobre correo electrónico y dirección IP : www.agpd.es.

Informe del Parlamento Europeo sobre las repercusiones éticas, jurídicas, económicas y sociales de la genética humana. Final A5-0391/2001, 8 de noviembre de 200

Recomendaciones dirigidas a usuarios de Internet, en: www.agpd.es

ARTÍCULOS DE REVISTAS ESPECIALIZADAS

*Alternative Distribution Channels of Insurance Products. European Outlook***.** A PartnerRe Publication. April, 2001.

*An análisis of the quality of Internet Life Insurance Advine***.** Risk Management and Insurance Review, 2002. Vol. 5, nº 2, 135-154.

*Así será 2007***.** Aseguranza, nº 114, de febrero 2007.

*Click seguros***.** Aseguranza, nº 117, de mayo 2007.

*Confianza y Credibilidad en Internet***.** ARAGON, Salvador. NotaEnter, nº 18, de 30 de mayo de 2006.

Derecho a la intimidad e informática. TRUJOL, A y VILLANUEVA ECHEVARRÍA, Información Jurídica, nº 318, julio-septiembre, 1973.
*DNI electrónico: la llave digital del apoderado***.** SZYMANSKI, Marek GRACIA, David. Estrategia Financiera, nº 229, junio 2006, pp.67-69.

*El Modelo Operacional de Clientes en el Sector Asegurador***.** ORTAL, Javier. Innovación y Tecnología, 2006, disponible en: www.capgemini.es.

El proyecto genoma humano y el seguro de personas, Mangialardi,E. R*evista Española de Seguros,* nº 1005, enero-marzo 2001, pp. 7-19.

*El Sector Asegurador Progresa hacia la Transacción por Internet***.** Aseguradores, enero-febrero 2004, pp.40-41.

El Sector Asegurador y de los Planes y Fondos de Pensiones, ICE, noviembre-diciembre 2006, nº 833, p.110.

*El Seguro Digital***.** Mercado Asegurador, 2007, pp. 24-29.

El seguro se topa con la Red. Revista Mediario, junio 2006.

*Evidencias electrónicas. Informática forense***.** Revista Sector Técnico-Profesional, nº 52, de noviembre 2006.

*Evolución del mercado asegurador en 2007***.** Boletín nº 86. ICEA.

*Fuentes de Información en Internet del Sector Seguros***.** REVILLA, Marisol. Centro de Documentación de la Fundación MAPFRE. Revista nº 96 pp. 59 a 65.

*Impulso a la contratación "on-line"***.** Actualidad Aseguradora, de 21 de noviembre de 2005, pp.16-17.

*Internet se impondrá en productos de escaso valor añadido***.** SIERRA, Rafael. Nº 109, de septiembre 2006.

Internet: por debajo de las expectativas. CHICOTE, Manuel. Actualidad Aseguradora, de 19 de marzo de 2007.

*Introducción a las Tecnologías WEB***.** Giménez Luis. Dpto. Informática Tributaria Agencia Tributaria. Madrid 2003.

La Confianza y el compromiso en las relaciones a través de Internet. FLAVIÁN, C. Cuadernos de Economía y Dirección de Empresa. Núm. 29, 2006, pp. 133-160.

La Libertad informática como derecho fundamental. ALVAREZ RICO, M y ALVAREZ-RICO GARCÍA, I. Revista Sociedad y Utopía. Revista de Ciencias Sociales, nº 13. Mayo 1999.

La mediación se enfrenta al reto de la protección de datos. Revista Mediario, febrero, 2007.

La minería de datos ya no es una tendencia dominante. DATAMATION. WATTERSON, Karen Edición española, febrero, 2000. http:www.techweb.com/encyclopedia.

La regulación de los seguros privados. ALVAREZ CAMIÑA, Sergio. Revista ICE, noviembre-diciembre, 2006, nº 833, p.112.

La Regulación de los Seguros Privados: Objetivos, Evolución y Nuevas Tendencias. ALVAREZ CAMIÑA, Sergio. El Sector Asegurado y de los Planes y Fondos de Pensiones. Revista ICE, noviembre-diciembre, 2006, nº 833, pp. 101-114.

La Transformación del Entorno Asegurador. MONTIJANO GUARDIA, Francisco. Economía de los Seguros. AIDA. 1999.

*Las Aseguradoras se suben al carro de Internet***.** Revista Sociedad y Utopía, mayo 2006, p.60.

Las Tecnologías de la Información en el Sector Asegurador. Estadística año 2006. Informe nº 958, de julio 2006. ICEA.

*Las TIC toman las riendas del sector Seguros***.** Revista Sociedad de la Información, mayo 2006.

*Líderes, las diez primeras entidades en cada ramo***.** Revista Mercado Previsor. 2007. pp.24-31

Los mediadores. Aseguranza, nº 116, de abril 2007.

*Los riesgos que vienen***.** RIBAGORDA, Arturo. Cuadernos de Seguridad, noviembre 1999, pp.43-36.

Nuevas coberturas para la exposición a Internet. Actualidad Aseguradora, de 20 de febrero de 2006.

*Privacidad e Identidad en el mundo digital***,** disponible en: http://blues.inf.tu-dresden.de/prime/EUT_Tutorial_V/spanish/PRIME_fs.htm.

*Retos del Seguros para 2007***.** LOZANO, Ricardo**.** Actualidad Aseguradora, de 5 de febrero de 2007, pp. 1-4.

*Soluciones para el Sector Asegurador***.** Informe de Getronics, disponible en : www.getronics.org.

The Right to Privacy. WARREN Y BRANDEIS Harvard Law Review, nº4, 1980.

*Tráfico Jurídico Electrónico y Contrato de Seguro***.** CAMACHO CLAVIJO, Sandra. Revista Española de Seguros, nº 127, julio-septiembre 2006, pp. 432-474.

AGENCIA DE PROTECCIÓN DE DATOS

Todas las referencias que se recogen a continuación estás disponibles en: www.agpd. es:

- *Informe* 182/2004 de la AEPD. Datos de salud.
- *Informe* 582/2004 de la Agencia de Protección de Datos
- *Informe* 526/2003, de la Agencia Española de Protección de Datos, relativo a la cesión de datos de salud a aseguradoras de asistencia sanitaria por centros sanitarios públicos.
- Informe jurídico 7/72005, disponible en: www.agpd.s/Canal_Documentacione/InformesJuridico.
- *Instrucción 2/1995***,** de 4 de mayo de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal**.** BOE, de 9 de mayo de 1995, p. 13324.
- *Instrucción de 1 de marzo de 1996***.** prestación de servicios de solvencia patrimonial y crédito**.** BOE, de 4 de marzo de 1995, p. 795.
- Memoria 2001, de la Agencia Española de Protección de Datos, pp. 260-261.
- Memoria del año 2000 de la Agencia Española de Protección de Datos
- *Procedimiento de la Agencia Española de Protección de Datos nº PS/00377/2005, contra la Correduría de Seguros R.F.I. Asunto: Recurso de Reposición.*
- *Procedimiento PS0076/2005 contra Eboseguros. Asunto: Recurso de Reposición.*
- *Recomendación 1/2005***,** de 5 de agosto, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid.

- *Recomendación 2/2004***,** de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid**,** sobre Custodia, Archivo y Seguridad de los Datos de Carácter Personal de las Historias Clínicas no informatizadas.
- *Resolución AEPD***.** Expediente nº E/0004/2004. Archivo de Actuaciones contra compañía MAPFRE.
- *Resolución AEPD*. Expediente nº E/00585/2004. Archivo de Actuaciones contra Banco Cetelem S.A y Cardif Assurances Risques Divers.
- *Resolución de 21 de marzo de 2000 de la AEPD*, dictada en el Expediente E/00055/1999, en relación a empresarios individuales o autónomos.
- *Resolución de 28 de octubre de 2005* contra la Compañía ARAG, Compañía Internacional de Seguros y Reaseguros
- *Resolución R/00490/2006 de la AEPD*, en el procedimiento sancionador PS/00005/2006, contra Gutysa Correduría de Seguros SL, Aegon Seguros y Winterthur Vida.
- *Resolución R/00566/2006 de la AEPD*, en el procedimiento sancionador PS/00041/2006, contra Centro Clínico La Chopera.
- *Resolución R/00594/2004 de la AEPD*, en el procedimiento sancionador PS 00037/2004, contra la entidad Victoria Meridional Compañía de Seguros y Reaseguros S.A y el Consulting de Asesores periciales CAP.
- *Resolución R/00600/2004 de la AEPD*, en el procedimiento sancionador PS/0042/2004, contra Caixa d'Estalvis Laietana y Preventiva Compañía de Seguros y Reaseguros.
- *Resolución R/00630/2006 de la AEPD*, en el procedimiento sancionador PS/00378/2005, contra Hilo Direct Seguros y Reaseguros S.A y Marsh S.A. Mediadores de Seguros.
- *Resolución R/00927/2005 de la AEPD*, en el procedimiento sancionador PS/00122/2005, contra MAPFRE..

LEGISLACIÓN

Convenio 108, de 1981, Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. BOE de 15 de noviembre de 1985.

Carta de San Francisco. Versión española de la versión revisada, aprobada por Resolución 45/95, de 14 de diciembre, de la Asamblea General de las Naciones Unidas (documento E/CN.4/1990/72, 20 de febrero de 1990).

Ley General de Sanidad 14/1986, de 25 de abril.

Ley 3/1994, de adaptación de la Segunda Directiva de Coordinación Bancaria.

Ley Orgánica 10/1995, de 23 de octubre, de Código Penal.

Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Ley 34/2003, de 4 de noviembre, de modificación y adaptación a la normativa comunitaria de la legislación de seguros privados. BOE, de 5 de noviembre de 2003.

Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley 20/2005, de 14 de noviembre, de creación del Registro de Contratos de Seguros de cobertura de fallecimiento, desarrollado por Real Decreto 398/2007, de 23 de marzo.

Ley 59/2003 de firma electrónica.

Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema nacional de Salud.

Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente.

Ley 26/2006, de julio de 2006, de Mediación del Seguro Privado.

Ley 13/2007, de 2 de julio, por la que se modifica el Texto Refundido de la Ley de Ordenación y Supervisión de los Seguros Privados, aprobado por el Real Decreto Legislativo 6/2004, de 29 de octubre, en materia de supervisión del reaseguro. BOE, de 3 de julio de 2007.

Directiva 95/46/CE, de protección de datos de carácter personal.

Directiva 2001/17/CE sobre saneamiento y liquidación de entidades aseguradoras.

Directiva 1999/93/CE, de 13 de diciembre, de firma electrónica.

Directiva 2000/31/CE, de 8 de junio, sobre el Comercio Electrónico.

Directiva 2002/12 y2002/13 sobre margen de solvencia de entidades aseguradoras de vida y de seguros distintos del de vida.

Directiva 2002/63/CE sobre seguros de vida, deroga la Directiva 2002/12 y refunde y codifica la normativa comunitaria sobre el seguro de vida.

Real Decreto-ley 14/1999, de 17 de septiembre, de firma electrónica.

Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de Ordenación y Supervisión de los Seguros Privados. BOE, de 5 de noviembre de 2004.

Real Decreto 2014/1997, de 26 de diciembre, por el que se aprueba el Plan de Contabilidad de las entidades aseguradora y normas para la formulación de las cuentas de los grupos de entidades aseguradoras.

Reglamento 994/1999, de 11 de junio, de Medidas de Seguridad.

Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LO 5/1992. BOE de 21 de junio

Real Decreto 2486/1998, de 20 de noviembre, por el que se aprueba el Reglamento de ordenación y Supervisión de Seguros Privados.

Real Decreto 996/2000, de 2 de junio, por el que se modifican determinados preceptos del Reglamento de Ordenación y Supervisión de los Seguros Privados y del Plan de Contabilidad de las entidades aseguradora, para adaptarlos a la Directiva 98/78/CE, de 27 de octubre, relativa a la supervisión adicional de la empresas de seguros que formen parte de un grupo de seguros.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

Orden Ministerial de 23 de diciembre de 1998, por la que se desarrollan determinados preceptos de la normativa reguladora de los seguros privados y se establecen las obligaciones de información como consecuencia de la introducción del euro.

Orden EHA/339/2007, de 16 de febrero, por la que se desarrollan determinados preceptos de la normativa reguladora de los seguros privados. BOE de 20 de febrero de 2007.

Recomendación nº R (97) 5 del Consejo de Europa. Perfil genético.

JURISPRUDENCIA

Sentencia del Tribunal Constitucional 142/1993, de 22 de abril. Relaciones sociales y profesionales.

Sentencia del Tribunal Constitucional 20/1992, de 14 de febrero. Captación de información y divulgación ilegítima de datos.

Sentencia del Tribunal Constitucional 197/1991, de 17 de octubre. Captación de información y divulgación ilegítima de datos.

Sentencia del Tribunal Constitucional 231/1988. Ámbito personal y familiar.

Sentencia del Tribunal Constitucional 11/1981, de 8 de abril. No existencia de derechos absolutos.

Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre. No existencia de derechos absolutos.

Sentencia de la Audiencia Provincial de Vizcaya, sección 5ª, de 29 de marzo de 2001, núm. 326/2001.

Sentencia de la Audiencia Nacional de 6 de julio de 2001. Banca a distancia.

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, sobre empresarios y autónomos Sentencia de 15 de febrero de 2006 de la Audiencia Nacional. Sala de lo Contencioso-Administrativo. Ausencia de consentimiento.

Sentencia de la Audiencia Nacional núm. 6201/2000, de 15 de noviembre (núm. Rec. 732/2000). Carácter escrito contratos prestación servicios.

Sentencia Audiencia Nacional de 11 de enero de 2002. Envío publicidad sin consentimiento.

Sentencia Audiencia Nacional de 8 de marzo de 2002. Datos disociados.

Sentencia Audiencia Nacional de 14 de junio de 2002.

Sentencia Audiencia Nacional, 13 de septiembre de 2002, núm. Rec. 1065/1999.

Sentencia Audiencia Nacional de 31 de enero de 2003. Consentimiento.

Sentencia de la Audiencia Nacional de 20 de mayo de 2005. Sanción a una empresa reaseguradora por infracción del artículo 11 de la LOPD.

Sentencia de la Audiencia Nacional de 22 de junio de 2005 en relación a la cesión de datos entre empresas del mismo grupo para la promoción, captación y seguimiento de su cartera de clientes.

Sentencia Audiencia Nacional de 21 de septiembre de 2005. Cesión del crédito mercantil.

Sentencia de la Audiencia Nacional de 15 de febrero de 2006. Ausencia de consentimiento.

Sentencia Audiencia Nacional de 18 de enero de 2006, (núm. Rec. 225/2004).

Sentencia de 31 de enero de 2003, de la Audiencia Nacional, núm. Rec. 3290/2001, caso “Gran Hermano”.

Sentencia Audiencia Nacional de 11 de abril de 2005, contra operador de telecomunicaciones.

Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre. Captación de información y divulgación ilegítima de datos.

Sentencia del Tribunal Constitucional 57/1994, de 28 de febrero. Captación de información y divulgación ilegítima de datos.

COLECCIÓN "CUADERNOS DE LA FUNDACIÓN"
Instituto de Ciencias del Seguro

Para cualquier información o para adquirir nuestras publicaciones puede encontrarnos en:

Instituto de Ciencias del Seguro
Publicaciones
Monte del Pilar, s/n – 28023 El Plantío, Madrid – (España)
Telf.: + 34 915 818 768
Fax: +34 913 076 641
publicaciones.ics@mapfre.com
www.fundacionmapfre.com/cienciasdelseguro

125. La seguridad jurídica de las tecnologías de la información en el sector asegurador. 2008

124. Las compañías aseguradoras en los procesos penal y contencioso-administrativo. 2008

123. Predicción de tablas de mortalidad dinámicas mediante un procedimiento *bootstrap*. 2008

122. Factores de riesgo y cálculo de primas mediante técnicas de aprendizaje. 2008

121. La solicitud de seguro en la Ley 50/1980, de 8 de octubre, de Contrato de Seguro. 2008

120. Propuestas para un sistema de cobertura de enfermedades catastróficas en Argentina. 2008

119. Análisis del riesgo en seguros en el marco de Solvencia II: Técnicas estadísticas avanzadas Monte Carlo y Bootstrapping. 2007

118. Los planes de pensiones y los planes de previsión asegurados: su inclusión en el caudal hereditario. 2007

117. Evolução de resultados tecnicos e financieros no mercado segurador iberoamericano. 2007

116. Análisis de la Ley 26/2006 de Mediación de Seguros y Reaseguros Privados. 2007

115. Sistemas de cofinanciación de la dependencia: seguro privado frente a hipoteca inversa. 2007

114. El sector asegurador ante el cambio climático: riesgos y oportunidades. 2007

113. Responsabilidade social empresarial no mercado de seguros brasileiro influências culturais e implicações relacionais. 2007

112. Contabilidad y análisis de cuentas anuales de entidades aseguradoras. 2007

111. Fundamentos actuariales de primas y reservas de fianzas. 2007

110. El *Fair Value* de las provisiones técnicas de los seguros de Vida. 2007

109. El Seguro como instrumento de gestión de los M.E.R. (Materiales Específicados de Riesgo). 2006

108. Mercados de absorción de riesgos. 2006

107. La exteriorización de los compromisos por pensiones en la negociación colectiva. 2006

106. La utilización de datos médicos y genéticos en el ámbito de las compañías aseguradoras. 2006

105. Los seguros contra incendios forestales y su aplicación en Galicia. 2006

104. Fiscalidad del seguro en América Latina. 2006

103. Las NIIF y su relación con el Plan Contable de Entidades Aseguradoras. 2006

102. Naturaleza jurídica del Seguro de Asistencia en Viaje. 2006

101. El Seguro de Automóviles en Iberoamérica. 2006

100. El nuevo perfil productivo y los seguros agropecuarios en Argentina. 2006

99. Modelos alternativos de transferencia y financiación de riesgos “ART”: situación actual y perspectivas futuras. 2005

98 Disciplina de mercado en la industria de seguros en América Latina. 2005

97 Aplicación de métodos de inteligencia artificial para el análisis de la solvencia en entidades aseguradoras. 2005

96. El Sistema ABC-ABM: su aplicación en las entidades aseguradoras. 2005

95. Papel del docente universitario: ¿enseñar o ayudar a aprender?. 2005

94. La renovación del Pacto de Toledo y la reforma del sistema de pensiones: ¿es suficiente el pacto político?. 2005

92. Medición de la esperanza de vida residual según niveles de dependencia en España y costes de cuidados de larga duración. 2005

91. Problemática de la reforma de la Ley de Contrato de Seguro. 2005

90. Centros de atención telefónica del sector asegurador. 2005

89. Mercados aseguradores en el área mediterránea y cooperación para su desarrollo. 2005

88. Análisis multivariante aplicado a la selección de factores de riesgo en la tarificación. 2004

87. Dependencia en el modelo individual, aplicación al riesgo de crédito. 2004

86 El margen de solvencia de las entidades aseguradoras en Iberoamérica. 2004

85. La matriz valor-fidelidad en el análisis de los asegurados en el ramo del automóvil. 2004

84. Estudio de la estructura de una cartera de pólizas y de la eficacia de un Bonus-Malus. 2004

83. La teoría del valor extremo: fundamentos y aplicación al seguro, ramo de responsabilidad civil autos. 2004

81. El Seguro de Dependencia: una visión general. 2004

80. Los planes y fondos de pensiones en el contexto europeo: la necesidad de una armonización. 2004

79. La actividad de las compañías aseguradoras de vida en el marco de la gestión integral de activos y pasivos. 2003

78. Nuevas perspectivas de la educación universitaria a distancia. 2003

77. El coste de los riesgos en la empresa española: 2001.

76. La incorporación de los sistemas privados de pensiones en las pequeñas y medianas empresas. 2003

75. Incidencia de la nueva Ley de Enjuiciamiento Civil en los procesos de responsabilidad civil derivada del uso de vehículos a motor. 2002

74. Estructuras de propiedad, organización y canales de distribución de las empresas aseguradoras en el mercado español. 2002

73. Financiación del capital-riesgo mediante el seguro. 2002

72. Análisis del proceso de exteriorización de los compromisos por pensiones. 2002

71. Gestión de activos y pasivos en la cartera de un fondo de pensiones. 2002

70. El cuadro de mando integral para las entidades aseguradoras. 2002

69. Provisiones para prestaciones a la luz del Reglamento de Ordenación y Supervisión de los Seguros Privados; métodos estadísticos de cálculo. 2002

68. Los seguros de crédito y de caución en Iberoamérica. 2001

67. Gestión directiva en la internacionalización de la empresa. 2001

65. Ética empresarial y globalización. 2001

64. Fundamentos técnicos de la regulación del margen de solvencia. 2001

63. Análisis de la repercusión fiscal del seguro de vida y los planes de pensiones. Instrumentos de previsión social individual y empresarial. 2001

62. Seguridad Social: temas generales y régimen de clases pasivas del Estado. 2001

61. Sistemas Bonus-Malus generalizados con inclusión de los costes de los siniestros. 2001

60. Análisis técnico y económico del conjunto de las empresas aseguradoras de la Unión Europea. 2001

59. Estudio sobre el euro y el seguro. 2000

58. Problemática contable de las operaciones de reaseguro. 2000

56. Análisis económico y estadístico de los factores determinantes de la demanda de los seguros privados en España. 2000

54. El corredor de reaseguros y su legislación específica en América y Europa. 2000

53. Habilidades directivas: estudio de sesgo de género en instrumentos de evaluación. 2000

52. La estructura financiera de las entidades de seguros, S.A. 2000

50. Mixturas de distribuciones: aplicación a las variables más relevantes que modelan la siniestralidad en la empresa aseguradora. 1999

49. Solvencia y estabilidad financiera en la empresa de seguros: metodología y evaluación empírica mediante análisis multivariante. 1999

48. Matemática Actuarial no vida con MapleV. 1999

47. El fraude en el Seguro de Automóvil: cómo detectarlo. 1999

46. Evolución y predicción de las tablas de mortalidad dinámicas para la población española. 1999

45. Los Impuestos en una economía global. 1999

42. La Responsabilidad Civil por contaminación del entorno y su aseguramiento. 1998

41. De Maastricht a Amsterdam: un paso más en la integración europea. 1998

Nº Especial Informe sobre el Mercado Español de Seguros 1997
Fundación MAPFRE Estudios

39. Perspectiva histórica de los documentos estadístico-contables del órgano de control: aspectos jurídicos, formalización y explotación. 1997

38. Legislación y estadísticas del mercado de seguros en la comunidad iberoamericana. 1997

37. La responsabilidad civil por accidente de circulación. Puntual comparación de los derechos francés y español. 1997

36. Cláusulas limitativas de los derechos de los asegurados y cláusulas delimitadoras del riesgo cubierto: las cláusulas de limitación temporal de la cobertura en el Seguro de Responsabilidad Civil. 1997

35. El control de riesgos en fraudes informáticos. 1997

34. El coste de los riesgos en la empresa española: 1995

33. La función del derecho en la economía. 1997

Nº Especial Informe sobre el Mercado Español de Seguros 1996
Fundación MAPFRE Estudios

32. Decisiones racionales en reaseguro. 1996

31. Tipos estratégicos, orientación al mercado y resultados económicos: análisis empírico del sector asegurador español. 1996

30. El tiempo del directivo. 1996

29. Ruina y Seguro de Responsabilidad Civil Decenal. 1996

Nº Especial Informe sobre el Mercado Español de Seguros 1995
Fundación MAPFRE Estudios

28. La naturaleza jurídica del Seguro de Responsabilidad Civil. 1995

27 La calidad total como factor para elevar la cuota de mercado en empresas de seguros. 1995

26. El coste de los riesgos en la empresa española: 1993

25. El reaseguro financiero. 1995

24. El seguro: expresión de solidaridad desde la perspectiva del derecho. 1995

23. Análisis de la demanda del seguro sanitario privado. 1993

Nº Especial Informe sobre el Mercado Español de Seguros 1994
Fundación MAPFRE Estudios

22. Rentabilidad y productividad de entidades aseguradoras. 1994

21. La nueva regulación de las provisiones técnicas en la Directiva de Cuentas de la C.E.E. 1994

20. El Reaseguro en los procesos de integración económica. 1994

19. Una teoría de la educación. 1994

18. El Seguro de Crédito a la exportación en los países de la OCDE (evaluación de los resultados de los aseguradores públicos). 1994

Nº Especial Informe sobre el mercado español de seguros 1993
FUNDACION MAPFRE ESTUDIOS

16. La legislación española de seguros y su adaptación a la normativa comunitaria. 1993

15. El coste de los riesgos en la empresa española: 1991

14. El Reaseguro de exceso de pérdidas 1993

12. Los seguros de salud y la sanidad privada. 1993

10. Desarrollo directivo: una inversión estratégica. 1992

9. Técnicas de trabajo intelectual. 1992

8. La implantación de un sistema de *controlling* estratégico en la empresa. 1992

7. Los seguros de responsabilidad civil y su obligatoriedad de aseguramiento. 1992

6. Elementos de dirección estratégica de la empresa. 1992

5. La distribución comercial del seguro: sus estrategias y riesgos. 1991

4. Los seguros en una Europa cambiante: 1990-95. 1991

2. Resultados de la encuesta sobre la formación superior para los profesionales de entidades aseguradoras (A.P.S.). 1991

1. Filosofía empresarial: selección de artículos y ejemplos prácticos. 1991