Francisco Ramón González-Calero Manzanares.
Experto en Derecho de las Nuevas Tecnologías.
Master en Comunidades Europeas y Unión Europea.
Licenciado en Derecho.

ASPECTOS JURÍDICOS DEL COMERCIO ELECTRÓNICO, EN ESPECIAL LA PROTECCIÓN DE DATOS, LA FIRMA ELECTRÓNICA Y LA PROPIEDAD INTELECTUAL.

ISBN: 699-9670-3.
Solicitud ante el Registro General de la Propiedad Intelectual: CR-111-02.
2ª Edición Madrid 2003.

Existe una máxima que dispone que “es de buen nacido el ser agradecido”, por ello no quiero comenzar la presente obra, sin mostrar mi más profundo y sincero agradecimiento, a las personas que han hecho posible que esta embarcación llegue a buen puerto.

En primer lugar quiero agradecer al Real Instituto de Estudios Europeos y a su Presidente D. Maximiliano Bernad y Alvarez de Eulate, la oportunidad de cursar este Master y la confianza prestada en mi persona, antes y durante la realización del mismo.

De igual forma quiero agradecer a mi tutor, Sergio Guillén Andreu, los sabios consejos, paciencia y diligencia, mostrados durante la elaboración de esta obra.

Finalmente, sólo queda reconocer el apoyo y la confianza mostrados por mi familia, vitales para el desarrollo y la culminación de este Master y la posterior ampliación de esta obra..

ABREVIATURAS UTILIZADAS.

A.E.A.T.	*Agencia Estatal de la Administración Tributaria.*
A.P.D.	*Agencia de Protección de Datos.*
B.E.I.	*Banco Europeo de Inversiones.*
B.O.E.	*Boletín Oficial del Estado.*
B.O.L.	*Boletín de la Unión Europea.*
C.E.	*Comercio Electrónico.*
C.E.E.	*Comunidad Económica Europea.*
CEN.	*Comité Europeo de Normalización.*
CENELEC.	*Comité Europeo de Normalización Electrónica.*
C.G.P.J.	*Consejo General del Poder Judicial.*
CNUDMI/UNCITRAL.	*Comisión de Naciones Unidas para el Derecho Mercantil Internacional.*
D.O.C.E.	*Diario Oficial de las Comunidades Europeas.*
D.O.U.E.	*Diario Oficial de la Unión Europea.*
EDI.	*Intercambio Electrónico de Datos.*
E.E.E.	*Espacio Económico Europeo.*
E.E.M.M.	*Estado Miembro de las Comunidades Europeas.*
EFTA/AELC.	*Asociación Europea de Libre Cambio.*
ETSI.	*European Telecommunications Standards Institute.*
F.D.	*Firma Digital.*
F.E.	*Firma Electrónica.*
F.E.A.	*Firma Electrónica Avanzada.*
FEDER.	*Fondo Europeo de Desarrollo Regional.*
F.E.I.	*Fondo Europeo de Inversiones.*
GATT.	*General Agreement Task and Tariffs.*
ICANN.	*Internet Corporation for Assigned Names and Numbers.*
IETF.	*Internet Engineering Task Force.*
IP.	*Internet Protocol/ Dirección IP.*
I.R.P.F.	*Impuesto de la Renta de las Personas Físicas.*
ISP/PSI.	*Proveedor de Servicios de Internet.*
IST/TSI.	*Tecnologías de la Sociedad de la Información.*
IVA.	*Impuesto Sobre el Valor Añadido.*
LOCM	*Ley de Ordenación del Comercio Minorista.*
LOPD.	*Ley Orgánica de Protección de Datos de Carácter Personal.*
LORTAD.	*Ley Orgánica de Tratamiento Automatizado de Datos.*
LSSI.	*Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.*
OCDE.	*Organización para la Cooperación y el Desarrollo Económico.*
OMC/WTO.	*Organización Mundial del Comercio.*

OMPI.	*Organización Mundial para la Propiedad Intelectual.*
PI	*Propiedad Intelectual.*
PIN/NPI.	*Número Personal de Identificación.*
PKI/ICP.	*Infraestructura en Clave Pública.*
PYME.	*Pequeñas y Medianas Empresas.*
R.M.S.	*Reglamento de Medidas de Seguridad.*
S.I.	*Sociedad de la Información.*
T.C.E.	*Tratado de la Comunidad Europea.*
TEDIS.	*Trade Electronic Data Interchange Systems.*
TIC.	*Tecnologías de la Información y Comunicación.*
T.J.C.E.	*Tribunal de Justicia de las Comunidades Europeas.*
TRPI	*Texto Refundido de Propiedad Intelectual.*
T.U.E.	*Tratado de la Unión Europea.*
U.E.	*Unión Europea.*
UMTS.	*Universal Mobile Telecommunications Systems.*
WWWC.	*World Wide Web Consortium. (W3C).*

INTRODUCCIÓN.

No hace mucho tiempo, pero ya queda lejos el nacimiento de Internet (Inter. –conexión-, Net- abreviatura del ingles *Networks* o red-), en 1969 a raíz de un proyecto de defensa norteamericano, desarrollado conjuntamente con la comunidad universitaria, que pretendía comunicar ordenadores a través de una red. Hoy podemos afirmar rotundamente que el Comercio Electrónico (C.E.), está cambiando nuestra vida cotidiana. Las posibilidades que ofrece a los usuarios son enormes, incalculables e inimaginables. El hecho de poder comprar sin horarios, a precios más bajos y con mayores facilidades de comparación entre distintas ofertas, es hoy ya una realidad. Pero aún provocará una mayor revolución el C.E. a través del teléfono móvil (denominado *M-Commerce*[1]), ya que al no necesitar un terminal fijo (ordenador o televisor), las ventajas se incrementan al ser posible la transacción independientemente del lugar donde se encuentre el usuario.

Para las empresas, también está reportando ventajas esta forma de negocio, en cuanto al ahorro de costes al necesitar menos personal, ahorro que repercuten al usuario con una bajada de precios. Igualmente mejora su modelo de negocio, mercado y ofrece nuevas formulas de atención al cliente.

Por dar una primera definición de C.E., para no adentrarnos más en el estudio del tema sin haber explicado en que consiste éste, cabría considerarlo como una prestación de bienes o servicios remunerada, en el que las partes se encuentran a distancia, llevada a cabo por medios electrónicos (como Internet o correo electrónico).

Como todo sector dinámico y en construcción plantea problemas que han de ser resueltos para su éxito. Así se necesita un marco jurídico acorde a las nuevas características y necesidades de esta práctica, sensibilizar a los consumidores y empresas de las ventajas que para ellos reporta el C.E., eliminar los obstáculos, incertidumbres y falta de confianza que lo rodea.

Por las razones indicadas, y otras que aparecerán a lo largo de la obra, se está actuando desde la U.E. y de ahí nace su objetivo, que no es otro que el de realizar un estudio de la legislación del Comercio Electrónico y de las distintas legislaciones conexas, como la Firma Electrónica (F.E.), la Protección de Datos de Carácter Personal o la Propiedad Intelectual, en la legislación de la U.E. y en la última parte de esta obra realizar una mención expresa a la transposición de esta legislación en España.

[1] Éste, es ya posible a través de la tecnología *Wap*, pero su despegue definitivo se producirá cuando entre en funcionamiento la UMTS, que dotará de mayor agilidad la transmisión de datos a través de la red.

Para ello se abordará una primera parte introductoria en la que se desarrollarán dos bloques diferenciados:

- Por un lado, se darán ciertas pinceladas sobre los beneficios del C.E. para la economía, el empleo, las empresas, los ciudadanos y la Administración Pública y se mencionarán los diversos programas que se han puesto en marcha en la U.E. para lograr los objetivos propuestos[2].

- Por el otro, se analizaran los aspectos más relevantes de las diferentes directivas y reglamentos en C.E.[3]que se han ido aprobando, o están en tramite legislativo, en el mundo comunitario, en aspectos tan diversos como: protección de los consumidores, protección de datos de carácter personal, contratación a distancia, derechos de autor, dinero electrónico, fiscalidad, tecnologías de seguridad de la información, derecho de la competencia, y seguridad de redes, por citar algunos, y para finalizar una breve referencia a aspectos internacionales, ya que si por algo se caracteriza el C.E. es por su carácter transfronterizo, y por eso a juicio del autor no realizar una breve referencia, supondría dejar inacabada esta obra. Por el contrario, no se entrará en cuestiones de organización y gestión de Internet, salvo la asignación de nombres de dominio, que por motivos de unidad de la didáctica de la materia, serán abordadas en el apartado que corresponde a la legislación española[4].

En la segunda parte, como ya se ha indicado anteriormente, se desarrollarán las Directivas de C.E. y de F.E., intentando aclarar bien los conceptos ya que es nota común de ambas la falta de claridad en su lectura para aquellos que son legos en la materia. Se comenzará por el estudio de la Directiva de C.E., para seguidamente explicar la segunda.

Para finalizar nos centraremos en la legislación española, particularmente en la recientemente aprobada Ley de Servicios de la Sociedad de la Información (LSSI[5]), que transpone la Directiva de C.E. y demás legislación en desarrollo o en complemento de está ley, como son las leyes 39/2002 y 47/2002. También nos referiremos brevemente al Real Decreto 1906/1999 de 17 de diciembre sobre la contratación telefónica o electrónica con condiciones generales en desarrollo del

[2] Sólo se mencionaran y explicaran brevemente estos programas. La única excepción será los programas eEurope en sus versiones 2002 y 2005 y las iniciativas Go Digital, que por su importancia serán desarrollados más detalladamente.

[3] Con excepción de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, 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) DOL 178 de 17.7.2000 y de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, DOL 13 de 19.1.2000, que serán objeto de estudio separado en el segundo capítulo.

[4] Esta asignación, la lleva a cabo el ICANN que es la sociedad de Internet de asignación de nombres y números. Destáquese que la U.E. ha regulado recientemente la materia a través del Reglamento (CE) nº 377/2002 del Parlamento Europeo y del Consejo de 22 de abril de 2002 relativo a la aplicación del dominio de primer nivel "eu". DOL 113 de 30 de abril de 2002.

[5] Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE 166 de 12 de julio de 2002. Corrección de error BOE de 8 de Agosto de 2002.

artículo 5.3 de la Ley 7/1998 de 13 de abril, BOE nº 98 de 14 de abril, de condiciones generales de la contratación[6], para realizar a continuación el estudio de la F.E. a través del Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma electrónica[7] y al Proyecto de Ley sobre firma electrónica, que en caso de ser aprobado, sustituirá al anterior. Finalizaremos el capítulo desarrollando, con mayor o menor detalle, las legislaciones sobre Protección de Datos de Carácter Personal y Propiedad Intelectual haciendo hincapié en las especialidades que se derivan en estas disciplinas jurídicas cuando estamos en el sector del C.E. No olvidemos que en toda página Web se nos ofrece una posibilidad de comunicación y envío de datos de carácter personal al prestador de servicios de S.I., ya sea a través de un correo electrónico o, a través de un formulario, o como veremos en el capítulo correspondiente, en ocasiones un tercero gestiona la aplicación informática en la que se tratan esos datos, que incluso puede estar ubicada en un servidor de Internet. También es importante conocer la problemática que afecta a los derechos de autor cuando estamos hablando de Internet, ya que ha proliferado prácticas nuevas, que vulneran los citados derechos, que exigen plantearse si hacen falta soluciones nuevas o si con las que se poseen actualmente basta para proteger los derechos de autor en sus diferentes vertientes.

El resto de la legislación española de transposición de las directivas mencionadas, en particular las que se encuentran en el capítulo primero, no será objeto de estudio detallado en esta obra ya que desbordaría las previsiones de lo que se espera de una obra de estas características. No obstante se darán algunas pinceladas sobre las normas que incorporan al derecho español las directivas que son objeto de estudio en el capítulo primero, en el supuesto de que esta incorporación se halla producido realmente. Todas ellas serán analizadas en el capítulo que corresponde a la LSSI, e irán a continuación de haberse producido su estudio.

[6] BOE 313 de 31 de diciembre de 1999.
[7] BOE 224 de 18 de septiembre de 1999.

CAPÍTULO PRIMERO:
EL COMERCIO ELECTRÓNICO.

En este capítulo, como se señaló anteriormente, se comenzará dando algunas pinceladas sobre el impacto que el C.E. produce en el marco de la nueva economía a empresas y consumidores, para pasar a abordar un estudio, más o menos amplio según sea el caso, de los diferentes programas lanzados desde la U.E. para facilitar la implantación de éste y, para finalizar se abordarán los aspectos más relevantes de las directivas que regulan aspectos relacionados con el C.E., a excepción de las ya mencionadas anteriormente, que serán objeto de estudio en el segundo capítulo.

I) El C.E. y la Nueva Economía.

El C.E. se muestra, según los expertos, como un factor esencial del crecimiento económico. Pese a que el primer intento de implantar esta tecnología en las transacciones comerciales fracasó en el año 2000 con la quiebra de las Puntocom (dot.com) o empresas virtuales, se continua apostando por ésta.

Sin ánimo de ser exhaustivo[8], a continuación daré unas breves pinceladas acerca del C.E. en la nueva economía y de las ventajas de su implantación.

Las tecnologías de la información y comunicación (Tic), propiciaron en los Estados Unidos 8 años de crecimiento económico consecutivo, con más de un 4% de este en los últimos años, un 2% de inflación y un 5% de paro lo que equivale a decir "pleno empleo". Este ciclo coincide con la puesta en marcha de la Red Electrónica Mundial en 1995 y aunque no puede atribuirse a ésta todo el éxito económico de esos años, es bien seguro que algo tuvo que ver.

Por otro lado, para las empresas supone un beneficio en sus procesos de producción y negocio la utilización de las Tic; de cuyos principales efectos, entre otros, destacaría los siguientes:

- Abaratamiento de los factores de producción, se accede a más proveedores, refuerza la oferta de productos y crea mayor competencia
- Menor nivel de existencias, técnicas de abastecimiento y distribución *just-in time.*
- Disminución de los costes de entrada en el mercado.
- Disminución del coste en las transacciones, servicio de seguimiento paso a paso del pedido y servicio post venta en línea.

[8] Para más información, pueden consultarse las comunicaciones de la Comisión: Estrategias para la creación de empleo en la S.I., Com. (2000) 48 final, El impacto de la economía electrónica en las empresas europeas, Com. (2001) 711 final y el informe de evaluación comparativa de la acción eEurope 2002, Com. (2002) 62 final.

Todas estas ventajas ya son reconocidas por las propias empresas[9], un 13% reconoce que ha disminuido costes y un 25% ha aumentado ingresos, aunque existen notables diferencias según el sector de que se trate[10], ya que unos se adaptan mejor que otros a las características propias de la red, como las floristerías o agencias de viaje, y otros han sabido mejorar el modelo de negocio y el valor añadido que ofrecen al consumidor final.

Estas razones han motivado que el volumen de negocio en Internet estimado para el año 2003 sea de entre 340/360.000 millones de euros, frente a los 17.000 millones de euros de 1997.

Vistas estas ventajas aún así el C.E. ha crecido menos de lo esperado, en octubre de 2000, el 31% de los usuarios de Internet había comprado en línea, mientras que en noviembre de 2001 lo hizo el 36%; pese a que el número de usuarios se incrementó en un 25%, sólo el 5% se calificó como comprador asiduo.

En cuanto a las empresas, cuanto más pequeñas son éstas, menos utilizan las Tic. El 42% de las Pyme tiene acceso a la red, pero sólo el 20%, la utiliza en operaciones comerciales. Además se compra más que se vende, ya que para comprar sólo se necesita una conexión y una tarjeta de crédito y para vender se necesita un sitio en red y mantenerlo en condiciones óptimas de seguridad.

Por si esto fuera poco se pone de manifiesto que existe un desfase mayor en las empresas Puntocom que en las de corte tradicional, ya que entre el 85-90% del C.E. se da entre empresas, es el llamado *business to business* (*B2B*)[11], frente a menos del 1% entre empresas y consumidores, el denominado *business to consumers* (*B2C*), debido a la incapacidad de las empresas para dar ofertas precisas, modelos comerciales adecuados y mala gestión en los aspectos de seguridad, confidencialidad, entrega del producto y prestación del servicio[12].

Por todo ello se aboga por la creación de un modelo mixto entre la empresa tradicional y una Puntocom, con presencia virtual y física, que se denomina modelo de *Bricks and Clicks*.

No quiero acabar sin referirme a un modelo que está ganando importancia y que por su naturaleza trae de cabeza a las compañías discográficas, denominado *Peer to Peer* (*P2P*), que será desarrollado en la parte que afecta a los derechos de autor.

[9] Véase la encuesta publicada en la página 31 y ss de la Comunicación de la Comisión, Com. (2000) 48 final.

[10] Para información sobre la penetración por sectores, véase página 24 de la Comunicación de la Comisión, Com. (2001) 711 final y página 10 y ss de la Iniciativa europea de comercio electrónico, Com. (1997) 157 final.

[11] Así, por ejemplo, en España cinco grandes, BBVA, Telefónica, TPI, Repsol YPF e Iberia se han unido recientemente creando la plataforma Adquira que pretende operar en este campo, ahorrando a las empresas matrices en la compra de bienes y servicios indirectos que, en algunos casos, supone el 25% del gasto de muchas compañías.

[12] Que influyeron en la anteriormente citada crisis de las Puntocom.

Para finalizar esta parte quiero resaltar algo que ya se puede deducir de lo analizado hasta ahora, el C.E. para desarrollarse necesita una premisa básica que es la confianza. Confianza del consumidor en una empresa, en una persona física a la que no ve, a la que no conoce personalmente. Salvo las grandes empresas que se benefician de la confianza que otorga la marca, el resto necesitan un marco jurídico claro y flexible que proteja al consumidor en aspectos tales como seguridad, autenticación, protección del consumidor, resolución de litigios rápida y barata..., aspectos que serán desarrollados en la segunda parte de este capítulo.

Pero no olvidemos que además de estos aspectos, la garantía del éxito del negocio radica en aportar un valor añadido al usuario, que algunos sectores como las agencias de viajes o servicios financieros[13] aportan al reducir los costes al consumidor al necesitar menos personal, y otros aportan elementos atractivos que invitan al consumidor a visitar la página web como es el caso de la empresa aragonesa Barrabes.com[14], en la cual toda la página principal son noticias sobre los deportes de montaña, con actualización diaria en dos turnos, mañana y tarde, o la empresa Levi`s Strauss que, al ver que por Internet y bajando los precios perjudicaba a su red de establecimientos autorizados, optó por vender única y exclusivamente pantalones personalizados a medida y diseño del consumidor.

II) Programas Comunitarios.

Desde que en 1993 en el Libro blanco sobre el crecimiento, la competitividad y el empleo. Retos y pistas para entrar en el siglo XXI[15], resaltara la importancia de avanzar hacia la sociedad de la información –primera vez que aparece este concepto- han sido numerosas las ocasiones en las que la implantación de ésta, así como el comercio electrónico aparecen en los textos comunitarios. Baste poner algunos ejemplos, tales como:

En la comunicación "la sociedad de la información: las nuevas prioridades surgidas entre Corfú y Dublin[16]", en su página 5 se lee: "...la Comisión está analizando los obstáculos que existen en potencia a los nuevos productos y servicios de la S.I., como en el caso del C.E.", o la Resolución del Consejo sobre las nuevas prioridades políticas en materia de sociedad de la información (S.I.[17]) de 21, de noviembre de 1996, que en su párrafo 21, insta a la Comisión a que analice los

[13] No vamos a entrar en la problemática del modelo de negocio de los bancos que operan por teléfono o Internet, que aunque ya disponen del 3% de los depósitos y la banca tradicional los ve como competidores, tendrán que reducir costes ya que el servicio es más caro de lo que se previó en un primer momento. Para más información pueden consultarse dos excelentes artículos sobre la materia en el "País de los Negocios" de 24 de marzo, página 5 y 2 de junio de 2002, página 7.

[14] Puesta como ejemplo, a nivel nacional e internacional, de Pyme virtual.

[15] Com. (1993) 700 final.

[16] Com. (1996) 395 final.

[17] DOC 376 de 12 de diciembre de 1996.

obstáculos potenciales al desarrollo de los nuevos servicios de la S.I., en particular el C.E..

Como resultado de éstas, las siguientes Comunicaciones van resaltando las prioridades de actuación y estableciendo un programa de trabajo con plazos de ejecución, tales como, la comunicación Europa a la vanguardia de la sociedad mundial de la información. Plan de actuación móvil[18], que subraya que constituye una prioridad garantizar el cumplimiento de las condiciones necesarias para la introducción del C.E., esto es, derechos de autor, protección de datos, firma digital... o la ya citada Iniciativa europea de C.E.[19], que haciendo un estudio sobre el C.E., pone las bases de su desarrollo posterior, a través de un plan de trabajo y fechas de realización en ámbitos tan dispares como el marco regulador, la seguridad, la firma electrónica, la protección de datos y de consumidores, la fiscalidad, los derechos de autor, la normalización y el consenso internacional (a través de la OMC, OMPI, OCDE, CNUDMI...).

Todas estas previsiones darán lugar, por un lado, a normas jurídicas que serán estudiadas en la tercera parte de este capítulo y, por el otro, a programas que serán estudiados a continuación.

A) El Programa eEurope.

Este programa fue aprobado en el Consejo Europeo de Helsinki de diciembre de 1999. En él, a través de sucesivas Comunicaciones de la Comisión Europea, se fija como objetivo promover la conexión generalizada en la red, lo mas rápidamente posible y llevar a la era digital a cada rincón de Europa, ciudadano, escuela o empresa. El acceso a Internet y su utilización ya sea mediante teléfono móvil, ordenador o decodificador de TV debe convertirse en algo casi natural.

Para ello se fijan una serie de áreas de actuación, con objetivos y plazos concretos[20]. Estos serán en un primer momento 10 líneas de actuación que posteriormente se fundirán en 3[21]. Éstas son:

1- Dar acceso a la juventud a la era digital.
2- Abaratar el acceso a Internet.
3- Acelerar la implantación del C.E.
4- Internet rápida para investigadores y estudiantes[22].

[18] Com. (1996) 607 final.
[19] Véase nota 10.
[20] Que al finalizar en el 2002, dio nombre a la primera versión del programa eEurope 2002.
[21] Por medio del documento Com. (2000) 330 final, los objetivos serán: una Internet más rápida, barata y segura, invertir en las personas y en la formación y estimular el uso de Internet.
[22] En este sentido, las Instituciones Europeas abogan por la rápida introducción de un protocolo que aumentará la rapidez de la red y que, de no hacerse coordinadamente y rápidamente, podría provocar los temidos cuellos de botella, es el IPv6, que sustituirá al actual IPv4. Aumentará el número de direcciones IP posibles, optimizando el encaminamiento de mensajes y mejorando las posibilidades de desplegar el otro Protocolo que se quiere adoptar, el

5- Tarjetas inteligentes para el acceso seguro aplicaciones electrónicas[23].
6- Capital riesgo para las Pyme de alta tecnología.
7- Participación de los discapacitados en la cultura electrónica[24].
8- Salud en línea.
9- Transporte inteligente.
10- Administración Pública en línea.

De todos estos puntos nos vamos ha centrar en el tercero, aunque cabe destacar que éste necesita de los otros para tener éxito. Así dando acceso a la juventud a Internet[25], al conectar todos los colegios a Internet, se está creando potenciales compradores en red en un futuro, así como solucionando el problema de falta de cualificación de personal en Tic que se verá mas adelante; o que la Administración preste sus servicios en línea, da confianza al usuario sobre la seguridad de la red (sí en España en el ejercicio fiscal de la renta de 2001, 1.200.000 contribuyentes han presentado la declaración del IRPF por Internet gracias a la firma electrónica que el Ministerio de Hacienda facilitaba a través de la red, con la colaboración de la Fabrica Nacional de la Moneda y Timbre, ¿por qué no estos usuarios, que por red han transmitido datos personales sobre sus ingresos y patrimonio, no van a comprar usando una tarjeta de crédito?). O como es lógico, a mayor rapidez y menor coste, más usuarios se decidirán por conectarse a la red.

Realizado el paréntesis, volvemos a ese tercer apartado al que nos referíamos anteriormente, que será explicado dentro del siguiente epígrafe por un motivo lógico: en su estructura y objetivos coincide plenamente con la iniciativa Go Digital[26] que nace de uno de los objetivos de ese tercer apartado del Programa eEurope, que trata de conseguir la implantación del C.E.. Ese objetivo, no es otro que ayudar a las Pyme a pasar a la fase digital.

En cuanto al recientemente aprobado, por el Consejo Europeo de Sevilla de 21 y 22 de junio de 2002, Programa eEurope 2005[27], tiene su origen tras el informe de evaluación comparativa[28] y las Conclusiones de la Reunión Informal de Ministros de Telecomunicaciones y Sociedad de la Información (Documento de la

---

IPSec, que ofrece confidencialidad, garantiza que los paquetes sólo los ve el receptor y suministra autenticación e integridad para garantizar que los datos del paquete son auténticos y proceden del remitente concreto.

[23] Que dio lugar al documento Com. (2000) 890 final, sobre seguridad en redes, que será estudiado más adelante.

[24] Dio pie a la Comunicación Com. (2001) 529 final, sobre accesibilidad a los sitios web públicos y de su contenido. Para evitar la fractura digital entre los discapacitados, quiere que se adopten las pautas de carácter voluntario que fija el WWWC que es un conglomerado de 160 empresas de informática, telecomunicaciones y contenidos, la mitad de las cuales son europeas, que está trabajando en una serie de iniciativas para conseguir una interoperabilidad de hecho entre las actuales tecnologías. En este mismo sentido, véase la Resolución del Consejo de 25 de marzo de 2002 sobre el plan de acción eEurope 2002: accesibilidad a los sitios web públicos y su contenido. DOC 86 de 10 de abril de 2002.

[25] Que se traduce en el programa eLearning que se explicará más adelante.

[26] Iniciativa Go Digital, ayudar a las Pyme a pasar a la fase digital, Com. (2001) 136 final.

[27] Una sociedad de la información para todos. Com. (2002) 263 final y Conclusiones de la Presidencia del Consejo Europeo de Sevilla, punto 54.

[28] Véase nota 8.

Presidencia), celebrada en Vitoria los días 22 y 23 de febrero de 2002, de los cuales se deduce que se ha avanzado pero aún queda mucho por hacer, y teniendo en cuenta que el programa acabaría a finales de 2002, era bueno prolongar su existencia hasta 2005.

El programa esta vez vuelve a incidir en áreas que ya trataba el anterior, esto es: servicios públicos en línea modernos (*e-government, e-learning, e-health*) ambiente dinámico para el C.E. y acceso barato, rápido y seguro a Internet. Las novedades del programa a destacar serán analizadas al final del siguiente apartado.

B) La iniciativa Go Digital[29].

Como ya se indicó, esta iniciativa tiene su origen en uno de los objetivos a alcanzar dentro del punto tercero del programa eEurope 2002.

Se proponen en ella las soluciones que se consideran oportunas para eliminar los obstáculos que afectan al C.E.. Éstas son las siguientes:

- Promover un entorno favorable para el C.E. y el espíritu empresarial, no basta sólo con la creación de la banda ancha, hacen falta medidas nacionales y el papel de la Comisión creando sinergia entre estas.

- Evaluar comparativamente esas estrategias europeas, nacionales, regionales y locales dentro del programa Best (simplificar el entorno empresarial) y determinar si los Fondos Estructurales y otras iniciativas pueden completar aquellas.

- Medición del grado de adopción de las Tic y el C.E. con la elaboración periódica de cuadros que permitan realizar debates con los E.E.M.M., informes sectoriales, seminarios especializados...

- Creación de un marco jurídico favorable. Sólo quedan dos Directivas por aprobar. Éstas y el resto de normas serán desarrolladas en la siguiente parte del capítulo.

- Interoperabilidad del C.E., las empresas necesitan soluciones normalizadas y compatibles con sus proveedores y usuarios, para ello deben buscarse soluciones y tecnologías aceptadas por un conjunto significativo del mercado que deberán basarse preferentemente en normas internacionales abiertas[30]. Está siendo promovida por los institutos Cen, Cenelec y Etsi, en el ámbito comunitario y

[29] Existe un claro antecedente a esta iniciativa, como lo es la Decisión del Consejo 98/253 de 30 de marzo de 1998 por la que se adopta un programa plurianual comunitario para estimular el establecimiento de la S.I. en Europa, DOL 107 de 7.4.1998, que en su artículo 2.b párrafo 8 indica " puesta en marcha de medidas para determinar las prioridades de las Pyme y vigilancia de las trabas que obstaculizan la utilización de las Tic por parte de las mismas".

[30] Difícilmente podrán comerciar dos personas físicas o jurídicas establecidas en diferentes países si el sistema de criptado del mensaje o el sistema de reconocimiento de firmas son diferentes, por poner sólo dos ejemplos.

WWWC y IETF a nivel internacional, con la participación directa de la industria en ambos casos[31].

- Proteger los intereses de los consumidores. También será explicado en la tercera parte del capítulo junto con el programa eConfidence.

- Sensibilizar sobre el paso a la fase digital, organizando determinadas manifestaciones del programa para que las Pyme comprendan mejor las herramientas y aplicaciones disponibles en relación con el C.E., a través de, asociaciones industriales, Cámaras de Comercio, Centros Europeos de Empresas e Innovación...

- Solventar los problemas de financiación y capital riesgo. Primero hay que adquirir el material, pero lo realmente costoso es el mantenimiento. Para ello se pone a disposición el programa IST (*Information society technologies*), subprograma del V Programa Marco de I+D 1998-2002[32], a través de:

?? Ensayos, para la introducción de tecnologías punta.
?? Buenas prácticas que aumenten la eficacia y calidad con un menor coste para el usuario.
?? Proyectos de demostración que prueben la viabilidad de las nuevas tecnologías.

En el año 2001 se seleccionaron 750 proyectos.

También se habilitan mecanismos de garantía de préstamos a Pyme para que inviertan en Tic y activos inmateriales (*hardware, software*...), así la Decisión 2000/819/CE del Consejo de 20 de diciembre de 2000 relativa al Programa plurianual en favor de la empresa y el espíritu empresarial, en particular para las pequeñas y medianas empresas (PYME) (2001-2005)[33], propone una serie de medidas, tales como, capital riesgo a través del FEI, *Business Angels*, viveros de empresas, patrocinio, mejor coordinación entre el BEI y FEI...

Especial importancia tienen los Fondos Estructurales en esta materia[34], propugnando una mejor utilización de estos. Dentro del actual marco financiero (2000-2006) se destinarán 400 millones de euros del Feder a acciones innovadoras[35] y se habla de financiar infraestructuras allí donde no sean rentables

[31] Destáquese la conocida como EESSI (*european electronic signatures standardization iniciative*), una iniciativa de la Industria de la Información y Comunicación Tecnológica (ICTSN).

[32] Este programa no sólo financia estos aspectos, sino que se adentra a financiar todo lo referente a las nuevas tecnologías, prestando especial interés en los aspectos de seguridad como tarjetas inteligentes y firmas electrónicas que se verán más adelante. Reseñar igualmente que en el futuro VI programa, la S.I. vuelve a ser una de las prioridades.

[33] DOL 333 de 29 de diciembre de 2000.

[34] Existe, ya hace tiempo, una preocupación por que en materia de la S.I. no se produzca una fractura digital entre las regiones más ricas y pobres. Véase en este sentido el apartado 10 de la Resolución del Consejo de 27 de noviembre de 1995 sobre los aspectos industriales para la U.E. en el desarrollo de la S.I. o en las citadas Decisión 98/253 o en el documento Com. (1996) 395 final o en el programa eEurope en sus dos versiones.

[35] Estas son dentro de las iniciativas Interreg III, Urban II, Equal y Leader+. Se quiere crear una nueva acción innovadora para el próximo marco financiero, sería eEurope Regio: la S.I. al servicio del desarrollo regional.

para evitar la temida fractura Norte-Sur. Por su parte el programa eEurope 2005 habla de cooperación entre los E.E.M.M. y la Comisión, en las regiones menos favorecidas, utilizando si fuera, posible Fondos Estructurales u otras iniciativas financieras.

- El apartado educativo pasa a ser explicado en el próximo epígrafe.

Por último, como ya se indicó, sólo basta mencionar las principales novedades que incorpora el programa eEurope 2005 y que serán, en coherencia con la línea planteada, sólo las que afectan al C.E.. Así se plantea a finales del 2003, revisar el marco jurídico en C.E. (cuestión poco novedosa ya que las Directivas 2000/31/CE de C.E. y 1999/93/CE sobre F.D. prevén una revisión de éstas, que comenzará con la publicación de una comunicación por parte de la Comisión sobre su aplicación, a mas tardar el 17 y 19 de julio de 2003, respectivamente), la seguridad en red, buscar la interoperabilidad en seguridad, transacciones, firmas, procedimiento y pagos. Se aboga por un consenso mundial en materia de interoperabilidad y legislación y como máxima novedad se propone para mediados de 2003 la creación de una *Task Force* sobre Ciberseguridad[36]. También queremos destacar que la Comisión ha cofinanciado un proyecto de información a las PYMES en relación con toda la legislación de los E.E.M.M., relativa al comercio electrónico. Para ello se han coordinado 15 Euro Info Centros y se ha creado una página Web[37] de información al respecto.

C) Otros programas[38].

- Promise: programa plurianual para el estímulo del establecimiento de la S.I. en Europa. Corresponde a la ya citada Decisión del Consejo 98/253[39]. El Programa finalizó el 31 de diciembre de 2002. Contaba con una dotación financiera para el periodo de vigencia del mismo de 25 millones de Ecus[40].

---

[36] A raíz de esta disposición, la Comisión ha presentado una Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se crea la Agencia Europea de Seguridad de Redes y de la Información, Com. (2003) 63 final. De entre los objetivos y funciones propuestos, cabe destacar el de facilitar la aplicación de las disposiciones comunitarias en materia de seguridad de redes y de la información, ayudar a garantizar la interoperabilidad de estas, recoger y analizar datos (incluyendo información sobre riesgos emergentes y actuales), asesorar a la Comisión y otros Órganos competentes en la materia, impulsar la cooperación y coordinación entre los organismos nacionales y comunitarios, facilitar un sistema de información rápida en casos de alerta, evaluar las normas sobre seguridad.

[37] www.ebusinesslex.net .

[38] Puede encontrarse información sobre estos programas en particular y sobre el C.E. en general en la página Web de la S.I. de la U.E.: "europa.eu.int/comm/dgs/information_society/index_es.htm".

[39] Véase nota 29.

[40] A raíz de la aprobación del Programa eEurope 2005, la Comisión Europea ha presentado una Propuesta de Decisión del Consejo, por la que se aprueba un programa plurianual (2003-2005) para el seguimiento de eEurope, la difusión de las buenas practicas y la mejora de la seguridad de las redes y la información (Modinis) Com. (2002) 425 final. Por medio de esta se trata de aprobar un programa plurianual (de 1 de enero de 2003 a 13 de diciembre de 2005) dotado con 25 millones de euros. Los objetivos del Plan son el de realizar un estudio comparativo de los resultados obtenidos por los EEMM y dentro de los mismos compararlos con los mejores del mundo y extraer de este estudio las consecuencias adecuadas, utilizando cuando sea posible estadísticas oficiales (benchmarking), apoyar a

- EContent: trata de mejorar el acceso e incrementar el uso de la información en el sector público, aumentar la producción de contenidos en un entorno multilingüe y multicultural, así como aumentar el dinamismo en el mercado de los contenidos digitales.

- Ecom-is (*electronic commerce open marketplace for industry sectors*): trata de crear debate y grupos de trabajo con la dirección del instituto Cen y la industria del sector en los ámbitos de la normalización y la implantación del C.E.

- ELearning: Trata de movilizar a las comunidades educativa y cultural además de los poderes sociales y económicos para operar cambios en la educación. También cabe destacar el denominado Espacio Carrera que trata de unir a la comunidad educativa y las empresas para ver las nuevas exigencias en materia de competencias en Tic, para trasladarlo a los planes de estudio. No olvidemos la importancia de este programa ya que se estima que en 2003 harán falta en Europa 3,8 millones de expertos en Tic.

- Ida (*interchange data between administrations*): trata de mejorar la eficacia del mercado interior permitiendo a la administración intercambiar información esencial vía redes telemáticas interoperables

- Ten-telecom (*trans-European telecommunications networks*): trata de apoyar servicios genéricos principalmente basados en Internet, los cuales son comunes al desarrollo de aplicaciones y servicios, que deberían tratar de lograr su interoperabilidad y seguridad. Igualmente dar un acceso fácil a las redes de telecomunicaciones a través de cable, telefonía móvil y satélites así como garantizar la interoperabilidad de la infraestructura de estos.

- Euromedis (*Euro-Mediterranean information society iniciative*): trata de desarrollar las redes de S.I. en los países mediterráneos y a su vez interconectar ésta, a la de los países europeos.

- @lis: de iguales características que el anterior pero se aplica a los países Iberoamericanos en sus diferentes foros de dialogo, Mercosur, Comunidad Andina, México y Chile[41].

---

los EEMM en las políticas que pongan en marcha dentro del programa eEurope tanto a nivel regional y nacional, desarrollando mecanismos de intercambio de experiencias, elaborar políticas adecuadas en relación con la competitividad y cohesión industriales y apoyar los esfuerzos nacionales y europeos para mejorar la seguridad de redes y de la información y de la banda ancha.

[41] Cítese igualmente los programas para Africa: PADIS (*african information society iniciative*) y para Asia: IT&C y ECOM (*electronic commerce promotion council of japan*), exclusivo para Japón.

- EEurope+: es la extensión del programa a los países candidatos a la ampliación. Trata de utilizar las posibilidades de la nueva economía en beneficio de estos y en un contexto más amplio el respaldo al crecimiento económico.

III) Marco Jurídico.

En este apartado, como ya se ha indicado anteriormente, se irán destacando los aspectos más relevantes de la normativa que afecta al C.E., sin ánimo de ser exhaustivos y entrar al mínimo detalle.

A) Protección de Consumidores.

Este apartado es vital para que el C.E. se desarrolle y se implante, como consecuencia de la necesidad de crear la confianza en esta práctica, a la que ya se aludió anteriormente. Aparte de una serie de directivas ya creadas para la protección, con carácter general, de los consumidores y de la salud pública[42], se ve la necesidad de incentivar la resolución de litigios en línea y otros procedimientos de protección como la autorregulación, la corregulación y dar directrices para elaborar códigos de conducta.

Como señala la Resolución del Consejo de 19 de enero de 1999 sobre la dimensión de los consumidores en la S.I.[43], para instaurar esa confianza, es necesario que exista un nivel de protección equivalente al que rige en las transacciones tradicionales, aplicándose a los nuevos productos y servicios los principios vigentes en materia de política de consumidores y en especial: a recibir información suficiente, a una protección contra prácticas comerciales no solicitadas incluida la publicidad, a la distribución equitativa de riesgos y responsabilidades y a la protección de la salud, la intimidad, los datos personales y la seguridad.

Por otro lado, para fomentar la autorregulación y los códigos de conducta, se lanzó en mayo de 2000 la iniciativa eConfidence, la cual pretende unir a los empresarios, los consumidores y la Comisión, para que juntos fijen códigos de conducta y buenas prácticas y den directrices de comportamiento.

Por lo que respecta a la resolución extrajudicial de litigios, no olvidemos que algo que caracteriza al C.E. es su carácter transfronterizo. Por ello se necesitan procedimientos eficaces y baratos que protejan al consumidor en las compras de escaso valor monetario. Para ello, baste citar la Resolución del Consejo de 25 de

[42] La Directiva 2000/31 de C.E. enumera una serie de directivas que seguirán manteniendo el mismo nivel de protección anterior a la entrada en vigor de ésta. La lista se dará en el siguiente capítulo cuando se estudie la citada Directiva.
[43] DOC 23 de 28 de enero de 1999.

mayo de 2000 sobre una red comunitaria de órganos nacionales responsables de la solución extrajudicial de litigios en materia de consumo[44], que alienta a los Estados a que fomenten las actividades de solución extrajudicial de conflictos en transacciones transfronterizas, sobre la base del domicilio del deudor que regulan, como regla general, los convenios de Roma y Bruselas[45], o la Recomendación de la Comisión de 4 de abril de 2001 relativa a los principios aplicables a los órganos extrajudiciales de resolución consensual de litigios en materia de consumo[46], que trata de ir mas allá de la Recomendación 98/257/CE[47], que sólo cubre la resolución de litigios por un tercero y no los procedimientos en los que se intenta acercar a las partes para alcanzar un mutuo acuerdo. Igualmente cita los principios que deben regir en estos órganos, los cuales son: imparcialidad, transparencia, eficacia y equidad.

Por último, la Comisión Europea ha creado una Red Extrajudicial Europea[48], que funciona de la manera siguiente: el consumidor tendría un único punto de contacto en su Estado para obtener información sobre los sistemas de resolución extrajudicial en los E.E.M.M. y, en su caso, facilitar un acceso sencillo y rápido a un sistema de solución extrajudicial en el país del proveedor o poner en contacto al consumidor con el punto de contacto del país del proveedor[49].

B) Protección de Datos.

El marco jurídico aplicable a la protección de datos es el recogido en la legislación general sobre la materia, que será de total aplicación a los servicios de la S.I.[50].

De esta manera es de aplicación la Directiva 1995/46/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 sus datos personales y la libre circulación de esos datos[51], en las condiciones que se dirán a continuación, y el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000[52] sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y los Organismos de la Comunidad y sobre la libre circulación de esos datos. El Reglamento se ocupa del

[44] DOC 155 de 6 de junio de 2000.
[45] Hoy sustituido por el Reglamento 44/2001 del Consejo de 22 de diciembre de 2000 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. DOL 12 de 16.1.2001.
[46] DOL 109 de 19 de abril de 2001.
[47] De 30 de marzo relativa a los principios aplicables a los órganos responsables de la solución extrajudicial de los litigios en materia de consumo, DOL 115 de 17 de abril de 1998.
[48] Para más información, véase documento de trabajo Sec (2000) 405 y: http://www.eejnet.org/
[49] En todo caso sería similar a la creada Fin-net: *financial services complaints network*, que resuelve los litigios en materia de servicios financieros. Para más información, véase la Comunicación sobre el C.E. y los servicios financieros, Com. (2001) 66 final.
[50] Véase considerando 14 de la Directiva 2000/31/CE. Para su correcta citación, véase nota 3.
[51] DOL 281 de 23 de noviembre de 1995.
[52] DOL 8 de 12 de enero de 2001.

tratamiento de datos personales por parte de Instituciones y Organismos Comunitarios, ya que éstos no entraban en el ámbito de la Directiva 1995/46/CE.

Pero la norma más importante para el C.E. es la recientemente aprobada Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002[53], relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas)[54], que viene a derogar a la Directiva 1997/66/CE[55], ya que se necesita un marco jurídico neutro y flexible que no se vea obsoleto por el desarrollo tecnológico, como ha sido el caso; y por ello lo primero que se hace es cambiar el término telecomunicaciones por el de comunicaciones electrónicas, concepto mucho más amplio, neutro y flexible.

La relación de ésta con la Directiva 1995/46/CE, antes aludida, se produce en el artículo 1.2, según el cual: "las disposiciones de la presente Directiva especifican y completan la Directiva 1995/46/CE a los efectos mencionados en el apartado 1"[56], es decir, en el de las comunicaciones electrónicas. Eso sí, atendiendo al artículo 3.1, la prestación de comunicaciones electrónicas sujeta a la Directiva, se entenderá para las que se presten al público en las redes públicas de comunicaciones de la Comunidad, con lo que se excluyen las comunicaciones electrónicas privadas, que utilicen líneas privadas.

Un supuesto de exclusión del ámbito de aplicación de la Directiva digno de destacar, viendo las noticias aparecidas en los medios de comunicación sobre la existencia de un borrador no publicado de Decisión Marco, que empezó a fraguarse en Presidencia Belga, se recoge en el artículo 1.3, para las actividades no comprendidas en el Tratado Constitutivo de la Comunidad Europea, como las reguladas por disposiciones de los Títulos V[57] y VI[58] del TUE, ni en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa y la

[53] DOL 201 de 31 de julio de 2002.

[54] Es la única directiva que faltaba por aprobar del denominado paquete Telecom que impulsó el Consejo Europeo de Lisboa de marzo de 2000 (Bol. 3-2000 punto 1.6). Las restantes son: Directiva 2002/19/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados y a su interconexión (directiva acceso), Directiva 2002/20/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (directiva autorización), Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (directiva marco), y Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (directiva servicio universal). Todas ellas publicadas en DOL 108 de 24 de abril de 2002. Posteriormente la Comisión ha distado la Directiva 2002/77/CE de la Comisión de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas DOL 249 de 17.09.2002, para adaptarse al nuevo marco regulador creado por las Directivas anteriormente mencionadas. En España todas estas Directivas van a ser Transpuestas al ordenamiento jurídico por la futura ley General de Telecomunicaciones, actualmente en trámite parlamentario.

[55] Del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. DOL 24 de 30 de enero de 1998.

[56] Además, el artículo 15 recoge la aplicación de determinadas disposiciones de la Directiva 95/46/CE.

[57] Política Exterior y de Seguridad Común.

[58] Espacio de Libertad, Seguridad y Justicia.

seguridad del Estado y las actividades del Estado en materia penal[59] (similar disposición recoge la Directiva 1995/46/CE). Es por ello que, a pesar de la polémica que suscitará, este autor no ve contradicción entre la "futura norma" y la Directiva, salvo en lo que pudiera referirse a datos de tráfico, que la Directiva regula en su artículo 6, según el cual, sólo podrán tratarse los datos necesarios a efectos de facturación, el tiempo que transcurra hasta la expiración del plazo en que pueda impugnarse legalmente la factura o exigirse su pago.

En cuanto a la seguridad, el artículo 4 impone al proveedor de un servicio de comunicaciones electrónicas disponible al público garantizarla a un nivel adecuado al riesgo existente. En caso de riesgo particular tiene el deber de notificarlo al abonado.

Cuestión destacable por su relevancia en la materia, es el supuesto regulado en el artículo 5.3, referente a la confidencialidad de las comunicaciones. En virtud de éste, los E.E.M.M. velarán porque sólo se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario, con la condición de que se facilite a dicho usuario información clara y concreta, en particular sobre los fines de tratamiento de los datos con arreglo a la Directiva 95/46/CE y que éste usuario o abonado siempre pueda negarse al tratamiento, salvo que éste se utilice únicamente para efectuar o facilitar una comunicación a través de una red de comunicaciones electrónicas o sea necesaria para facilitar un servicio expresamente solicitado a la empresa por el usuario o abonado. En lo que está pensando la Directiva, es en aquellos dispositivos ocultos que se introducen en el terminal de comunicaciones para acceder a información, archivar información oculta o rastrear las actividades del usuario (observar qué *Webs* visita para averiguar cuáles son sus gustos y preferencias comerciales...). También detectan la dirección de nuestro ordenador o IP[60]. Éstos, sólo podrán ser utilizados para fines legítimos y previo conocimiento del usuario, con lo que los denominados chivatos o *cookies* que tengan fines legítimos, como

[59] Con lo que la intención de la Presidencia Danesa del Consejo de formalizar una Decisión Marco que, de prosperar en los términos previstos, obligará a las empresas de telecomunicaciones y ISP a crear un registro de llamadas, correos electrónicos y visitas a *Web*, el cual debe contener los datos necesarios para identificar al emisor, destinatario, hora e identificación del dispositivo de comunicación, por un periodo de 12 a 24 meses, que podrá ser consultado por la policía con autorización judicial para la lista de delitos incluidos en el artículo 3.4 del borrador. Como se verá en el tercer capítulo la LSSI contiene un precepto similar. El borrador no publicado está disponible, junto con otra información útil sobre la propuesta, en la *Web* de la Organización de defensa de los derechos civiles Statewatch, que es la que ha denunciado el asunto. La dirección de consulta es: www.statewatch.org/news/2002/aug/05datafd2.htm. Véase igualmente Diario ABC de 21 de agosto de 2002, página 21, y Diario ABC de 25 de Agosto de 2002, página 29. Al final esta cuestión parece que va a resolverse por el recientemente creado Proyecto Europeo Sherlock Homes que permitirá identificar y recopilar pruebas electrónicas a través del rastro que dejan los correos y ficheros en la red. Para ello se fijarán unas pautas metodológicas comunes de guarda y conservación de esos rastros. Para más información, véase IP/03/1443.

[60] La IP puede ser ocultada a través de un programa denominado "anonimizador", que impide a la Web de destino obtener nuestra IP, aunque el uso de estos programas puede acarrear algunos inconvenientes, como no ver la Web correctamente. Para más información, véase ABC "Tecnología" de 20.11.2002.

analizar la efectividad del diseño y la publicidad de una *Web* o para verificar la identidad de un abonado en una transacción en línea, deberán ser autorizados.

Pero sin duda lo más relevante de esta Directiva para el C.E. es el artículo 13 que regula las comunicaciones electrónicas no solicitadas[61], fenómeno conocido como *spam*, que al incluir entre sus supuestos al correo electrónico, creemos será desarrollado mejor en el siguiente capítulo, conjuntamente con la Directiva en cuestión.

Entrando a continuación a analizar la Directiva 1995/46/CE, debemos comenzar indicando que el interés de las Instituciones Comunitarias por regular esta materia, radica en la preocupación de que las diferencias en el nivel de protección de los derechos y libertades de las personas y en particular, el derecho a la intimidad, impida la libre circulación de esos datos por los distintos E.E.M.M., obstaculizando así el desarrollo del Mercado Interior (Considerando 7).

De esta manera, podemos indicar ya que el objeto de la Directiva es garantizar por parte de los E.E.M.M. la protección de los derechos fundamentales y las libertades públicas de las personas físicas, y en particular el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales[62], no pudiendo establecerse ninguna restricción a la libre circulación de esos datos por el territorio comunitario.

La Directiva se aplica tanto al tratamiento de datos personales, ya sea parcial, o totalmente automatizado, así como al tratamiento no automatizado[63] de datos personales contenidos o destinados a un fichero[64], por lo que ya avisamos al lector, que esta materia, aunque incide directamente en el C.E., puesto que siempre se piden una serie de datos de carácter personal, previo a la contratación electrónica, es de aplicación a cualquier actividad empresarial o profesional, pública o privada, en la que se utilicen datos de carácter personal. Y es en este momento cuando podemos reflexionar en voz alta, preguntándonos que actividad no está exenta de esta normativa, ya que no se nos ocurre, a *grosso modo*, algún negocio que no cuente por lo menos, con un fichero de clientes. La única excepción a lo mencionado en las líneas anteriores, es el supuesto de una persona física que utilice

[61] También reguladas en la Directiva 2000/31/CE de C.E. en su artículo 7.

[62] Atendiendo al artículo segundo, entendemos por dato de carácter personal: "toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". Se entiende por tratamiento de datos de carácter personal: "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

[63] Por ejemplo un fichero en soporte papel.

[64] Entendemos por fichero, atendiendo al artículo 2 c.): "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

datos de carácter personal para fines exclusivamente personales o domésticos. En nuestra opinión, esta excepción debe entenderse en el sentido más estricto posible, poniendo el acento a la hora de delimitar que es o que no es uso de carácter personal o domestico, en el uso y la finalidad que se dé por parte de esta persona a esos datos.

En otro orden de cosas, la Directiva intenta delimitar cuando se aplica la legislación nacional de cada E.E.M.M., en lo que respecta a la libre circulación de datos de carácter personal por el territorio de la Comunidad. Para ello establece una serie de reglas que son las siguientes:

- Si el tratamiento es efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento[65] en el territorio del E.E.M.M, se entenderá sometido a la legislación de ese Estado. Si el responsable del tratamiento está establecido en el territorio de varios estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de esos establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable.
- Si el responsable del tratamiento no está establecido en el territorio del E.E.M.M., sino en el lugar en el que se aplica su legislación nacional en virtud del Derecho internacional público, se aplicará la legislación de ese Tercer Estado.
- El responsable del tratamiento no está establecido en el territorio de la Comunidad y recurre, para el tratamiento de datos personales a medios, automatizados o no, situados en el territorio del E.E.M.M., salvo en el supuesto de que dichos medios se utilicen sólo con fines de tránsito por el territorio de la Comunidad. En este supuesto, el responsable del tratamiento deberá nombrar a un representante establecido en algún E.E.M.M..

La Directiva establece una serie de principios y normas que deben inspirar a las legislaciones de los E.E.M.M. que regulen la protección de datos. Estos principios afectan, entre otros, a la calidad de los datos, el deber de recabar el consentimiento del afectado, deber de establecer un régimen especial de protección para determinados datos, deber de informar al interesado, deber de establecer en cada E.E.M.M., al menos, una autoridad de control[66], deber de notificar a la autoridad de control del E.E.M.M. sobre la existencia, uso y finalidades de ese tratamiento etc., en los cuales no vamos a entrar. No obstante estos principios y normas serán

[65] Atendiendo al artículo 2 d), entendemos por este: "la persona física o jurídica, autoridad publica, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el derecho nacional o comunitario".

[66] La lista completa de autoridades de control nacionales se encuentra en la dirección de la Comisión siguiente: http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm

analizados con posterioridad cuando se analice la legislación española de transposición de esta Directiva.

En lo que sí vamos a entrar, aunque sea sólo desde la perspectiva de las competencias de la Comisión, es en las transferencias internacionales de datos. Atendiendo al artículo 25 de la Directiva, estas sólo podrán ser autorizadas por un E.E.M.M., cuando el país tercero al que se transfieran los datos, cuente con un nivel de protección adecuado. Esta disposición, conlleva la obligación para los E.E.M.M. y la Comisión, de informarse recíprocamente cuando constaten que un tercer país no dispone de un nivel de protección adecuado. Es más, la Comisión puede en el ejercicio de sus competencias decidir si un país tiene o no, ese nivel adecuado de protección[67]. También se encuentra habilitada para alcanzar acuerdos internacionales con esos estados[68]. En caso de que dictamine desfavorablemente, los E.E.M.M. vienen obligados a tomar todas las medidas necesarias para impedir la transferencia a ese tercer país, salvo que puedan acogerse a alguna de las excepciones previstas en la Directiva.

También la Comisión, en virtud del artículo 26.4, puede considerar que determinadas cláusulas contractuales tipo, ofrecen garantías suficientes para este tipo de transferencias. Para dar cumplimiento a esta disposición, la Comisión ha dictado dos decisiones: la Decisión 2001/497/CE de 15 de junio de 2001 de la Comisión, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE[69], y otra específica para el supuesto que exista un encargado de tratamiento[70]; nos estamos refiriendo a la Decisión 2002/16/CE de 27 de diciembre, de la Comisión, relativa a cláusulas contractuales tipo para la transferencia de datos personales a los encargados de tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE[71]. En virtud de estas Decisiones, se considera que las cláusulas contractuales tipo recogidas en los anexos, cumplen con las garantías relativas a la

[67] Ejerciendo esta competencia y por poner sólo un ejemplo, la Comisión acaba de reconocer que Argentina ofrece un nivel adecuado de protección. IP/03/932. El resto de Decisiones pueden consultarse en la Web de la Dirección General del Mercado Interior de la Comisión Europea:: http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm.

[68] Cabe destacar el acuerdo alcanzado con el Departamento de Comercio de Estados Unidos el 31 de mayo de 2000, denominado Declaración de Puerto Seguro (safe harbour), a través de la Decisión de la Comisión de 26 de julio de 2000. En virtud de este acuerdo, se extenderá un certificado por empresa o sector (por el momento los servicios financieros se encuentran excluidos), indicando que cumplen con todos los principios sobre la normativa de protección de datos, evitando así tener que solicitar una autorización para cada transferencia. En aras de la transparencia, estas empresas estarán sometidas al control de la autoridad estadounidense competente según el sector. Para más información, véase Aparicio Salom "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal" Aranzadi, Pamplona 2ª edición 2002, páginas 223 y ss. También puede consultarse la siguiente dirección de la Dirección General del Mercado Interior (Comisión Europea): http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm

[69] DOL 181 de 4.7.2001

[70] De momento no vamos a analizar en detalle esta figura, sólo daremos la definición que se recoge en el artículo 2 e) de la Directiva: "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 de tratamiento".

[71] DOL 6 de 10.1.2002.

protección otorgada a los particulares por la normativa europea sobre protección de datos. Es por ello que ante la existencia de un supuesto de transferencia internacional de datos a un país tercero, recomendamos la inclusión de estas cláusulas, a los efectos de conferir apariencia de legalidad a esa transferencia en sí, evitando así la amenaza de imposición de sanciones, que como se verá cuando se estudie la legislación española, son muy elevadas.

Finalizaremos este apartado indicando que la Comisión estará asistida en las competencias atribuidas por esta Directiva, por un Grupo de Protección de las personas en lo que respecta al tratamiento de datos personales y un Comité. Las competencias y funciones de cada órgano, se encuentran también recogidas en el articulado de la Directiva, por lo que no entraremos a analizar esas funciones y cometidos.

C) Contratación a Distancia.

1º- La Directiva 1997/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia[72].
Lo primero que vamos a tratar, en lo que a esta norma se refiere, es la justificación de su aplicación al C.E., y la encontramos en el artículo 13.1 según el cual, ésta se aplicará en la medida en que no existan en la normativa comunitaria, disposiciones particulares que regulen determinados tipos de contratos a distancia en su globalidad. En caso de contradicción en un punto en particular, se resolverá aplicando las disposiciones de la normativa específica, artículo 13.2[73]. A modo de ejemplo el artículo 4 de la Directiva, que regula la información exigible antes de realizar un pedido, no se aplicaría, si la Directiva 2000/31/CE que regula en su artículo 10 la misma materia, no hiciera la salvedad de que estos requisitos de información podrán completarse con otros existentes en otras disposiciones comunitarias.

Sólo se van a destacar algunos derechos recogidos, como el derecho de resolución, artículo 6, por el cual el consumidor en todo contrato negociado a distancia, dispondrá de un plazo de 7 días laborales para rescindir el contrato sin penalización alguna y sin tener que indicar los motivos. O la posibilidad de anular un pago fraudulento realizado mediante tarjeta de crédito, como recoge el artículo 8. Por último, cabe señalar que los consumidores no podrán renunciar a los derechos que se les reconocen en la presente Directiva, artículo 12.1.

[72] DOL 144 de 4 de junio de 1997.
[73] En esta misma línea, véase Pinochet Olave, Ruperto. “Contratos Electrónicos y Defensa del Consumidor” 2001 Marcial Pons. Páginas 165 y ss.

2º- La Directiva 2002/65/CE del Parlamento Europeo y del Consejo de 23 de septiembre de 2002, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, y por la que se modifican la Directiva 90/619/CEE del Consejo y las Directivas 97/7/CE y 98/27/CE[74].

Teniendo en cuenta que la Directiva 97/7/CE en su artículo 3.1 excluye de su ámbito de aplicación a los servicios financieros enumerados en la lista no exhaustiva que figura en el Anexo II de la Directiva, la Comisión Europea lanzó su propuesta[75]. El proceso de aprobación de esta Directiva fue largo y costoso, debido a la falta de acuerdo en cuanto al nivel de protección a aplicar a los consumidores, si de máximos o mínimos, lo que llegó incluso a provocar una mención expresa en el Consejo Europeo de Barcelona de 15 y 16 de marzo de 2002, que solicitó que se adoptara lo antes posible[76]. Idénticas dificultades que las que están sufriendo las propuestas de Directivas que faltan para completar el marco jurídico del C.E.[77].

Por dar algunas pinceladas sobre la regulación jurídica de la Directiva, comenzaremos mencionando que otorga una protección de máximos a los consumidores, debido a la regulación que a lo largo de su articulado se recoge. Cabría destacar que el derecho de rescisión por parte del consumidor se eleva, con carácter general, de 7 a 14 días, se aumentan las exigencias de información previa a la celebración del contrato, se regulan las comunicaciones no solicitadas y la gran novedad de esta Directiva, los servicios no solicitados, según el cual, el silencio del consumidor no es equivalente a consentimiento.

D) Derechos de Autor.

En materia de derechos de autor tenemos como principal exponente la Directiva 2001/29/CE del Parlamento Europeo y del Consejo de 22 de mayo de 2001[78], relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.

En este ámbito, la U.E. ha ido publicando una serie de Directivas sectoriales que, salvo las excepciones del artículo 11, quedarán intactas (artículo 2). Además la presente Directiva se basa en principios y normas ya fijados por las normas que

[60] DOL 271 de 9.10.2002.
[75] Com. (1998) 468 final. Posteriormente modificada por el documento Com. (1999) 385 final y la última en recientes fechas Com. (2002) 360 final de 26 de junio de 2002.
[76] Véase Conclusiones de la Presidencia del Consejo Europeo de Barcelona, punto 35.
[77] Estas son las propuestas de directivas que abren la contratación pública a la red. Fueron presentadas en el año 2000 y en 2002 han sido modificadas esas propuestas, por lo que no entraremos en ellas. Son la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la coordinación de los procedimientos de adjudicación de los contratos públicos de suministro, servicio y obras. Com. (2000) 275 final, modificado por Com. (2002) 236 final y Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la coordinación de los procedimientos de adjudicación de los contratos públicos en los sectores del agua, energía, transportes y telecomunicaciones. Com. (2000) 276 final, modificado por Com. (2002). 235 final.
[78] DOL 167 de 22 de junio de 2001.

veremos a continuación, que serán de aplicación, salvo disposición en contra de la presente Directiva[79]. Estas normas son las siguientes:

- Directiva 91/250/CEE del Consejo de 14 de mayo de 1991[80], relativa a la protección jurídica de programas de ordenador. Esta Directiva otorga a los creadores una protección como derechos de autor. Actualmente se está trabajando en otorgar protección sobre la base de la Propiedad Industrial y según la propuesta, ambas serían compatibles y complementarias[81].

- Directiva 92/100/CEE del Consejo de 19 de noviembre de 1992[82] sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en al ámbito de la propiedad intelectual.

- Directiva 93/83/CEE del Consejo de 27 de septiembre de 1993[83] sobre coordinación de determinadas disposiciones relativas a los derechos de autor y derechos afines a los derechos de autor en el ámbito de la radiodifusión vía satélite y de la distribución por cable.

- Directiva 93/98/CEE del Consejo de 29 de octubre de 1993[84] relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines.
- Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996[85] sobre la protección jurídica de bases de datos.

Además han de ejercerse los derechos regulados de acuerdo con el Convenio de la Unión de Berna para la protección de las obras literarias y artísticas de 9 de septiembre de 1886[86], el Tratado de la OMPI sobre derechos de autor y el Tratado de la OMPI sobre interpretación o ejecución de fotogramas, ambos firmados en Ginebra en 1996[87].

Volviendo a la Directiva 2001/29/CE, sólo cabe señalar que adapta la defensa de los derechos de autor y afines, esto es, derecho de reproducción, de comunicación al público de obras, de poner a disposición del público prestaciones protegidas y distribución, a las características de la S.I., ya que se utiliza una terminología

[79] Véase considerando 20.
[80] DOL 122 de 17 de mayo de 1991, modificada por Directiva 93/98/CEE.
[81] Véase páginas 8 y ss, de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la patentabilidad de las invenciones implementadas en ordenador Com. (2002) 92 final. Así la propiedad intelectual protege al autor en cuanto a los derechos de distribución y reproducción y la propiedad industrial protege a la idea a través de la patente con lo que la defensa es mayor y podría venderse o traspasarse como activo.
[82] DOL 346 de 27 de noviembre de 1992, modificada por Directiva 93/98/CE.
[83] DOL 248 de 6 de octubre de 1993.
[84] DOL 290 de 24 de noviembre de 1993.
[85] DOL 77 de 27 de marzo de 1996.
[86] BOE 81 de 4 de abril de 1974 y 260 de 30 de octubre de 1974.
[87] DOL 89 de 11 de abril de 2000.

adecuada, tal como, medios alámbricos e inalámbricos, medidas tecnológicas... quedando al margen de la Directiva dos cuestiones importantes: los derechos morales y la ley aplicable. En cuanto a los primeros, existía una total falta de acuerdo entre los Quince, a la hora de establecer la regulación en la materia, y en cuanto a los segundos, se consideró que era mejor continuar estudiando el tema[88], ya que el establecimiento de la ley aplicable plantea numerosos problemas según se opte por uno u otro sistema, ya sea el del país de carga *uploading* o el del país de descarga *downloading*, o soluciones combinadas, ya que si se aplica la regla del Convenio de Berna de proteger por la legislación del país en la que se produjo el daño, al ser Internet universal, tendríamos que ir reclamando país por país, en la proporción al daño sufrido en ese país. Otros miembros de la doctrina abogan por aplicar otros criterios, tales como, la ley del país del titular de los derechos patrimoniales, o la ley del país donde se reclama la protección, o la ley más protectora, o la del país donde radique el servidor.

No obstante, dado el carácter abierto y universal de la red, ponemos en duda la eficacia de la Directiva si en su transposición, al imponer a los E.E.M.M. que adopten las medidas necesarias para proteger los derechos allí recogidos, no se tiene en cuenta este carácter de universalidad y tampoco se consigue una flexibilidad que supere el desarrollo tecnológico. Baste poner como ejemplo la aplicación *P2P*, ya mencionada, que consiste en la creación de vínculos directos entre usuarios particulares y vendedores, o entre los propios usuarios, la cual es muy utilizada en el ámbito musical. Cuando alguien instala el programa, se crea automáticamente una carpeta con los ficheros que desea compartir. De esa manera, circulan por la red miles de ficheros, de otros tantos usuarios. Teniendo en cuenta que hasta ahora los Tribunales han declarado legales a las empresas que crean el *software*, pero sí puede ser ilegal el uso que de ellos hagan los usuarios, o lo que es lo mismo, se permite la copia privada de la obra, por parte del que la haya adquirido legalmente, para su uso personal, pero no la comercialización de esa copia. Es por ello, que se hace imposible el control de éstas, por parte de la policía[89]. El problema ha llegado a ser tan sangrante para las compañías discográficas y de *software* que ha llevado a estas últimas a presentar una denuncia ante la Policía española, para que se investigue a unos 95.000 usuarios de Internet, sospechosos de copiar archivos en las redes *P2P* . La identificación de estos usuarios ha sido posible gracias a un potente programa informático que permite rastrear la red e identificar a esas personas[90]. En nuestra opinión, la batalla legal debe ir contra las compañías que diseñan esos programas de intercambio de archivos, ya que incurren, en nuestra opinión, en un fraude de ley ya que para evitar que se actué contra ellas, participan como meros intermediarios de la operación, ya que ponen en contacto a los usuarios que desean compartir ficheros, es decir en

[88] Para más información, véase Garrote Fernández-Díez, Ignacio. El Derecho de Autor en Internet. Páginas 103 y ss.
[89] Véase en este sentido, diario ABC Tecnología de 1 de mayo de 2002, página 35.
[90] Para más información, véase Diario ABC Tecnología de 16.7.2003.

ningún caso comercializan y reproducen. La solución al problema, ni va a ser rápida, ni va a estar exenta de dificultades ni de opiniones en contra, aunque soluciones no faltan incluidas las tecnológicas. De este modo se han creado las *One Stop Shops* o ventanillas únicas, que contienen un listado con las obras disponibles, el nombre del titular de los derechos de autor y la cantidad estipulada en concepto de royalties. También cabe destacar el EMMS (*Electronic Music Management System*) o el *Secure Mp3,* aunque de momento estos sistemas provocan el rechazo de los usuarios que prefieren música gratis aunque la copia sea de peor calidad.

Finalizaremos este apartado mencionando que también pueden darse problemas si no existe una armonización internacional en la materia, ya que una obra distribuida por Internet a través de un país A con un elevado nivel de protección y descargada en un país B con un menor nivel, puede provocar que lo lícito en B sea ilícito en A. No obstante, a tenor de los principios establecidos en el centenario Convenio de Berna, podemos decir que existe un gran elemento de armonización y seguridad jurídica en lo que respecta a la protección de los derechos de autor, puesto que los principios aún siguen siendo válidos. Estos principios son los siguientes:

- Principio de trato nacional: la obra originaria de un país signatario del Convenio, tiene derecho a ser protegida en el resto de los países signatarios, con idénticas garantías que las que se ofrecen en sus legislaciones a los autores nacionales.
- Principio de independencia de la protección de la obra de un tercer país (no signatario del Convenio), si se publica en un país firmante del Convenio, gozará de toda la protección que otorga el Convenio.
- Principio de protección automática, sin necesidad de registrar previamente la obra. Ésta estará protegida, por el mero hecho de su creación.

E) Dinero electrónico.

Esta materia es otra de las relevantes para el desarrollo y la implantación del C.E.. Así para comprar en la red hace falta, como en cualquier actividad comercial, un medio de pago. Éste podría ser una tarjeta de crédito pero por razones de seguridad y confianza se están desarrollando otros medios como las tarjetas inteligentes, dinero a través de la memoria del ordenador o con arreglo a otras características que no se regulan en estas Directivas, el pago por teléfono móvil conocido como el móvil monedero[91].

Por este motivo se han aprobado dos Directivas en la materia. Por un lado tenemos la Directiva 2000/28/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000[92], por la que modifica la Directiva 2000/12/CE relativa al acceso a la actividad de las entidades de crédito y a su ejercicio. Esta Directiva se

[91] Sobre esta modalidad de pago, véase ABC de Economía de 28 de abril de 2002, página 11.
[92] DOL 275 de 27 de octubre de 2000.

limita a ampliar la definición de entidad de crédito contenida en el artículo 1 de la Directiva modificada[93], incluyendo a las entidades de dinero electrónico, que serán aquellas que están reguladas en la Directiva que estudiaremos a continuación.

La Directiva 2000/46/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000[94], sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión de cautelar de dichas entidades, viene como es lógico, a regular éstas en toda su amplitud. No obstante, para nosotros sólo son necesarias las precisiones que realizaré a continuación.

Por entidad de dinero electrónico ha de entenderse una empresa o cualquier otra persona jurídica distinta de una entidad de crédito, tal y como se define en la letra a) del párrafo primero del punto 1 del artículo 1 de la Directiva 2000/12/CE, que emita medios de pago en forma de dinero electrónico (artículo 1.3 a).

Por dinero electrónico, partiendo de la base de que se está pensando en pagos de cuantía limitada, se entenderá con arreglo al artículo 1.3 b):
Un valor monetario representado por un crédito exigible a su emisor,
i) almacenado en un soporte electrónico
ii) emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido
iii) aceptado como medio de pago por empresas distintas del emisor.

Hay que destacar el derecho de reembolso del portador del dinero electrónico, regulado en el artículo 3, según el cual, durante el periodo de validez del mismo, el portador podrá solicitarlo al emisor que deberá realizarlo en moneda y billetes de banco o por transferencia a una cuenta sin otros gastos que los necesarios para realizar la operación, con un límite mínimo de reembolso, de no más de 10 euros.

Sin animo de ser repetitivos, es preciso traer a colación una vez mas la neutralidad y flexibilidad para no obstaculizar la innovación tecnológica, de la cual se hace eco la Directiva[95].

F) Fiscalidad.

Llegados a este apartado, tenemos que romper el hilo conductor de esta exposición y afirmar que en esta materia, la regulación no corresponde a un interés, por parte de las Instituciones Comunitarias, de acelerar la implantación del C.E., sino muy por el contrario, la justificación de esta regulación radica en la preocupación de las Instituciones, por el no cumplimiento de las obligaciones fiscales, con el consiguiente perjuicio a las arcas públicas, especialmente en materia de IVA,

[93] Directiva 2000/12/CE del Parlamento Europeo y del Consejo de 20 de marzo de 2000 relativa al acceso a la actividad de las entidades de crédito y a su ejercicio, DOL 126 de 26 de mayo de 2000.
[94] DOL 275 de 27 de octubre de 2000.
[95] Considerando 5.

debido a la imposibilidad de control efectivo por estas, debido al carácter abierto y universal de la red que se ve agravado por el uso de productos digitalizados[96].

Así la ya mencionada Iniciativa europea de C.E.[97], en su página 28 se plantea estudiar si hay que modificar la normativa fiscal en la materia, bajo el principio de neutralidad (las consecuencias fiscales serán idénticas para bienes y servicios independientemente de que se suministre *on line/off line* y que se adquiera dentro o fuera de la U.E.) y rechaza de plano la creación de un impuesto sobre los *bits*[98].

Por su parte la Conferencia de Turku (Finlandia) de noviembre de 1997, dentro del marco de la OCDE, acordó que la tributación no puede ser un obstáculo al C.E., pero el desarrollo de éste no debe favorecer la inaplicación de normas fiscales. Fija a su vez unos principios rectores en esta materia que son los de equidad, simplicidad, seguridad, eficiencia, eficacia y proporcionalidad.

El siguiente paso hacía la regulación de la materia fue la Conferencia de Ottawa de octubre de 1998[99], que contiene las siguientes conclusiones: los actuales principios tributarios pueden y deben ser aplicados al C.E., no es necesario crear nuevas categorías tributarias, la mejor opción de gravamen del consumo es el lugar donde éste se produce y los productos digitalizados deben ser considerados como prestación de servicios.

Centrándonos a la normativa en vigor, tenemos que comenzar por la reforma operada en la VI Directiva IVA[100] por la Directiva 1999/59/CE del Consejo de 17 de junio de 1999[101]. Establece que, a efectos de IVA, se entenderá que los servicios

---

[96] Baste con poner un ejemplo: el contenido musical de los discos compactos se entrega en línea de un país A, a un país B, es decir no se envían bienes físicos que atraviesen las aduanas, sino que la música es descargada por el cliente. El país B no puede cobrar el IVA salvo que el consumidor declare voluntariamente. Además dejaría en clara desventaja competitiva a un proveedor del país B porque éste, si estaría obligado a repercutir el IVA en su país.

[97] Véase nota 10.

[98] El llamado *bit tax* gravaría el volumen de información transmitido. Esto iría en perjuicio de pequeñas transmisiones, las cuales, son muy numerosas y favorecería a las grandes transmisiones que no fueran muy numerosas. En este mismo sentido, véase Cazorla Prieto y Chico de la Cámara, "Los impuestos indirectos en el comercio electrónico" Aranzadi páginas 19 y ss.

[99] Para fijar la posición de la U.E. en esta Conferencia, la Comisión publicó la comunicación Comercio Electrónico y fiscalidad indirecta Com. (1998) 374 final. Fija tres principios rectores: seguridad, simplicidad y neutralidad, así como unas directrices en esta materia. Éstas son:

i) Ausencia de nuevos impuestos.

ii) La transmisión electrónica en tanto que servicio: La puesta a disposición de un usuario de un producto digitalizado es una prestación de servicios.

iii) Garantizar la neutralidad. Los servicios prestados por C.E. y destinados al consumo en la U.E., se gravaran en la U.E. independientemente de su origen, y viceversa, si el producto se exporta desde la U.E. y en ésta no está gravado, tiene derecho a deducción.

iv) Facilitar el cumplimiento de las obligaciones. Debe ser lo más fácil y simple posible para todos los operadores.

v) Garantizar el control y cumplimiento del impuesto.

vi) Facturación electrónica. Regularla en la normativa comunitaria y buscar armonización a nivel internacional.

[100] Directiva 77/388/CEE del Consejo de 17 de mayo de 1977, en materia de armonización de las legislaciones de los Estados Miembros relativas a los impuestos sobre el volumen de negocios –sistema común del impuesto sobre el valor añadido: base imponible uniforme -. DOL 145 de 13 de junio de 1977.

[101] Por la que se modifica la Directiva 77/388/CEE en lo que respecta al régimen del impuesto sobre el valor añadido aplicable a los servicios de telecomunicaciones. DOL 162 de 26.6.1999.

de radiodifusión, televisión y los servicios prestados por vía electrónica a partir de terceros países a personas establecidas en la Comunidad o a partir de la Comunidad a destinatarios establecidos en terceros países, deberían estar gravados en el lugar de establecimiento del destinatario de los servicios.

Para mejorar este sistema, recientemente se ha vuelto a modificar la VI Directiva IVA por medio de la Directiva 2002/38/CE del Consejo de 7 de mayo de 2002[102], según la cual, los proveedores de los servicios indicados anteriormente, que los presten a título oneroso a clientes establecidos en la Comunidad podrán acogerse a un régimen especial transitorio (de tres años a partir del 1 de julio de 2003), que grava el lugar de consumo.

Como complemento a esta Directiva, se aprobó el Reglamento (CE) Nº 792/2002 del Consejo de 7 de mayo de 2002[103], por el cual, los sujetos pasivos no establecidos en la Comunidad y sin obligación de identificarse podrán, si se acogen a este régimen especial, identificarse en un E.E.M.M., en el que cumplimentaran todas las obligaciones fiscales (declaración trimestral, liquidación...) y este Estado pasará la información al resto de E.E.M.M., así como el importe económico de la liquidación del impuesto al E.E.M.M. beneficiario de ésta.

Para finalizar nos referiremos a la Directiva 2002/115/CE del Consejo de 20 de diciembre de 2001[104]. En esta Directiva se viene a regular la factura electrónica, así como, los requisitos para su validez. Para ello, la factura electrónica podrá ser expedida por los sujetos pasivos, por un cliente (auto facturación)[105] o en su nombre y cuenta por un tercero (se piensa en una gestoría o empresa de similares características).

Los E.E.M.M. estarán obligados a aceptar estas facturas, siempre que esté asegurada la autenticidad de su origen y la integridad de su contenido, que deberán garantizarse durante todo el periodo de conservación de estas, bien a través de una firma electrónica avanzada con arreglo al apartado 2 del artículo 2 de la Directiva 1999/93/CE de firma electrónica (que será desarrollada en el siguiente capítulo), aunque sin embargo, podrá exigirse por parte de los E.E.M.M., que la firma electrónica avanzada esté basada en un certificado reconocido y la cree un

[102] Por la que se modifica y se modifica temporalmente la Directiva 77/388/CEE respecto del régimen del impuesto sobre el valor añadido aplicable a los servicios de radiodifusión y de televisión y a algunos servicios prestados por vía electrónica. DOL 128 de 15 de mayo de 2002. Esta Directiva ha sido incorporada al ordenamiento jurídico español por la ley 53/2002 de 30 de diciembre de 2002 de medidas fiscales, administrativas y del orden social, BOE 313 de 31 de diciembre de 2002.

[103] Por el que se modifica temporalmente el Reglamento (CEE) Nº 218/92 sobre cooperación administrativa en materia de impuestos indirectos (IVA), en cuanto a medidas adicionales relativas al comercio electrónico. DOL 128 de 15 de mayo de 2002.

[104] Por la que se modifica la Directiva 77/388/CEE con objeto de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el impuesto sobre el valor añadido. DOL 15 de 17 de enero de 2002.

[105] Para que ésta sea válida, tiene que existir un acuerdo previo entre las partes y a condición de que cada factura sea objeto de un procedimiento de aceptación por el sujeto pasivo que realiza la entrega de bienes o la prestación de servicio.

dispositivo seguro de creación de firmas con arreglo a los apartados 6 y 10 del artículo 2 de la mencionada Directiva o bien mediante un intercambio electrónico de datos (EDI), tal y como, se define en el artículo 2 de la Recomendación 1994/820/CE de la Comisión de 19 de octubre de 1994[106], relativa a los aspectos jurídicos del intercambio electrónico de datos, si en el acuerdo de intercambio se prevé la utilización de mecanismos que garanticen la autenticidad del origen y la integridad de datos, sin perjuicio de que los E.E.M.M. pueden exigir la presentación de un documento adicional recapitulativo en papel.

Acabaremos este apartado manifestando escepticismo ante la posibilidad de que las medidas expuestas puedan facilitar el cumplimiento de las obligaciones tributarias, tal y como, nos referíamos al principio. Los productos digitalizados, que como se indicó, no poseen soporte material y se descargan en un archivo son de difícil control, pero además teniendo en cuenta que para que exista obligación tributaria es necesaria la onerosidad, nos preguntamos ¿qué ocurre si una *Web* permite descargar archivos gratuitamente, ya que los ingresos los obtiene por la publicidad, cuya cuantía está basada en el número de personas que visita la página? ¿no está el usuario pagando por su visita, aunque él no satisfaga la prestación?. Se hace por tanto necesario una mención expresa, de similares características a la recogida en la LSSI, según la cual, el concepto de servicio de S.I. se entiende de manera amplia, al no ser requisito indispensable la remuneración del servicio, ya que basta simplemente con que represente una actividad económica al prestador de servicios.

G) Tecnologías de Seguridad de la Información.

En la búsqueda de crear una industria de las tecnologías de la seguridad de la información, como son la criptografía o la firma digital, la Unión Europea ha reformado el Reglamento sobre el control a la exportación de productos y tecnologías de doble uso[107], para facilitar su exportación[108]. Baste indicar que esta reforma era necesaria y no exenta de dificultades, ya que la criptografía y las técnicas de seguridad biométricas, como el reconocimiento del iris humano son susceptibles de aplicación militar o usos ilícitos, (por ejemplo, los terroristas podrían usar el cifrado en sus comunicaciones para hacerlas indetectables).

[106] DOL 338 de 28 de diciembre de 1994.

[107] Reglamento (CE) Nº 458/2001 del Consejo de 6 de marzo de 2001 por el que se modifica el Reglamento (CE) nº 1334/2000 con respecto a la lista de productos y tecnologías de doble uso cuando se exporten. DOL 65 de 7 de marzo de 2001 y DOL 159 de 30 de junio de 2000 (modificado por el Reglamento (CE) nº 2889/2000 DOL 336 de 30 de diciembre de 2000), respectivamente.

[108] En este sentido, el *Secure Socket Layer* (SSL), creado en 1994, es un sistema que encripta el mensaje entre el servidor *Web* y el usuario se vio frenado en su desarrollo durante mucho tiempo, debido a las restricciones a la exportación por parte de Estados Unidos. Este sistema adolecía de un inconveniente, sólo encripta la comunicación entre el comprador y el vendedor, dejando al descubierto al operador de la tarjeta de crédito. Por este motivo en 1995 VISA y Mastercard crearon el SET (*Secure Electrónic Transaction*). Que aporta autenticidad a las tres partes.

H) Comercio Electrónico y Derecho de la Competencia.

En este apartado, nos dedicaremos sólo a resaltar algunos de los problemas que, en relación con el Derecho de la Competencia, está provocando el C.E.

En este sentido, el Derecho de la Competencia viene regulado en los artículos 81 y ss del TCE, en cuyo contenido no vamos a detenernos.

El primer problema destacable que pudiera plantearse, sería en relación con la libre prestación de servicios. Se entiende que la competencia se vería falseada si las posibilidades que ofrece el C.E., sólo están disponibles a determinados operadores, por ello se necesitaba un entorno abierto y competitivo que fue resuelto por la Directiva 2000/31/CE, al regular esta libertad en su artículo 4, estableciendo el principio de no autorización previa.

De igual forma, el C.E. está obligando, en lo que respecta a este sector, a cambiar la noción de "mercado relevante". Así se tiene que determinar el contenido y la extensión de mercado relevante, en cuanto al mercado del producto y al mercado geográfico. Por el primero ha de entenderse, él de productos idénticos y considerados por los destinatarios finales como intercambiables, teniendo en cuenta sus características, precio y uso. Por ello se plantea si los productos ofrecidos por Internet son sustitutivos de los ofrecidos por los canales tradicionales. La Comisión Europea ha tenido que actuar en este ámbito, en la investigación preliminar del asunto de la empresa de viajes que querían crear las empresas T-online, TUI y Neckermann para la venta de viajes en línea. Se consideró a éste, como un mercado en toda regla distinto al de las agencias de viaje tradicionales, ya que extiende, a cualquier hora del día, el horario de compra y ofrece precios más baratos[109]. En esta misma línea, se entiende que los productos digitalizados constituyen un mercado propio.

En cuanto al mercado geográfico, sólo baste remitirnos a lo ya mencionado, Internet carece de barreras físicas y el comercio no entiende de fronteras, se mueve en un entorno globalizado.

Problemática diferente es la ocasionada a raíz de las plataformas *B2B,* ya mencionadas, ya que podría vulnerar el TCE en cuanto a la agrupación de empresas, acuerdos entre empresas o prohibición de cártel.

La Comisión Europea en este sentido, ve las dos caras de la moneda, la primera por las razones expuestas y la segunda porque como reconoce ella misma[110], estas plataformas benefician a la competencia en cuanto que mejoran la transparencia del mercado, favorecen la bajada de precios y una mayor integración de los mercados geográficos distintos y mejora los modelos de negocios de las empresas (cuestión

[109] Unión Europea. Noticia de prensa IP/01/338 de 14 de junio de 2001.
[110] Véase XXX Informe sobre la Competencia 2000, página 70.

ya expuesta en la primera parte del capítulo) y que, por mucho que la empresa matriz creadora de la Puntocom tenga una posición dominante en el mercado tradicional, en el virtual está todo por hacer, y conseguir, como la confianza del consumidor, y de lo único que podría beneficiarse, es de la imagen que otorga la marca y del nombre conseguido por los años de operar en el mercado tradicional.

Es por ello que en algunas ocasiones ha aceptado la operación y en otros no. Baste para finalizar poner algunos ejemplos en cada caso.

Por el lado de las autorizaciones cabe destacar el caso de MyAircraft.com[111], creada por United Technologies Corp. Y Honeywell International Inc para la venta de productos y servicios aéreo espaciales. Se consideró que las alternativas en este sector son posibles y que en el sector hay o habrá otros operadores, con lo que la competencia será posible.

Otros casos afirmativos fueron: Emaro.com, creada por Deutsche Bank y Software Company SAP, para el suministro de material de oficina[112], el ejemplo de Cártel de empresas Volbroker.com, creado por los 6 grandes bancos para las opciones sobre divisa extranjeras[113], entre otros[114].

Por el lado de las denegaciones, sólo voy a citar el asunto del intento de unión, en febrero de 2000 de Ford, General Motors, Chrysler, Renault, Nissan, Oracle y i2, para la creación de un único portal de intercambio de suministro. La Comisión Europea, no concedió la carta de conformidad[115], ya que consideró que esta unión otorgaba a las partes un enorme poder sobre otros suministradores[116].

Pero también se puede vulnerar el Derecho de la Competencia Comunitario, desde una perspectiva de las nuevas tecnologías, pero con procedimientos tradicionales, como ha ocurrido recientemente con la imposición de una multa a Wanadoo por abuso de posición de dominio[117] de 10,35 millones de euros. La Comisión ha detectado que Wanadoo (poseída en un 72% por el operador France Telecom.) bajó los precios de conexión a banda ancha a través de su servicio ADSL, de manera que impedía la competencia de otras empresas en este sector. Aunque Wanadoo sufrió perdidas cuantiosas, fueron amortizadas por un aumento de los ingresos en la empresa matriz France Telecom., por lo que la Comisión no ha tenido dudas a la hora de calificar esa conducta como abuso de posición de dominio conforme al artículo 82.a del TCE, que prohíbe imponer directa o indirectamente precios de compra, de venta u otras condiciones de transacción no equitativas.

[111] M.1969 – UCT/Honeywell/i2/MyAircraft.com
[112] M.2027 – Deutsche Bank/SAP/JV.
[113] 38.866 – Volbroker (Deutdche Bank/UBS/Goldman Sachs/Citibank/JP Morgan/Natwest.).
[114] Para más información, véase página 70 del Informe citado en nota 81.
[115] 38.064 – Covisint (GM, Ford, DaimlerChrysler, Renault, Nissan).
[116] Para más información en este sentido, véase Computers&Law, december 2000/ january 2001 volume II, issue 5, páginas 24 y ss. "Is the EU Competition Law the limit for the Internet?".
[117] IP/03/1025.

Para finalizar mencionaremos el recientemente aprobado Reglamento (CE) nº 1400/2002 de la Comisión de 31 de julio de 2002, relativo a la aplicación del apartado 3 del artículo 81 del TCE a determinadas categorías de acuerdos verticales y prácticas concertadas en el sector de los vehículos de motor, DOL 203 de 1.8.2002, en virtud del cual, el derecho regulado en el presente Reglamento de todo distribuidor a vender vehículos de motor nuevos o recambios y el derecho de un taller autorizado a vender servicios de reparación o mantenimiento, incluye el derecho a utilizar Internet o sitios de referencia de Internet.

I) Seguridad de Redes.

Adentrándonos en el estudio de esta materia, tenemos que distinguir dos aspectos bien diferenciados, por un lado tendríamos los aspectos de confidencialidad de la información así como su integridad y autenticidad y por el otro tendríamos todo lo referente a los delitos del ciber espacio en sus distintas modalidades, como pornografía, ataques a sistemas informáticos, protección de menores...

i) Comenzando por el primer aspecto, y mencionando que dejaremos la F.E., como ya se indicó, para el siguiente capítulo, expondré que el primer intento claro de establecer una seguridad en redes, es a través del EDI[118]. El EDI es un sistema de intercambio electrónico de datos, que a diferencia de Internet se realiza por redes privadas de comunicación, como la red SWIFT, utilizada por las entidades financieras para el intercambio electrónico de datos de las transferencias bancarias. El primer documento sobre este sistema, lo constituye una Comunicación de la Comisión sobre la transmisión electrónica de datos comerciales mediante las redes de comunicación TEDIS y una propuesta de Reglamento del Consejo por el que se establece la fase preparatoria de un programa comunitario relativo a la transferencia electrónica de datos de uso comercial utilizando las redes de comunicación TEDIS[119]. Al final ésta no prosperó y el citado programa comunitario fue aprobado por una Decisión del Consejo[120]. Esta Decisión se justificaba ante la ausencia de normas comunes en interoperabilidad y normalización de los sistemas. A tal fin se dotaba de una carga financiera al programa[121], para coordinar a nivel comunitario los trabajos realizados por los E.E.M.M. en esta materia, sensibilizar a los potenciales usuarios y productores, buscar soluciones a los problemas jurídicos, estudiar las necesidades de estos sistemas en materia de seguridad a fin de

[118] Queremos justificar primeramente que la regulación del EDI, a través de las diferentes Decisiones del Consejo, trata de potenciar el desarrollo de una red de intercambio electrónico de datos en su globalidad, muy a la imagen y semejanza del programa eEurope, con lo que podría haberse explicado como antecedente a este programa. No obstante observamos que se incide más en ámbitos de seguridad, normalización e interoperabilidad por lo que serán tratados en este apartado.

[119] Com. (1986) 662 final.

[120] Decisión del Consejo 1987/499/CEE de 5 de octubre de 1987 por la que se establece un programa comunitario relativo a la transferencia electrónica de datos de uso comercial utilizando las redes de comunicación TEDIS. DOL 285 de 8 de octubre de 1987.

[121] 5,3 millones de Ecus.

garantizar la confidencialidad de los mensajes, ayudar a las PYME con proyectos piloto...

La siguiente Decisión en la materia[122], es la Decisión 1991/385/CEE del Consejo de 22 julio de 1991 por la que se establece la segunda fase del programa TEDIS[123]. El objetivo no será otro en ésta ocasión, que la creación de los sistemas de intercambio electrónico de datos se realice de la mejor manera posible, para ello se actuará en la normalización, necesidades específicas del EDI en materia de telecomunicaciones, aspectos jurídicos del EDI, seguridad de los mensajes, impacto en empresas y campañas de sensibilización, entre otros[124].
Al tratarse de dos programas ya finalizados no vamos a entrar en la valoración de los resultados de los mismos[125].

Para finalizar nos referiremos brevemente a la Recomendación de la Comisión 1994/820/CE de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos[126], en la cual, la Comisión insta a los agentes económicos y organizaciones que usan el EDI en sus intercambios comerciales, a que utilicen el Modelo Europeo de Acuerdo de EDI (que fija unas normas contractuales a las que las partes pueden someterse voluntariamente) y las correspondientes observaciones que figuran en el Anejo de la Recomendación[127]

Otro programa específico fue el de la Decisión 1992/242/CEE del Consejo de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información[128], por la que se adoptó una acción por 24 meses, en el ámbito de la seguridad de los sistemas de la información que incluía el desarrollo de estrategias globales para la seguridad de estos sistemas, como la definición de las necesidades de usuarios y prestadores de servicios en esta materia y elaboración en el medio y corto plazo de soluciones para estas necesidades, desarrollo de la normalización, certificación y evaluación en la materia, así como favorecer innovaciones técnicas en seguridad.

Más reciente es la Comunicación de la Comisión sobre seguridad de las redes y de la información: Propuesta para un enfoque político europeo[129]. Se justifica su publicación en base a que la seguridad de las redes electrónicas y de los sistemas de

[122] Con la salvedad de que por la Decisión 1989/241/CEE del Consejo de 5 de abril de 1989, que modifica a la Decisión 1987/499/CEE por la que se establece un programa comunitario relativo a la transferencia electrónica de datos de uso comercial utilizando las redes de comunicación TEDIS. DOL. 97 de 11 de abril de 1989, por la que se abre el programa a los países terceros de la Comunidad.
[123] DOL 208 de 30 de julio de 1991.
[124] Para ello se aportaron 25 millones de Ecus.
[125] No obstante, facilitamos el siguiente documento donde si se recoge esta valoración: Comunicación de la Comisión sobre la evaluación del programa de sistemas de intercambio electrónico de datos comerciales (TEDIS). Com. (1997) 335 final.
[126] DOL 338 de 28 de Diciembre de 1994.
[127] En este Anejo, se regula todo aquello que pudiera afectar a un intercambio de datos utilizando el EDI, con vistas a eliminar la inseguridad jurídica, en aspectos tales como, la definición del EDI y mensaje de EDI, validez y formación del contrato, acuse del mensaje, valor probatorio del mensaje, seguridad, confidencialidad...
[128] DOC 123 de 8 de mayo de 1992.
[129] Com. (2001) 298 final.

información, suscita cada vez más preocupación, en paralelo al rápido aumento del número de usuarios y del valor de sus transacciones. La seguridad por tanto, ha cobrado una importancia crítica ya que constituye un requisito previo al desarrollo del C.E.

Por seguridad de las redes y de la información puede entenderse la capacidad de estas para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad[130], autenticidad[131], integridad[132] y confidencialidad[133] de los datos almacenados o transmitidos y de los correspondientes servicios que se presten. Añádase que las redes están interconectadas, son internacionales y que el problema de seguridad es dinámico debido al desarrollo tecnológico.
Sin animo de ser exhaustivos, las principales amenazas a la seguridad de redes son:

- Interceptación de las comunicaciones, los mensajes son leídos por personas no autorizadas que además podrían copiar o modificar estos datos. Cabe distinguir la interceptación legal, que sería la operada para la investigación de un delito con orden judicial, de la ilegal, que sería para la explotación ilegítima de esos datos para usos comerciales, sabotaje, utilización fraudulenta de tarjetas de crédito... Para esta amenaza, lo único que cabe es el uso de tecnologías de seguridad de la información, como la criptografía, la F.E....

- Ataques a ordenadores y redes de ordenadores, con un uso malintencionado para copiar, modificar, destruir datos o por mera satisfacción intelectual (*Hacking*). La solución es la misma que en el anterior punto: utilizar tecnologías de seguridad, como el filtro cortafuegos que bloquea peticiones de la red, que utilizan puertos concretos de intrusión, en base a unos criterios definidos de antemano y configurados por el usuario.

- Ataques a través de virus informáticos. El virus es un programa informático que, generalmente, reproduce su propio código adhiriéndose a otros programas, de manera que, cuando se ejecuta el programa infectado activa el código del virus. La única defensa contra éstos, es la instalación de programas antivirus. Existen muchas modalidades y clases de virus, pero por citar algunas mencionaremos las siguientes: virus puro, caballo de troya, bomba lógica, gusano o *worm,* virus de arranque, virus residentes en memoria, virus de red, etc.

[130] Los datos son accesibles. Esto puede acarrear serios problemas en caso de ataque a estos, a la seguridad nacional o a sectores estratégicos como la electricidad, agua o gas.
[131] Debe confirmarse la identidad declarada de los usuarios o personas jurídicas, tanto en el correo electrónico como en la visita a una *Web* (estas visitando la *Web* de un banco pero ¿es realmente ese banco o es una suplantación?, o el que dice ser empleado del banco ¿lo es realmente?). También debe garantizarse la posibilidad del anonimato para aquellos servicios en los que la autenticación no sea necesaria.
[132] Del mensaje transmitido.
[133] Que el mensaje no haya sido interceptado y leído por parte de personas no autorizadas.

Vista la problemática, cabria destacar algunas de las medidas a adoptar en la materia, así la Comisión Europea propone la creación de un sistema europeo de alarma e información contra ataques que coordine a los existentes en los E.E.M.M. que operan de forma diferente, con lo que se dificulta la labor de alerta. Creado éste, debería crearse otro a nivel mundial que sustituyera al CERT/CC, que está parcialmente financiado por Estados Unidos, como el que se creó en el seno del G8[134], sobre puntos de contacto para combatir la delincuencia de alta tecnología. En España, el organismo encargado de la alerta temprana de virus es el Centro de Alerta temprana sobre virus y seguridad informática[135], que depende de la entidad pública empresarial Red.es.

ii) En el segundo aspecto comenzaré indicando que sólo nos vamos a centrar en la lucha contra los contenidos nocivos e ilícitos. Las otras manifestaciones de la ciberdelincuencia no serán analizadas. Baste decir que dentro del Tercer Pilar para la creación de un Espacio de Libertad, Seguridad y Justicia, se está trabajando para combatir estas formas delictivas[136].

En cuanto a la lucha contra los contenidos ilícitos y nocivos en Internet, comenzaremos por mencionar el Libro verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de la información[137]. En él, se distinguen los contenidos que han de prohibirse con carácter general por atentar contra la dignidad humana, como la pornografía infantil, la violencia gratuita, la incitación a la discriminación racial..., de aquellos que han de estar prohibidos a los menores exclusivamente. Se distinguen dos modelos de emisiones, las de radiodifusión[138] y las emisiones en línea, en las que la información puede consultarse permanentemente, como es el caso de Internet, para las que las soluciones recomendadas son, la utilización de filtros de navegación que impiden el acceso al material nocivo o memorización de la navegación, para ver qué *Webs* se han visitado.

---

[134] Fue adoptada en la reunión del G8 de los días 9 y 10 de diciembre de 1997 en Washington. A esta red se han añadido otros Estados que no pertenecen al G8. En este sentido, véase Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología, DOC 187 de 3 de julio de 2001, la cual insta, a los E.E.M.M. que aún no se han adherido a la red, a que lo hagan.

[135] Cuya dirección es: http://www.alerta-antivirus.es/

[136] En este sentido y por conexión directa con el apartado anterior, cabe resaltar que actualmente se está tratando de adoptar una Decisión Marco relativa a los ataques de los que son objeto los sistemas de la información, Com. (2002) 173 final, que trata de armonizar las legislaciones en esta materia, regulando el acceso ilegal, intromisión ilegal, inducción, complicidad y tentativa, sanciones, circunstancias agravantes, responsabilidad de las personas jurídicas por los daños causados por sus trabajadores, sanciones a estas, competencia... Para una visión sobre la actuación en otro tipo de delitos de alta tecnología, véase la Comunicación de la Comisión creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos, Com. (2001) 890 final.

[137] Com. (1996)483 final.

[138] La emisión va de principio a fin por ello se proponen soluciones tales como regular el horario de las emisiones, facilitar información sobre la programación al abonado en los servicios de acceso condicional, sistema de llaves, señales de advertencia acústica o visual...

Como consecuencia de este Libro Verde, el Consejo emitió la Recomendación 1998/560/CE de 24 de septiembre de 1998[139], que poca novedad aportó, salvo que recomienda la autorregulación, la adopción de buenas practicas en el sector y la sensibilización de los padres y educadores, y anteriormente abogó por el desarrollo y utilización de los mecanismos de filtrado en una Resolución[140].

Por último destacaremos la Decisión 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999, por la que se crea un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales[141]. Por ésta, se crea un programa de 4 años de duración que finalizará el 31 de diciembre de 2004, con una aportación de 38,3 millones de euros[142]. Este plan continua la línea fijada por los documentos anteriores, proponiendo medidas como la autorregulación, el filtrado, el asesoramiento de padres y educadores... y para ello fija tres líneas básicas de actuación, que son la creación de una red europea de líneas directas, en las cuales, los usuarios podrán denunciar los contenidos ilícitos y esta denuncia será trasladada al organismo competente (policía, juzgado...), la elaboración de sistemas de filtrado y calificación[143], para que padres y educadores puedan restringir la información a los menores (no obstante estos filtros no funcionan tan bien como es deseado, ya que, o bien se produce un sobre bloqueo de la información restringida o todo lo contrario, de ahí viene la necesidad de financiar dentro de este programa estos sistemas) y fomento de actividades de sensibilización para menores, padres, educadores o público en general.

J) Aspectos Internacionales.

A lo largo de la exposición ya han aparecido ejemplos de búsqueda del consenso y coordinación internacional, en los ámbitos de la fiscalidad, autenticación y los

[139] Relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana. DOL 270 de 7 de octubre de 1998.

[140] Resolución del Consejo y de los Representantes de los Gobiernos de los Estados Miembros reunidos en el seno del Consejo de 17 de febrero de 1997, sobre contenidos ilícitos y nocivos en Internet. DOC 70 de 6 de marzo de 1997.

[141] DOL 33 de 6 de febrero de 1999.

[142] En un principio, el plan duraba hasta el 31 de diciembre de 2002, y contaba con un presupuesto de 25 millones de euros, pero la Comisión consideró oportuno prorrogar el plazo del Plan y su cuantía presupuestaria, por lo que lanzó su propuesta "Comunicación de la Comisión sobre el seguimiento al plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales y propuesta de Decisión del Parlamento Europeo y del Consejo por la que se modifica la Decisión nº 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales, Com. (2002) 152 final", que ha derivado en la aprobación de la Decisión 1151/2003/CE del Parlamento Europeo y del Consejo, de 16 de junio de 2003, que modifica la Decisión 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales, DOUE serie L 162 de 1.7.2003.

[143] En cuanto a la calificación, véase las Conclusiones del Consejo de 17 de diciembre de 1999, sobre la protección de los menores ante el desarrollo de los servicios audiovisuales digitales, DOC 8 de 12 de enero de 2000.

derechos de autor. En este apartado, nos limitaremos a señalar brevemente uno más.

No podemos comenzar sin referirnos a un documento de gran valor para entender la problemática en la materia, que será y ha sido utilizado para el planteamiento de la situación. Éste, es la comunicación de la Comisión La mundialización y la sociedad de la información, necesidad de reforzar la coordinación internacional[144], en el cual, se hace un estudio sobre la problemática en los diferentes sectores. Aparte de los ya destacados, queremos resaltar el siguiente:

- Jurisdicción: debido a que Internet no posee fronteras físicas, una empresa situada en un país A es accesible desde otro país aunque no preste sus servicios. Por ello, es importante incidir en este sector y buscar normas armonizadas. Sin ánimo de exhaustividad debemos, por un lado, remitirnos a la normativa de derecho internacional privado que sería aplicable al C.E. en tanto que tuviera la operación un componente de transnacionalidad, principalmente a través del Convenio de Roma sobre la ley aplicable a las obligaciones contractuales de 19 de junio de 1980[145] y el Reglamento (CE) 44/2001 del Consejo de 22 de diciembre de 2000[146], y por el otro, citar dos importantes documentos elaborados en el seno de la CNUDMI para lograr el máximo posible de uniformidad en el C.E. y la F.E., que no son otros que la Ley modelo de la CNUDMI sobre el comercio electrónico con la guía para su adaptación al derecho interno de 1996, con la adición del artículo 5 bis en la forma aprobada en 1998 y la Ley modelo de la CNUDMI sobre firmas electrónicas con la guía para su incorporación al derecho interno de 2001[147]. Teniendo en cuenta que en la materia ya hay regulación comunitaria, no vamos a estudiar el contenido de estas leyes modelo y sólo se acudirá en algún momento en el próximo capítulo a éstas, en la medida que tengan elementos interesantes para la explicación.

Para finalizar este capítulo, vamos a resaltar que en el marco de las organizaciones internacionales, se trabaja intensamente en la materia. Aparte de los documentos ya citados anteriormente, recuérdese las Conferencias en el marco de la OCDE en el apartado de fiscalidad y otros que no han sido citados como las directrices sobre criptografía de la OCDE (recomendaciones del Consejo de 27 de marzo de 1997), en los que no nos vamos a detener[148]. También cabe destacar las directrices de la

[144] Com. (1998) 50 final.
[145] BOE 171 de 19 de julio de 1993; corrección de errores BOE 189 de 9 de agosto de 1993.
[146] Relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, DOL 12 de 16 de enero de 2001, que sustituye al convenio de Bruselas de 27 de septiembre de1968 sobre la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
[147] Ambas pueden consultarse en: "www.uncitral.org/sp_index.htm".
[148] Los documentos de la OCDE sobre el C.E. y la F.E. pueden consultarse en: "www.oecd.org/EN/home/0,,EN-home-29-nodirectotate-no-no-29,00htlm".

OCDE sobre privacidad y las directrices de Naciones Unidas sobre datos automatizados[149].

[149] Ambas pueden ser consultadas en la siguiente dirección: http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm

CAPÍTULO SEGUNDO:
LAS DIRECTIVAS
2000/31/CE DE COMERCIO ELECTRÓNICO
Y
1999/93/CE DE FIRMA ELECTRÓNICA.

I) La Directiva 2000/31/CE[150].

A) Objeto. Ambito de Aplicación. Mercado Interior.

Comenzaremos el estudio de la Directiva, como no podía ser de otra manera, señalando el objetivo que ésta persigue. Regulado en el artículo 1.1, no es otro que contribuir al correcto funcionamiento del mercado interior, garantizando la libre circulación de los servicios de la S.I.[151] entre los E.E.M.M., ya que se considera que el desarrollo de estos servicios en un espacio sin fronteras interiores, es esencial para eliminar las barreras que dividen a los pueblos europeos. En definitiva, es importante que el C.E. pueda beneficiarse plenamente del mercado interior y que alcance un alto grado de integración comunitaria.

Planteado el objetivo pasamos a analizar el ámbito de aplicación de la Directiva, y no podemos comenzar éste sin indicar que, de acuerdo con el principio de proporcionalidad, ésta es una Directiva de mínimos, sólo se actuará en la medida necesaria para asegurar el correcto funcionamiento del mercado interior (considerando 10 y artículo 1.2, en el cual, se dispone que sólo se actuará en la medida en que resulte necesario para alcanzar el objetivo que persigue la Directiva y en unas determinadas áreas predeterminadas, que son las reguladas por la presente norma).

La publicación de ésta, no afectará al nivel de protección aportado por otras disposiciones comunitarias o estatales en los ámbitos de la salud pública y la protección del consumidor[152], en la medida en que no restrinjan la libertad de

[150] Para una correcta citación, véase nota 3.

[151] Entenderemos por servicios de la S.I., según el artículo 2.a), aquellos regulados en el artículo 1.2 de la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la S.I., DOL 204 de 21.7.1998, modificada por Directiva 98/48/CE, DOL 217 de 5.8.1998. Este artículo los define como "todo servicio de la S.I., es decir, todo servicio prestado normalmente a cambio de una remuneración a distancia, por vía electrónica y a petición individual de un destinatario de servicios. A los efectos de esta definición, se entenderá por: distancia, un servicio prestado sin que las partes estén presentes simultáneamente; por vía electrónica: un servicio enviado desde la fuente y recibido por el destinatario por equipos electrónicos de tratamiento (incluida la comprensión digital) y de almacenamiento de datos que se transmiten, canalizan y reciben enteramente por hilos, radios, medios ópticos o cualquier otro medio electromagnético; a petición individual de un destinatario de servicios, un servicio prestado mediante transmisión de datos a petición individual.". Indíquese que el Anejo V de la Directiva 98/34/CE contiene una lista indicativa de servicios que no se incluyen en la definición dada, estos se dividen en aquellos que no se prestan a distancia, no son ofrecidos por vía electrónica y no son a petición individual de un destinatario de servicios.

[152] Se enumeran en el considerando 11, una serie de Directivas a las que afecta esta premisa en particular, que pasamos a reproducir literalmente: Directiva 93/13/CEE del Consejo de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores, DOL 95 de 21.4.1993, Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia, DOL 144 de 4.6.1997, Directiva 84/450/CEE del Consejo de 10 de septiembre de 1984, sobre publicidad engañosa y publicidad comparativa, DOL 250 de 19.9.1984, cuya última modificación la constituye la Directiva

prestar servicios de la S.I. (artículo 1.3). Tampoco se podrá invocar esta Directiva para privar a los consumidores[153] de las prerrogativas que se les otorgan en la legislación relativa a la protección en materia de obligaciones contractuales en contratos celebrados con consumidores[154].

Cabe destacar que se rechaza de plano crear normas adicionales de derecho internacional privado (artículo 1.4), como podrían ser las relativas al lugar de celebración del contrato, la legislación aplicable, el tribunal competente en la resolución de litigios..., lo que ha provocado cierto malestar en algún sector doctrinal[155], al que le hubiera gustado la inclusión de estos y otros aspectos, y que como preconizaron, han tenido que ser regulados (como se verá en el siguiente capítulo) por la normativa nacional. A favor tendríamos a Illescas Ortiz[156], para el

---

97/55/CE del Parlamento Europeo y del Consejo, DOL 290 de 23.10.1997, Directiva 87/102/CEE del Consejo de 22 de diciembre de 1986, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de crédito al consumo, DOL 42 de 12.2.1987, cuya última modificación la constituye la Directiva 98/7/CE del Parlamento Europeo y del Consejo, DOL 101 de 1.4.1998, Directiva 93/22/CEE del Consejo de 10 de mayo de 1993, relativa a los servicios de inversión en el ámbito de los valores negociables, DOL 141 de 11.6.1993, cuya última modificación la constituye la Directiva 97/9/CE del Parlamento Europeo y del Consejo DOL 84 de 26.3.1997, Directiva 90/314/CEE del Consejo de 13 de junio de 1990, relativa a los viajes combinados, las vacaciones combinadas y los circuitos combinados, DOL 158 de 23.6.1990, Directiva 98/6/CE del Parlamento Europeo y del Consejo de 16 de febrero de 1998, relativa a la protección de los consumidores en materia de indicación de los precios de los productos ofrecidos a los consumidores, DOL 80 de 18.3.1998, Directiva 92/59/CEE del Consejo de 29 de junio de 1992, relativa a la seguridad general de productos, DOL 228 de 11.8.1992, Directiva 94/47/CEE del Parlamento Europeo y del Consejo de 26 de octubre de 1994, sobre el derecho de utilización de inmuebles en régimen de tiempo compartido, DOL 280 de 19.10.1994, Directiva 98/27/CE del Parlamento Europeo y del Consejo de 19 de mayo de 1998, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, DOL 166 de 11.6.1998, modificada por Directiva 1999/4/CE DOL 171 de 7.7.1999, Directiva 85/374/CEE del Consejo de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por daños causados por productos defectuosos, DOL 120 de 7.8.1985, modificada por Directiva 1999/34/CE del Parlamento Europeo y del Consejo, DOL 141 de 4.6.1999, Directiva 1999/44/CE del Parlamento Europeo y del Consejo de 25 de abril de 1999, sobre determinados aspectos de la venta y las garantías de los bienes de consumo, DOL 171 de 7.7.1999, y la Directiva 92/28/CEE del Consejo de 31 de marzo de 1992 relativa a la publicidad de los medicamentos para uso humano, DOL 113 de 30.4.1992

Especial atención requiere la mención a la Directiva 98/43/CE del Parlamento Europeo y del Consejo de 6 de julio de 1998, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de publicidad y de patrocinio de los productos del tabaco, DOL 213 de 30.7.1998, la cual fue anulada en su totalidad por el TJCE en su sentencia de 5 de octubre de 2000. Como consecuencia de esta anulación, la Comisión lanzó una nueva propuesta (Com. (2001) 283 final), que ha dado lugar a la Directiva 2003/33/CE del Parlamento Europeo y del Consejo de 26 de mayo de 2003, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de publicidad y patrocinio de los productos del tabaco, DOUE 152 de 20.6.2003. En virtud de esta Directiva, que es de aplicación a la publicidad y patrocinio de productos del tabaco a través de los servicios de la sociedad de la información (artículo 1-C), queda prohibida la publicidad y patrocinio del tabaco, salvo que se dirija únicamente a los profesionales del comercio del tabaco y a publicaciones impresas y editadas en terceros países, siempre que no estén destinadas principalmente al mercado comunitario.

[153] Por consumidor entenderemos de acuerdo con el artículo 2-e) "cualquier persona física que actúa con un propósito ajeno a su actividad económica, negocio o profesión". Según destaca Pinochet Olave (ob.cit.), el concepto de consumidor es prácticamente idéntico al regulado en el artículo 2-b) de la Directiva 93/13/CEE, siendo un concepto amplísimo de consumidor, consecuente con el resto de la legislación comunitaria de consumo.

[154] Como por ejemplo la conferida a través de las mencionadas Directivas 93/13/CEE y 97/7/CE.

[155] Ferrer Ramírez, Raquel. "El comercio electrónico y la U.E.". Noticias de la U.E. nº 183. 2000. Pág. 61. También Pinochet Olave, ob.cit. Pág. 21 y ss., para el cual, la realidad electrónica supondrá modificaciones estructurales en algunas áreas del derecho.

[156] Illescas Ortiz, Rafael. "Derecho de la contratación electrónica". Civitas. 2001. Pág. 46 y ss.

cual, el C.E. no debe provocar una alteración sustancial del derecho preexistente de obligaciones y contratos privados a nivel nacional e internacional. Para él, la contratación electrónica no es mas que un nuevo soporte, un medio de transmisión de voluntades negociales, pero nunca un nuevo derecho regulador. Esto no obsta a que se adapte la legislación a las nuevas características o que en ésta exista una laguna legal (como el acuse de recibo que nunca había sido regulado) o que sea necesario derogar normas obsoletas. Y esto es así, porque el autor tiene en la cabeza el Principio de Equivalencia Funcional, recogido en la ya citada Ley Modelo de C.E. de la CNUDMI, según el cual, hay que aplicar al mensaje de datos electrónico una pauta de no discriminación respecto de las declaraciones de voluntad, ciencia manual, verbal o gesticular efectuadas por el mismo sujeto, es decir los efectos jurídicos apetecidos por el declarante han de producirse independientemente del medio utilizado. Para ello hay que analizar los objetivos y funciones del requisito tradicional de la presentación de escrito consignado en papel, con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado C.E.. Por poner un ejemplo, ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos, asegurar la inalterabilidad de éste a lo largo del tiempo, permitir la reproducción del mismo y suscribirlo con firma. Para estos casos, al hacerlo de forma electrónica se puede ofrecer una seguridad equivalente al papel, por lo que requiere ir viendo caso por caso. Bajo ninguna circunstancia, podrá aplicarse el principio aludido al documento público o notarial.

Pero lo dicho hasta ahora no vale para todos las materias reguladas por la legislación comunitaria y nacional. La Directiva señala unas áreas a las que ésta no se aplicará, ya que se rigen por su propia normativa, están afectadas por el ámbito de la autoridad pública o simplemente, se pensó en excluirlas para regularlas específicamente. Éstas son las siguientes:

a) En materia de fiscalidad, en particular el Iva.
b) A cuestiones relacionadas con los servicios de la S.I. que estén reguladas por la normativa sobre protección de datos, que serán de total aplicación a estos servicios.
c) A cuestiones relacionadas con acuerdos o prácticas que se rijan por la legislación sobre cárteles.
d) A las siguientes actividades de los servicios de la S.I.:

- Las actividades de los notarios o profesiones equivalentes, en la medida en que impliquen una conexión directa y específica con el ejercicio de la autoridad pública.
- La representación de un cliente y la defensa de sus intereses ante los tribunales.
- Las actividades de juegos de azar que impliquen apuestas de valor monetario incluidas loterías y apuestas.

Centrándonos a continuación en el último apartado del epígrafe, resaltaremos que a efectos de control de los prestadores de servicios de la S.I.[157], éste recae en el E.E.M.M. donde el prestador esté establecido, actividad de control que deberá entenderse para las disposiciones a las que se refiere el ámbito coordinado de la Directiva[158] (artículo 3.1).

Por ello, los E.E.M.M. no podrán restringir la libertad de prestación de servicios de la S.I. de otro E.E.M.M., por razones inherentes al ámbito coordinado. No obstante cabe señalar que el TJCE siempre ha sostenido que un E.E.M.M. conserva el derecho de adoptar medidas contra un prestador de servicios establecido en otro E.E.M.M., cuya actividad se dirige principalmente o en su totalidad, hacia el territorio del primer Estado, cuando dicho establecimiento se haya realizado con la intención de evadir la legislación que se hubiera aplicado al prestador de servicios (considerando 57). De igual manera, el artículo 3.4 habilita a los E.E.M.M. a establecer excepciones, sin perjuicio de los procesos judiciales, incluidas las actuaciones preliminares y los actos realizados en el marco de una investigación criminal, a la regla anterior, si el servicio de la S.I. va en detrimento o existe un riesgo grave y serio por los siguientes motivos:

- Orden público, en particular la prevención, investigación, descubrimiento y procesamiento del delito, incluidas la protección de menores y la lucha contra la instigación al odio por motivos de raza, sexo, religión o nacionalidad, así como las violaciones de la dignidad humana de personas individuales.
- Protección de la salud pública.
- Seguridad pública, incluidas la salvaguarda de la seguridad y defensa nacionales
- Protección de los consumidores, incluidos los inversores.

La medida deberá ser proporcional a los motivos indicados y siempre se adoptará después de haber solicitado al E.E.M.M. que tome medidas, y éste no haya actuado o de haberlo hecho, actuara de manera insuficiente, siempre después de haber notificado a la Comisión y al E.E.M.M su intención de adoptar tales medidas. Estos

[157] La Directiva diferencia entre prestador de servicios (artículo 2-b) "cualquier persona física o jurídica que suministre servicios de la S.I.", y prestador de servicios establecido (artículo 2-c) "prestador que ejerce de manera efectiva una actividad económica a través de una instalación estable y por un periodo de tiempo indeterminado. La presencia y utilización de los medios técnicos y de las tecnologías utilizadas para prestar el servicio no constituyen en sí mismos el establecimiento del prestador de servicios". Así se debe tener en cuenta para determinar el lugar de establecimiento la jurisprudencia del TJCE, según la cual, el concepto de establecimiento implica la realización efectiva de una actividad económica a través del establecimiento fijo durante un periodo indefinido. También cabría por tiempo definido. (considerando 19). Cabe también añadir que el concepto de prestador de servicios debe entenderse respecto del establecido en algún E.E.M.M., con lo que no podrá aplicarse toda la normativa aplicable a estos, si está establecido en un tercer país (considerando 58). Para este último supuesto, habrá que estar a lo dispuesto en el epígrafe sobre aspectos internacionales del capítulo anterior.

[158] Atendiendo al artículo 2-h), entendemos por éste "los requisitos exigibles a los prestadores de servicios en los regímenes jurídicos de los E.E.M.M. aplicables a los prestadores de servicios de la S.I. a los servicios de la S.I., independientemente de sí son de tipo general o destinados específicamente a los mismos" y artículo 2-i) según el cual, éste se refiere a los requisitos que ha de cumplir el prestador de servicios en relación con: el inicio de la actividad de un servicio de la S.I. en lo relativo a las autorizaciones, cualificaciones o notificaciones y el ejercicio de la actividad de acuerdo a los requisitos de comportamiento, calidad y contenido del servicio o la responsabilidad.

requisitos podrán ser exceptuados en casos de urgencia pero deberán ser notificados a la Comisión y al E.E.M.M. lo más pronto posible.

Para supervisar la legalidad de las medidas adoptadas en base a este artículo, será competente la Comisión.

Todo lo explicado con respecto al Estado de origen del servicio de la S.I., no será de aplicación a las materias que se recogen en el Anexo de la Directiva[159].

B) Materias reguladas.

El primer elemento al que vamos a hacer referencia, es al ya mencionado principio de no autorización previa, según el cual, los E.E.M.M. no podrán someter al prestador de servicios de S.I. al requisito de autorización previa, ni a otros de forma equivalente, para el acceso a la prestación de servicios de la S.I.[160].

Eso sí, los E.E.M.M. deben garantizar, además de otros requisitos en la materia, que el prestador de servicios de la S.I. mantenga una serie de datos permanentemente al alcance de las autoridades competentes y del destinatario del servicio[161], con la única finalidad de otorgar al destinatario la tan mencionada confianza, que se ve favorecida al identificar claramente a la persona física o jurídica que no ves físicamente. Como mínimo, estos requisitos serán: el nombre del prestador de servicios; dirección geográfica del lugar donde está establecido el

[159] Estos ámbitos son los siguientes:
- Derechos de autor, derechos afines y derechos mencionados en la Directiva 87/54/CEE, DOL 24 de 27.1.1987 y en la Directiva 96/9/CE, DOL 77 de 27.3.1996, así como los derechos de propiedad industrial.
- Emisión de moneda electrónica por parte de las Instituciones a las que los E.E.M.M. hayan aplicado una de las excepciones previstas en el apartado 1 del artículo 8 de la Directiva 2000/46/CE, DOL 275 de 27.10.2000.
- Apartado 2 del artículo 44 de la Directiva 85/611/CEE, DOL 375 de 31.12.1985, cuya última modificación la constituye la Directiva 95/26/CE, DOL 168 de 18.7.1995
- Artículo 30 y Título IV de la Directiva 92/49/CEE, DOL 228 de 11.8.1992,cuya última modificación es Directiva 95/26/CE. , Título IV de la Directiva 92/96/CEE, DOL 360 de 9.12.1992, cuya última modificación la constituye la Directiva 95/26/CE, artículos 7 y 8 de la Directiva 88/357/CEE, DOL 172 de 4.7.1988, cuya última modificación constituye la Directiva 92/49/CEE y artículo 4 de la Directiva 90/619/CEE, DOL 330 de 29.11.1990, cuya última modificación constituye la Directiva 92/96/CEE.
- Libertad de las partes de elegir la legislación aplicable al contrato
- Obligaciones contractuales relativas a los contratos celebrados por los consumidores.
- Validez formal de los contratos por los que se crean o transfieren derechos en materia de propiedad inmobiliaria, en caso de que dichos contratos estén sujetos a requisitos formales obligatorios en virtud de la legislación del E.E.M.M. en el que esté situada la propiedad inmobiliaria.
- Licitud de las comunicaciones comerciales no solicitadas por correo electrónico.

[160] No obstante como indica el apartado 2 del artículo 4, este principio se aplicará sin perjuicio de los regímenes de autorización que no tengan por objeto específico y exclusivo los servicios de la S.I., ni los regímenes cubiertos por la Directiva 97/13/CE del Parlamento Europeo y del Consejo de 10 de abril de 1997, relativa a un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones, DOL 117 de 7.5.1997. Hay que indicar que la nueva Directiva en la materia, Directiva autorización (para su correcta citación véase nota 51) establece en su artículo 17 que las autorizaciones existentes deberán ser adaptadas a los requisitos impuestos por la nueva Directiva, por lo que a los efectos mencionados, está también habrá de tenerse en cuenta en la aplicación de la Directiva 2000/31/CE.

[161] Atendiendo al artículo 2-d), entenderemos por éste "cualquier persona física o jurídica que utilice un servicio de la S.I. por motivos profesionales o de otro tipo y especialmente, para buscar información o para hacerla accesible".

prestador de servicios; señas que permitan ponerse en contacto rápidamente con el prestador de servicios y establecer una comunicación directa y efectiva con él, incluyendo su dirección de correo electrónico; si el prestador de servicios está inscrito en un registro mercantil u otro registro público similar, nombre de dicho registro y número de inscripción asignado en él al prestador de servicios, u otros medios equivalentes de identificación en el registro; si una determinada actividad está sujeta a régimen de autorización, los datos de la autoridad de supervisión correspondiente; en lo que se refiere a las profesiones reguladas[162] si el prestador de servicios pertenece a un colegio profesional o institución similar, deberá facilitar los datos de dicho colegio o institución, de igual manera deberá facilitar su título profesional expedido y el E.E.M.M. que lo expidió y hacer referencia a las normas profesionales aplicables en el E.E.M.M. de establecimiento y los medios de acceder a las mismas; si el prestador de servicios ejerce una actividad gravada por el Iva, deberá mostrar el número de identificación al que hace referencia el artículo 22.1 de la Directiva 77/388/CEE[163]; si hacen referencia estos servicios a precios, estos deberán estar indicados claramente y sin ambigüedades, constando de manera clara si incluyen impuestos indirectos y costes de envío.

Cuestión diferente y por ello no menos importante, son las comunicaciones comerciales[164] que adquieren determinada relevancia si se producen a través del correo electrónico, propiciando el denominado *spam*, que provoca la saturación de la bandeja de entrada del correo por la llegada masiva e indiscriminada del mismo, con el consiguiente perjuicio para el usuario que, independientemente de la modalidad de pago que posea, es facturado por el tiempo que se mantenga conectado a Internet. Por todo ello, las comunicaciones comerciales serán claramente identificables como tales, así como la persona física o jurídica en el nombre de la cual se realicen esas comunicaciones. Lo mismo ocurre con las ofertas, concursos o juegos promocionales, los cuales deberán estar claramente identificados, así como los requisitos y condiciones de participación.

---

[162] Entenderemos por profesión regulada de acuerdo con el artículo 2-g) "cualquier profesión en el sentido o bien de la letra d) del artículo 1 de la Directiva 89/48/CEE del Consejo de 21 de diciembre de 1988, relativa a un sistema general de reconocimiento de títulos de enseñanza superior que sancionen formaciones profesionales de una duración mínima de tres años, DOL 19 de 24.1.1989 o de la letra f) del artículo 1 de la Directiva 92/51/CEE del Consejo de 18 de junio de 1992, relativa a un segundo sistema general de reconocimiento de formaciones profesionales que completa a la Directiva 89/48/CEE, DOL 209 de 24.7.1992, cuya última modificación la constituye la Directiva 97/38/CE de la Comisión, DOL 184 de 12.7.1997".

[163] Véase nota 100.

[164] Entenderemos por éstas, de acuerdo con el artículo 2-f) "todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o de profesiones reguladas. No se consideran comunicaciones comerciales en sí mismas las siguientes:

- Los datos que permiten acceder directamente a la actividad de dicha empresa, organización o persona y, concretamente el nombre de dominio o la dirección de correo electrónico.
- Las comunicaciones relativas a los bienes, servicios o a la imagen de dicha empresa, organización o persona, elaboradas de forma independiente de ella, en particular cuando éstas se realizan sin contrapartida económica".

Si la comunicación comercial se produce a través del correo electrónico y no ha sido solicitada por el destinatario, es decir, no se la han remitido a petición propia, además de que ha de ser recibida de acuerdo con los requisitos ya mencionados, los E.E.M.M. han de garantizar, si perjuicio de las Directivas 97/7/CE[165] y 97/66/CE[166], que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas, consulten regularmente las listas de exclusión voluntaria (*opt-out*) en las que podrán inscribirse las personas físicas que no deseen recibir tales comunicaciones y las respeten. A este efecto, como ya se mencionó en líneas anteriores debemos traer a colación de nuevo el artículo 13 de la Directiva 2002/58/CE, el cual regula también las comunicaciones no solicitadas. La Directiva introduce el principio opuesto, éstas sólo serán válidas si el abonado ha dado su consentimiento expreso, con la excepción que la dirección de correo electrónico del cliente se haya obtenido de conformidad con lo establecido en la Directiva 95/46/CE[167], siempre que se permita al usuario que, de manera sencilla y sin coste alguno pueda oponerse a la utilización de sus señas en cada comunicación que reciba.

Con la salvedad del inciso anterior, los E.E.M.M. podrán optar o bien por el sistema de consentimiento expreso del abonado o bien, por el de exclusión voluntaria.

Lógicamente, a tenor de lo expuesto puede plantearse el lector una duda de cómo han de aplicarse las dos Directivas, en principio contradictorias. Baste decir que la Directiva 2000/31/CE regula las comunicaciones no solicitadas en los servicios de la S.I., de acuerdo con la definición que se dio en su momento, y la Directiva 2002/58/CE regula éstas, pero en los servicios de llamada automática, fax o correo electrónico, lo que en la práctica supone que al menos el correo electrónico esté regulado por ambas Directivas. Pero la contradicción no queda ahí, sino que se ve agudizada al imponer la Directiva 2002/58/CE la obligatoriedad del consentimiento expreso (artículo 13.1), para dejar después la elección del sistema a los E.E.M.M. (artículo 13.3), con lo que nos aventuramos a decir que en la aplicación de este apartado habrá polémica y diferencias interpretativas.

No obstante por intentar "humildemente" clarificar la situación podría entenderse que el artículo 13.1 al imponer este consentimiento expreso, lo está haciendo para cualquier modalidad de las dos posibles. Así en el caso de que el E.E.M.M. optara por el consentimiento expreso, no habría problemas de interpretación y en cuanto a la exclusión voluntaria, debería entenderse que el abonado debe dar su consentimiento expreso ya sea otorgándolo al prestador de servicios o negándoselo, al inscribirse en una lista voluntaria de exclusión, debiendo en todo caso ejercitar

[165] Véase nota 72.
[166] Derogada por la Directiva 2002/58/CE. Para correcta citación, véase nota 55.
[167] Véase nota 51.

obligatoriamente una de esas dos opciones, siempre que éste sea persona física, de acuerdo con el artículo 13.5.

Por lo que se refiere a la contradicción entre las dos Directivas, sólo destacaremos que la Directiva 2000/31/CE habla de destinatario de la comunicación y la Directiva 2002/58/CE habla de abonado, con lo que entendemos que la primera se aplica a los prestadores que mandan comunicaciones comerciales en aras de captar clientes y la segunda es de aplicación entre la empresa de comunicaciones electrónicas y su cliente.

Para finalizar las comunicaciones comerciales, hay que citar el régimen especial que se impone a las que realicen aquellos cuya actividad cae dentro del ámbito de las profesiones reguladas. Para estos profesionales su utilización no está vedada, pero habrán de emitirlas de acuerdo a las normas profesionales relativas a la dignidad y el honor de la profesión, la independencia, el secreto profesional y la lealtad hacia el cliente y colegas. Para facilitar su cumplimiento, los E.E.M.M. y la Comisión fomentarán la elaboración de códigos de conducta por parte de los colegios y asociaciones profesionales.

Dejando las comunicaciones comerciales para continuar el estudio de la Directiva, destacaremos a continuación el artículo 9, el cual reconoce la validez y eficacia de los contratos celebrados por vía electrónica. Validez y eficacia que, como reconoce Pinochet Olave[168], no es sólo un principio, es una obligación de resultado que obliga a los E.E.M.M. a dar facilidades a los agentes sociales para que puedan comerciar electrónicamente.

No obstante, lo dispuesto en este artículo no será de aplicación, si así lo consideran los E.E.M.M., para las siguientes categorías de contratos:

a) Los contratos de creación o transferencia de derechos en materia inmobiliaria, con la excepción de 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 en materia de derecho de familia o de sucesiones.

Avanzando en nuestro estudio, nos centraremos ahora en la regulación que afecta a un pedido solicitado a través de un servicio de la S.I. El articulo 10 regula la información que ha de facilitarse al usuario (excepto cuando las dos partes no son consumidores y así lo hayan pactado) antes de que este realice un pedido:

a) Los diferentes pasos técnicos que deben darse para celebrar el contrato.

[168] Ob.cit. página 138.

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.
e) Los códigos de conducta a los que se acoja y la manera de consultar electrónicamente estos.

No obstante, lo anterior no se aplicará cuando los contratos se celebren exclusivamente por intercambio de correo electrónico o comunicación individual equivalente, y es que como señala Pinochet Olave[169], al igual que lo que ocurre con el acuse de recibo, que será estudiado a continuación, la Directiva de C.E. está pensando en la contratación a través de una *Web* en la que no existe intercambio de información, el usuario simplemente pulsa el ratón en un cuadrante y automáticamente se acepta un contrato con un clausulado, sin posibilidad de negociación y aclaración de dudas.

De igual manera, las condiciones generales de los contratos deberán estar disponibles de tal manera que el usuario pueda almacenarlas y reproducirlas.

Para finalizar el apartado de información previa, nos referiremos a la complementariedad de la Directiva en esta materia, con la Directiva 97/7/CE[170], con lo que tendríamos que añadir a estos requisitos, las características esenciales del bien o servicio, el precio de éste (incluidos los impuestos) la existencia de un derecho de resolución, el coste de utilización de la técnica de comunicación a distancia, el plazo de validez de la oferta y la duración mínima del contrato, cuando se trate de contratos de suministro de productos o servicios destinados a una ejecución permanente o repetida.

Para la realización del pedido se han de respetar los principios siguientes, excepto cuando las partes no sean consumidores y así lo acuerden:

- El prestador de servicios debe acusar recibo del pedido del destinatario sin demora indebida y por vía electrónica, salvo que el contrato se celebre exclusivamente a través de correo electrónico o comunicación equivalente. Como se señaló recientemente el legislador está pensando en la contratación a través de una *Web*.
- Se considerará que se han recibido el pedido y el acuse de recibo, cuando las partes a las que se dirigen puedan tener acceso a las mismas. Como señala Pinochet Olave[171], la regulación es adecuada porque, cuando lo emite el prestador no sabe realmente si ha llegado al destinatario o no, pero obligar al destinatario a emitir confirmación de la recepción del acuse de recibo supondría

[169] Ob.cit pág 143.
[170] Véase nota 72.
[171] Ob.cit. página 145.

crear un circulo vicioso que nunca acabaría. Basta con que las partes tengan acceso al mismo, es decir, parece que la Directiva está pensando en el momento en el que el acuse de recibo es depositado en la bandeja de entrada del correo electrónico, pero hágase notar que es un concepto neutro y abierto, que posibilita el avance tecnológico en un futuro y las interpretaciones diversas en el presente.

Para finalizar el epígrafe, nos referiremos a la responsabilidad del prestador de servicios de la S.I., que viene regulada a través de tres supuestos que pasamos a relatar a continuación.

El primer supuesto en el que podría incurrir en responsabilidad el prestador de servicios, sería por la transmisión de datos en un servicio de la S.I. que consista en la transmisión de datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones. Se exonera de responsabilidad al prestador si se dan los siguientes requisitos:

- Que no haya originado él mismo la transmisión.
- Que no seleccione al destinatario de la transmisión.
- Que no seleccione ni modifique los datos transmitidos.

Hay que tener en cuenta que estas actividades descritas engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos, siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión. Esto quiere decir que la actividad del prestador es meramente técnica, automática y pasiva, lo que implica que no tiene conocimiento ni control de la información transmitida o almacenada o lo que es lo mismo, sólo actúa como intermediario.

El segundo supuesto regulado es el de la memoria tampón (*caching*), consistente en la utilidad que posee la memoria base de un ordenador o Ram, denominada memoria caché que utiliza entre 2 y 5 megas de la capacidad de ésta, que sirve para mejorar su capacidad de utilización final. Así cuando se navega, el programa almacena las páginas visitadas con anterioridad para recuperarlas más fácilmente. En este supuesto, el prestador de servicios no será responsable sí:

- No ha modificado la información.
- Si cumple las condiciones de acceso a la información.
- Si cumple las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector.
- Si no interfiere en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información

- Si actúa con prontitud para retirar la información que haya almacenada, o hacer que el acceso a ella sea imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se encontraba inicialmente, que se ha imposibilitado el acceso a dicha información o que un tribunal o autoridad administrativa ha ordenado retirarla o impedir el acceso a ella.

El tercer supuesto es el alojamiento de datos, para un servicio que consiste en el almacenaje de datos facilitados por el destinatario del servicio como el de correo electrónico. Como en los casos anteriores, no será responsable el prestador de servicios sí:

- No tiene conocimiento efectivo que la actividad realizada es ilícita.
- Actúa con prontitud en cuanto tenga conocimiento de ello para retirar esos datos.

Finalizaremos este apartado con la premisa de que no se puede imponer a los prestadores de servicios una obligación general de supervisión de datos, ni de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas en cuanto a los supuestos recién explicados. Como señala Pinochet Olave[172], existían dos corrientes doctrinales, de las cuales, una abogaba por responsabilizar a los prestadores por los contenidos que publicaban, al igual que los editores lo son por las obras que editan y la otra optaba por la asimilación de la responsabilidad de las librerías, ya que se reconoce la imposibilidad de controlar el enorme volumen de información dinámica o estática que los usuarios introducen en el servidor, por ello el autor considera que la primera opción, aparte de desproporcionada, hubiera impuesto a los prestadores una obligación de garante, que por antonomasia, recae en los órganos estatales, amén de la conculcación de los Derechos Fundamentales de los ciudadanos, en especial el de privacidad. No hay que dejar de tener presente que la principal responsabilidad es del autor.

C) Aplicación de la Directiva.

A continuación señalaremos tres supuestos que regula la Directiva en lo referente a su aplicación, en las áreas de la solución extrajudicial de conflictos y códigos de conducta, la resolución judicial de conflictos y la imposición de sanciones. El primer supuesto es el de la fijación de los Códigos de conducta, a los que ya nos referimos en el capítulo anterior, al explicar el epígrafe referente a la protección de consumidores. Se pretende que los E.E.M.M. y la Comisión fomenten la elaboración a nivel comunitario de estos códigos por parte de las asociaciones u organizaciones comerciales, profesionales o de consumidores, en lo que respecta a la correcta aplicación de las materias tratadas a lo largo de este epígrafe (con la salvedad el principio de no autorización previa). De igual manera se debería remitir

[172] Ob.cit. página 156 y ss.

voluntariamente a la Comisión el proyecto de esos Códigos, ya sean a nivel estatal o comunitario.

Debe fomentarse igualmente que se pueda acceder a estos por vía electrónica en las lenguas comunitarias y la creación de códigos específicos en materia de protección de menores y de la dignidad humana.

En cuanto a la resolución extrajudicial de conflictos, la legislación de los E.E.M.M. no puede obstaculizar la resolución de controversias, incluso utilizando medios electrónicos, entre un prestador de servicios y el destinatario del mismo.

En lo relativo a los recursos judiciales, la legislación de los E.E.M.M. ha de permitir que se puedan adoptar rápidamente medidas, ya sean provisionales o no, destinadas a poner término a cualquier presunta infracción y evitar nuevos perjuicios a los intereses afectados. De la misma manera, esta Directiva entrará dentro del ámbito de aplicación de la Directiva 98/27/CE[173], según la cual, se podrán interponer acciones de cesación para la protección de los intereses colectivos de los consumidores, conforme a los requisitos establecidos en el artículo 2 de la citada Directiva, por parte de las entidades habilitadas para ello. Podrá ser entidad habilitada cualquier organismo u organización, legalmente constituida con arreglo a la legislación de un E.E.M.M., que posea un interés legítimo en que se respeten cualquiera de los intereses protegidos en el artículo 1 de la Directiva 98/27/CE.

Para finalizar este apartado, señalaremos que corresponde a los E.E.M.M. determinar las sanciones aplicables a las infracciones que se deriven de lo regulado en la presente Directiva, así como cooperar con el resto de E.E.M.M. a través de puntos de contacto, que serán accesibles como mínimo por vía electrónica y a los que podrán dirigirse los prestadores y destinatarios de servicios para obtener información sobre sus derechos y obligaciones, mecanismos de recurso y reclamación disponibles, datos de asociaciones y organizaciones del sector.

[173] Del Parlamento Europeo y del Consejo de 19 de mayo de 1998, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, DOL 166 de 11.6.1998.

II) La Directiva 1999/93/CE de F.E.[174].

A) Introducción.

No podemos comenzar el estudio de la Directiva, sin realizar una breve explicación sobre la materia que actúe de modo clarificador para el lector, debido a la complejidad técnica de ésta.[175].

Lo primero que debemos hacer es diferenciar la F.E. de la Firma Digital (F.D.). Así la primera actúa como firma en un documento electrónico, sustituyendo a la firma autógrafa y la segunda añade otros requisitos, como la confidencialidad, el origen y la integridad del mensaje, con lo que aquí cabria interponer una primera crítica a la Directiva, que utiliza el término F.E., cuando está pensando también en estos requisitos.

La F.D[176]. no es mas que una firma numérica basada en criptografía de clave pública.

La firma se crearía por medio de mecanismos técnicos, tales como, la utilización de un lápiz especial que recogería ésta en la pantalla, la analizaría y la convertiría en un conjunto de caracteres numéricos o por otros mecanismos como la utilización de un número PIN, el uso de tarjetas inteligentes, y *passwords* o los métodos biométricos que recogen características anatómicas o fisiológicas del firmante, como la huella digital, el reconocimiento del iris o la pupila...

Creada ésta, se utiliza la criptografía para generar un certificado[177], que no es otra cosa que el cifrado del mensaje de datos que se quiere transmitir, utilizando algoritmos que convierten a éste en formas aparentemente ininteligibles, para devolverlos con posterioridad a su forma habitual, es decir, como señala Illescas Ortiz[178], el cifrado actuaría como el sobre postal, impidiendo su interceptación y avisando al receptor en caso de que ésta se haya producido. Existen dos modelos de firmas, uno basado en criptosistemas simétricos, el cual, utiliza una dave privada única para cifrar y descifrar el mensaje y otro asimétrico, que utiliza dos claves diferentes una pública y otra privada, de manera que una cifra el mensaje y la otra

[174] Para su correcta citación, véase nota 3.
[175] No obstante, puede completarse la información con el siguiente artículo: Mason, Stephen. "Electronic Signatures: The technical and legal ramifications". Computers&Law. December 1999/january 2000. Volume 10. Issue 5.
[176] Podemos obtener firmas electrónicas a través de la Fabrica Nacional de la Moneda y Timbre. Real Casa de la Moneda www.fnmt.es y del consejo Superior de Cámaras, exclusivamente para empresas www.camaramadrid.es/innovacion/innovacion_2_3.htm.
[177] Podemos obtener certificados a través de la Agencia Española de Certificación www.aec.es, y las empresas Verisign www.verisign.com y Thawte www.thawte.com.
[178] Ob.cit. páginas 59 y ss.

lo descifra y verifica la firma. El sistema simétrico es bastante fiable pero plantea un inconveniente, que las dos partes han de conocer la clave, con lo cual se plantea un problema cuando se tienen que mandar muchos mensajes cifrados a diferentes personas, con lo que o mucha gente conoce tu clave privada o dispones de gran multitud de ellas, una para cada persona, e imaginémonos que ocurriría si se trata de un comerciante, aunque este extremo es rebatido en base a que, por ejemplo, los supermercados o grandes almacenes proporcionan gran multitud de tarjetas de crédito distintas, una por cada cliente. No obstante, el método más utilizado es el de clave pública ya que sólo requiere la emisión de dos claves. Este sistema, está basado en el empleo de funciones algorítmicas que generan dos claves diferentes, pero matemáticamente relacionadas entre sí por el empleo de números primos. Aunque estas dos claves estén matemáticamente relacionadas entre sí, el diseño y la ejecución de un criptosistema asimétrico, hace virtualmente imposible que las personas que conozcan la clave pública puedan adivinar la privada, ya que al utilizar el sistema de números primos, una vez multiplicados entre sí para obtener un nuevo número, constituye una tarea larga y difícil determinar cuales fueron los números que crearon un número mayor. Además los actuales sistemas son aún más seguros al utilizar los criptosistemas basados en curvas elípticas.

Por lo dicho anteriormente, la clave privada se utiliza sólo por el firmante para crear una firma numérica y la clave pública que, de ordinario conocen más personas, sirve para verificar (ésta también incluye además de la identidad y la confidencialidad, la integridad del mensaje, es decir, que no ha sido modificado) y descifrar la firma numérica. Por tanto es necesario que la clave privada se mantenga en secreto e incluso no es necesario que la conozca, porque puede accederse a ella, como se indicó antes, a través de una tarjeta inteligente, numero PIN o método biométrico.

Por poner un ejemplo, si A quiere mandar un mensaje a B, utilizaría la clave pública de B para cifrar el mensaje y una vez recibido por B, éste utilizaría su clave privada para descifrarlo. También cabe la operación inversa. Mas aún, partiendo del mismo supuesto, si B quiere tener certeza de que es realmente A, quien le manda el mensaje, en ese caso, A debería cifrar el mensaje con la clave pública de B, mas la clave privada de A y para descifrarlo ,B utilizaría su clave privada, mas la clave pública de A.

Pero aún no tenemos cerrada la problemática que afecta a esta materia. Pensemos por un momento que un impostor se quiere hacer pasar por A, con lo cual crea una clave privada de A, con su correspondiente clave pública. Las personas al ver que con la clave pública se descifra el mensaje de datos, creerán realmente que es A quien les ha enviado el mensaje. Para evitar esto, se utiliza la denominada PKI (*Public Key Infraestructure*) que basa su funcionamiento en los denominados terceros de confianza, entidad certificadora o prestador de servicios de certificación que además de crear la clave privada y publica del solicitante, se aseguran que es

realmente quien dice ser. Esto se produce por la emisión de un certificado, por parte de este tercero de confianza, en el que se indica que los datos en él consignados son ciertos, por eso es vital para el éxito de este sistema que se aplique a nivel internacional la regla del reconocimiento mutuo a los certificados.

Para finalizar, alguien podría decir que este sistema, aún siendo casi perfecto, podría tener un cierto porcentaje de riesgo, pero debemos plantearnos que éste siempre existe en todos los ámbitos de la vida diaria, y que para combatirlo, el mejor criterio a seguir es el de la lógica económica, el cual prescribe que, para estos casos, debe crearse un sistema cuya violación resulte más cara de lo que estén dispuestos a asumir los piratas informáticos. Pues bien, este sistema al ser abierto, ya que los mecanismos de acceso a la clave privada pueden evolucionar, así como las técnicas de cifrado, permite pensar que se puede aplicar con garantías de éxito este principio, eso sí, volviendo a señalar que el nivel cero de riesgo es prácticamente imposible de alcanzar y que por ello, se debe trabajar con la máxima de lograr un nivel adecuado de seguridad aceptado como óptimo por el mercado[179].

B) Antecedentes de la Directiva.

Las primeras referencias a la F.D. y al cifrado pueden verse en documentos de principios de los 90[180], pero es en 1997 cuando la materia se desarrolla de manera considerable.

Por un lado tenemos la "Iniciativa europea de C.E.[181]", la cual resalta que "la F.D. es un instrumento esencial para fomentar la seguridad y la confianza en las redes abiertas y en el comercio canalizado a través de las mismas" y por el otro, la Comisión Europea público su tan anunciada comunicación sobre "El fomento de la seguridad y la confianza en la comunicación electrónica. Hacia un marco europeo para la firma digital y el cifrado[182]", que al igual que la contemporánea iniciativa europea de C.E., plantea los problemas que afectan a la materia, como el fraccionamiento del mercado interior, la necesidad de coordinación internacional y llevar a cabo reformas legislativas..., estableciendo para ello un calendario de trabajo con plazos de ejecución. Pero por si algo destaca, es por fijar los principios en los que debería basarse la futura Directiva en la materia, principios que no son otros que los siguientes:

- La existencia de una iniciativa legislativa creciente sobre la materia en los E.E.M.M., supone un peligro de fragmentación del mercado interior que obliga a adoptar un proceso de armonización a nivel europeo.

[179] Este mismo criterio puede aplicarse a los ataques que sufren los sistemas informáticos, que estudiamos en el apartado I-i) del capítulo anterior.
[180] Como la comunicación del la Comisión "Europa en marcha hacia la S.I.. Plan de actuación". Com. (1994) 347 final, entre otros.
[181] Véase nota 10.
[182] Com. (1997) 503 final.

- Una Directiva europea en la materia debe ser neutral desde el punto de vista tecnológico, de forma que debe comprender no sólo la figura actualmente mas evolucionada (en estos momentos la F.E. basada en la criptografía asimétrica en clave pública y privada), sino cualquier F.D. que surja en un futuro.
- Conveniencia de evitar los sistemas de autorización previa obligatoria para los proveedores de servicios de certificación, sin perjuicio de la creación de sistemas de acreditación voluntarios con el objeto de incrementar la confianza de los consumidores.
- Garantizar el reconocimiento jurídico de la F.D. y los proveedores de servicios de certificación.

A su vez también destaca las funciones que debe cumplir la F.D., que aunque se explicaron en el apartado anterior, pasamos a reproducir a modo de recapitulación:

- Asegura que aquel con quien se contrata es realmente quien dice ser (autenticidad).
- El mensaje no ha sido modificado o alterado en su contenido (integridad).
- Nadie no autorizado lo ha leído o ha accedido al mismo (confidencialidad).
- No podrá ser rechazado una vez aceptado, salvo pacto de retractación o desistimiento (no repudiación).
- La clave pública es conocida por todos y la privada sólo por el titular, un mensaje cifrado por una clave privada sólo puede ser descifrado por una determinada clave pública, o viceversa.

C) Regulación jurídica.

Por último nos centraremos en el estudio de la Directiva, que es lo que nos ocupa en este capítulo, no sin antes haber aclarado los conceptos que afectan a la materia y haber situado los antecedentes que propiciaron la aprobación de la Directiva. La finalidad perseguida es facilitar el uso de la F.E.[183] y contribuir a su reconocimiento jurídico, no entrando a regular otros aspectos relacionados con la celebración y la validez de los contratos u otras obligaciones legales, cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectar a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de los documentos.

El primer aspecto a destacar es que se establece el principio de no autorización previa para la prestación de servicios de certificación. Este principio no ha dejado a la doctrina impasible, sino que más bien ha despertado opiniones encontradas. Así para Díaz Fraile[184], la regla general de no autorización previa crea desprotección al

[183] A efectos de la Directiva entenderemos por F.E., según el artículo 2.1: "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación".
[184] Díaz Fraile, Juan María. "El documento electrónico y la firma digital: su regulación en la U.E.", Noticias de la U.E. nº.177. 1999.

consumidor, al quedar expuesto a abusos y fraudes; por eso cree que la mejor opción hubiera sido un trámite obligatorio de homologación, ya que supone en caso contrario una privatización de funciones públicas (en particular el otorgar fe pública) que va en detrimento de la protección del consumidor y de la seguridad jurídica de la contratación. Por el contrario, Illescas Ortiz[185] mantiene que un monopolio de acceso a estos servicios ni tiene justificación económica, ni tecnológica y tampoco sería coherente con los postulados constitucionales españoles y constitutivos europeos, opinión que nos parece más autorizada, ya que como se verá mas adelante, lo que se pretende es que la firma electrónica avanzada (F.E.A.), goce de la misma validez y eficacia que la firma manuscrita en un soporte de papel, firma que goza de valor probatorio pero que en ningún caso tiene la misma fuerza probatoria que un documento público o notarial, documento que no entra en el ámbito de aplicación de la presente Directiva, con lo que a modo de recapitulación los proveedores de servicios de certificación suplen a la firma manuscrita pero no dan fe pública, con lo que siempre cabe prueba en contra.

No obstante, los E.E.M.M podrán establecer sistemas voluntarios de acreditación[186], destinados a incrementar la confianza en estos servicios. Las condiciones de acreditación voluntaria deberán ser transparentes, objetivas, proporcionales y no discriminatorias y no podrán ampararse en esta Directiva para limitar el número de proveedores de servicios de certificación[187].

Aunque el acceso a la actividad no está sujeto a autorización, si que deberán establecerse sistemas de supervisión de la actividad para todos aquellos proveedores de servicios de certificación que emitan certificados reconocidos[188]. Para esta modalidad en particular, los proveedores han de cumplir una serie de requisitos que se encuentran regulados en el Anexo II de la Directiva:

---

[185] Ob.cit. página 100.

[186] Según el artículo 2.13 la acreditación voluntaria es: "todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, cuando el proveedor de servicios de certificación no este habilitado para ejercer los derechos derivados del permiso hasta que haya recaído decisión positiva de dicho organismo".

[187] Atendiendo al artículo 2.11 estos son: "la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la F.E,".

[188] Por éste entendemos, según el artículo 2.10: "el certificado que cumple los requisitos establecidos en el Anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos del Anexo II". Por aclarar los términos, entendemos por certificado, según el artículo 2.9: "la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de este". En cuanto a los requisitos que han de contener los certificados reconocidos, se encuentran recogidos en el Anexo I y son los siguientes:

a) La indicación de que el certificado se expide como certificado reconocido.
b) La identificación del proveedor de servicios de certificación y el Estado en que está establecido.
c) El nombre y los apellidos del firmante o un seudónimo que conste como tal.
d) Un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado.
e) Los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del firmante.
f) Una indicación relativa al comienzo y fin del período de validez del certificado.
g) Un código identificativo del certificado.
h) La F.E.A. del proveedor de servicios de certificación que expide el certificado.
i) Los límites de uso del certificado, si procede.
j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.
b) Garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato.
c) Garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó el certificado.
d) Comprobar debidamente, de conformidad con el derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido.
e) Emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: la competencia en materia de gestión, conocimientos técnicos en al ámbito de la F.E. y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas.
f) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan.
g) Tomar medidas contra la falsificación de certificados y en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos.
h) Disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro adecuado.
i) Registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos.
j) No almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicio de gestión de claves.
k) Antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado.
l) Utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:
- sólo personas autorizadas puedan hacer anotaciones y modificaciones,

- pueda comprobarse la autenticidad de la información,
- los certificados estén a disposición del público para su consulta, sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado,
- el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados.

Corresponde a los E.E.M.M. disponer qué organismos, ya sean públicos o privados, emiten la conformidad de los dispositivos seguros de creación de firma[189]. Eso sí, deberán respetar los criterios que fije la Comisión para la determinación de estos[190]. Una vez emitida por el organismo la conformidad, se aplicará en todos los E.E.M.M. la regla del reconocimiento mutuo. En este sentido, la Comisión con arreglo al procedimiento de comitología podrá determinar y publicar en el DOCE los números de referencia de las normas que gocen del reconocimiento general para productos de firma electrónica[191], y para estos, los E.E.M.M. deberán presumir que se ajustan a la letra f) del Anexo II y al Anexo III.

Igualmente, los E.E.M.M. y la Comisión cooperarán para promover el desarrollo y la utilización de los dispositivos de creación de firma, a la luz de las recomendaciones para la verificación segura de firma que figuran en el Anexo IV[192].

---

[189]Según el artículo 2.6 son "aquellos los dispositivos de creación de firma que cumplen los requisitos recogidos en el Anexo III". Por dispositivo de creación de firma entendemos: "un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de la firma" y por datos de creación de firma entendemos: "los datos únicos tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica". En cuanto a los requisitos del Anexo III, son los siguientes:

- Los dispositivos seguros de creación de firma garantizarán como mínimo, por medios técnicos y procedimientos adecuados que:

a) los datos utilizados para la generación de firma, sólo pueden producirse una vez en la practica y se garantiza razonablemente su secreto,

b) existe la seguridad razonable de que los datos utilizados para la generación de la firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad,

c) los datos utilizados para la generación de la firma pueden ser protegidos, de forma fiable, por el firmante legítimo contra su utilización por otros.

- los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse, ni impedirán que dichos datos se muestren al firmante antes del proceso de firma.

[190] Se fijarán utilizando el procedimiento del artículo 9 de la Directiva según el cual se creará un Comité de F.E., que se regirá por el procedimiento de gestión de comitología del articulo 4 de la Decisión 1999/468/CE. Éste tendrá, además, otras competencias, que están recogidas en el artículo 10 de la Directiva.

[191] De acuerdo al artículo 2.12, éstos son: "el programa informático o el material informático o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o verificación de firmas electrónicas".

[192] Por dispositivo de verificación de la firma entendemos, según el artículo 2.8, "un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de verificación de la firma" y por datos de verificación de la firma entenderemos "los datos, tales como los códigos o claves criptográficas públicas, que se utilizan para verificar la firma". Pasando a las recomendaciones del Anexo IV para la verificación segura de firma, son las siguientes:

Durante el proceso de verificación de firma, deberá garantizarse, con suficiente certeza, que:

a) los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador,

b) la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente,

c) el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados,

Para el uso de la F.D. en el sector público se podrán establecer, por parte de los E.E.M.M., requisitos adicionales que deberán ser objetivos, transparentes, proporcionales, no discriminatorios y no pudiendo obstaculizar la prestación de servicios transfronterizos al ciudadano.

Al igual que en la Directiva 2000/31/CE, el E.E.M.M. de control es aquél en el que está establecido el proveedor de servicios de certificación, pero a diferencia de la Directiva citada, en este ámbito no pueden restringir la prestación de servicios de certificación por parte de proveedores situados en otro E.E.M.M.. De igual forma, los productos de firma electrónica que se ajusten a esta Directiva podrán circular libremente por el mercado interior.

Los E.E.M.M. asimismo, procurarán que la F.E.A.[193], basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma, satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica, del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel y sea admisible como prueba en procedimientos judiciales (aunque también deberá garantizarse su admisibilidad como prueba ante la falta de uno de los siguientes presupuestos: no presentarse en forma electrónica, no basarse en un certificado reconocido, no basarse en un certificado expedido por un proveedor de servicios de certificación acreditado o no estar creada por un dispositivo seguro de creación de firma).

Ante este reconocimiento de la F.E.A. como firma autógrafa, como bien señala Illescas Ortiz[194], el principio de neutralidad tecnológica en esta ocasión quiebra, ya que la Directiva tiene un carácter bifronte al apostar por la tecnología mas usada y segura hoy, la F.E.A. basada en clave pública y privada con la intervención del proveedor de servicios de certificación, otorgándole una posición privilegiada con respecto a otras tecnologías presentes y futuras.

En otro orden de cosas, la responsabilidad de los proveedores de servicios de certificación está regulada en el artículo 6, según el cual, estos proveedores, como mínimo, serán responsables de los daños ocasionados por los certificados reconocidos presentados al público, en lo que respecta a la veracidad en el momento de la expedición de los datos recogidos en el certificado reconocido, que

---

d) se verifican de forma fiable la autenticidad y la validez del certificado exigido al verificarse la firma,
e) figuran correctamente el resultado de la verificación y la identidad del firmante,
f) consta claramente la utilización de un seudónimo,
g) puede detectarse cualquier cambio pertinente relativo a la seguridad.

[193] Ésta consiste, atendiendo al artículo 2.2, en: "la firma electrónica que cumple los requisitos siguientes:
a) estar vinculada al firmante de manera única,
b) permitir la identificación del firmante (persona que esta en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa),
c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control,
d) estar vinculada a los datos a que se refiere dé modo que cualquier cambio ulterior de los mismos sea detectable."

[194] Ob.cit. página 53.

los datos relativos al firmante obraban en poder de éste, en el momento de la expedición del certificado y la garantía de que los datos de creación y verificación de firma pueden utilizarse complementariamente, salvo que demuestren que no actuaron con negligencia. De igual manera y bajo la misma excepción, serán responsables por no registrar la revocación del certificado reconocido. Igualmente al estarles permitido establecer límites al uso y un valor límite en las transacciones del certificado reconocido, no serán responsables en lo que respecta al uso mas allá de esos límites.

En lo que respecta al reconocimiento de los certificados reconocidos por un tercer país, deben ser reconocidos por los E.E.M.M. como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad, si cumple alguna de las siguientes condiciones:

a) que el proveedor de servicios de certificación cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema de acreditación voluntaria en un E.E.M.M.,
b) que un proveedor de servicios de certificación establecido en la Comunidad que cumpla las prescripciones de la presente Directiva avale el certificado,
c) que el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

Para la gestión del tercer apartado será competente la Comisión Europea, previo mandato de negociación otorgado por el Consejo de la U.E..

Para finalizar, mencionaremos que los proveedores de servicios de certificación están sometidos a la Directiva 95/46/CE[195] en cuanto a la protección de datos personales de sus clientes. Sólo podrán recabar datos directamente del titular de estos y previo consentimiento explícito de éste, en la medida necesaria para la expedición del certificado. Para otro uso distinto al mencionado, será necesario el consentimiento explícito del titular.

[195] Para su correcta citación, véase nota 51.

CAPÍTULO TERCERO:
LA NORMATIVA ESPAÑOLA SOBRE COMERCIO ELECTRÓNICO, FIRMA DIGITAL, PROTECCIÓN DE DATOS Y PROPIEDAD INTELECTUAL.

I) La Ley de Servicios de la Sociedad de la Información[196].

Continuando con nuestro estudio, nos adentramos a continuación en la reciente y no por ello menos famosa LSSI, en vigor desde el 12 de octubre de 2002 (sin perjuicio de varias disposiciones finales y transitorias que entraron en vigor al día siguiente de su publicación). Ley que durante su elaboración, incluso desde fases muy tempranas (no olvidemos que esta ley ha tenido tres borradores de Anteproyecto de Ley que fueron sometidos a consulta pública[197], amén de otros 25 anteriores), ha suscitado gran polémica en diversos aspectos, tales como, su retraso (de acuerdo con la Directiva 2000/31/CE su transposición debía haberse llevado a cabo antes del 17.1.2002[198]), o su regulación[199], sobre todo en lo referente a las comunicaciones comerciales y a la posibilidad de clausurar la prestación de servicios de S.I., como se verá en su momento, que llegó incluso a ser calificada por algunos como inconstitucional[200]. Posteriormente ha sido modificada en algunos aspectos por la Ley 32/2003 General de Telecomunicaciones, que deroga asimismo a la LGT 11/1998, a la que se hace mención en varios apartados de la obra.

No obstante, aunque a la vista de las referencias indicadas, el Anteproyecto no gustó mucho a algunos sectores, hay que señalar que la LSSI es minuciosa en lo que respecta a la protección de garantías y derechos reconocidos por el ordenamiento jurídico español, como se irá viendo a lo largo de la explicación, así como que va a otorgar una gran confianza a los consumidores, debido al régimen estricto de obligaciones que han de seguir los prestadores de servicios, incluida la inspección por parte de funcionarios y agentes públicos y del estricto régimen sancionador al que se les somete. También deben ayudar las garantías que se ofrecen al consumidor, en cuanto a la fase anterior y posterior a la celebración del

[196] Para su correcta citación, véase nota 5.

[197] Se aportaron al Anteproyecto las apreciaciones de hasta 66 entidades (asociaciones, empresas, colegios profesionales y colectivos), así como de todos los Ministerios (exceptuando los de Ciencia y Tecnología, Economía, Sanidad y Consumo y Justicia, los cuales, fueron los creadores del Anteproyecto), además de los dictámenes preceptivos de acuerdo con la legislación española. En este sentido, Véase Diario ABC de 7 y 8 de febrero de 2002.

[198] No obstante, atendiendo a fuentes gubernamentales, el retraso lo provocó la espera del dictamen preceptivo del CGPJ, el cual, cuando le fue remitido dicho dictamen en octubre de 2001, se encontraba en pleno proceso de renovación. Véase Diario ABC de 16.1.2002. De todos modos, debido a la brevedad de ese retraso, no se puso en marcha el procedimiento de Recurso de Incumplimiento, previsto en los artículos 226-228 del TCE.

[199] A los grupos de la oposición parlamentaria no les gustaba dicho Anteproyecto que veían como intervencionista, al igual que diversas asociaciones del sector que tampoco veían con buenos ojos algunos preceptos de dicho Anteproyecto. Para más información sobre las reacciones de estos, véase Diario ABC de 9.2.2002.

[200] No obstante, el ya mencionado Dictamen del CGPJ, respaldó sin fisuras el Anteproyecto, afirmando que no modifica en absoluto el régimen jurídico preexistente en nuestro ordenamiento jurídico en materia de protección de los Derechos Fundamentales. Igualmente, señaló que debe valorarse positivamente en cuanto reafirma la importancia del respeto a los parámetros de constitucionalidad en toda actividad administrativa que pudiera incidir en los Derechos Fundamentales de la persona. Véase Diario ABC de 16.1.2002.

contrato por vía electrónica, así como el reconocimiento de la validez y eficacia de estos, incluida una regulación jurídica de los aspectos más sensibles de estos contratos. Cabe finalizar, indicando que da más seguridad jurídica a las partes la existencia de una regulación que la ausencia de ésta, por lo que creemos que la LSSI contribuirá en gran medida al desarrollo del C.E. en España, país que, como reflejan las encuestas está a la cola de los países europeos en número de conexiones a Internet[201].

A) Disposiciones Generales. Ámbito de Aplicación[202].

La finalidad que persigue la Ley, es la transposición al ordenamiento español de la Directiva 2000/31/CE, así como la incorporación parcial a éste de la Directiva 98/27/CE, al regular la primera, como ya se vio en su momento, una acción de cesación contra las conductas que contravengan lo establecido en su articulado.

También debemos señalar antes de comenzar su explicación detallada, que la LSSI aspira a regular sólo aquellos aspectos que por su novedad o por sus peculiaridades, no están cubiertos por la legislación preexistente, acogiéndose así al principio de equivalencia funcional que vimos en su momento.

El objeto de la LSSI es regular el régimen jurídico de los servicios de la S.I.[203] y de la contratación por vía electrónica[204] en lo referente a las obligaciones de los

[201] Véase ABC Economía de 17.3.2002, páginas 5 y ss.

[202] Puede encontrarse información sobre la interpretación que el Ministerio de Ciencia y Tecnología da a la LSSI en la siguiente dirección: www.lssi.es .

[203] Atendiendo al Anexo, punto a), entendemos por servicios de la S.I. o servicios: "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la S.I. comprende también los servicios no remunerados por los destinatarios, en la medida en que constituyan una actividad económica del prestador de servicios. **En lo que respecta a este último supuesto, el Ministerio de Ciencia y Tecnología entiende que el servicio no remunerado ha de proporcionar capacidad económica, por lo que entiende que si el servicio de la S.I. se presta con fines de patrocinio o publicidad, estará sometido a esta ley.**

Son servicios de la S.I., entre otros y siempre que representen una actividad económica, los siguientes:

1º La contratación de bienes o servicios por vía electrónica.

2º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3º La gestión de compras en la red por grupos de personas.

4º El envío de comunicaciones comerciales.

5º El suministro de información por vía telemática.

6º El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento del suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán consideración de servicios de la S.I. los que no reúnan las características en el primer párrafo de este apartado y en particular, los siguientes:

1º Los servicios prestados por medio de telefonía vocal, fax o telex.

2º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994 de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE del Consejo, de 3 de octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los E.E.M.M. relativas al ejercicio de actividades de radiodifusión televisiva, o cualquiera otra que la sustituya.

prestadores de servicios[205], incluidos los que actúan como intermediarios[206], en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica[207], la información previa o posterior a la celebración de los contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la S.I..

Las disposiciones de la LSSI deberán entenderse sin perjuicio de lo establecido en otras normas, ya sean estatales o autonómicas ajenas al ámbito normativo coordinado[208] o que tengan como finalidad la protección de la salud o seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor[209], el régimen tributario aplicable a los servicios de la S.I., la protección de datos personales y la normativa reguladora de defensa de la competencia.

Pasando ya a estudiar la segunda parte del epígrafe, que no es otra que el ámbito de aplicación, señalaremos en primer lugar, la regulación referente al prestador de servicios que esté establecido en España.

4º Los servicios de radiodifusión sonora.
5º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de plataformas televisivas.".

[204] Entendemos por contrato celebrado por vía electrónica, de acuerdo con el punto h) del Anexo: "todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectado a una red de telecomunicaciones".

[205] Atendiendo al punto c) del Anexo, éstos son: "persona física o jurídica que proporciona un servicio de la S.I.".

[206] Según el punto b) del Anexo, por servicio de intermediación entendemos: "servicio de la S.I. por el que se facilita la prestación o utilización de otros servicios de la S.I. o el acceso a la información.
Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet".

[207] Según el punto f) del Anexo, éstas son: "toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.
A efectos de esta Ley, no tendrán la consideración de comunicación comercial, los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica".

[208] Atendiendo al punto i) del Anexo, este consiste en. "todos los requisitos aplicables a los prestadores de servicios de la S.I., ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:
1º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismos públicos o privado.
2º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.
No quedan incluidos en este ámbito, las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos".

[209] Atendiendo al punto e) del Anexo, éste es: "persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/84 de 19 de julio, General para la Defensa de los Consumidores y Usuarios". Atendiendo al artículo 1.2 de la citada Ley, son consumidores o usuarios las personas físicas o jurídicas que adquieren, utilizan o disfrutan, como destinatarios finales, bienes muebles o inmuebles, productos, servicios, actividades o funciones, cualquiera que sea la naturaleza pública o privada, individual o colectiva, de quienes los producen, facilitan, suministran o expiden.

Así, la LSSI se aplicará a los prestadores de servicios establecidos en España y a los servicios prestados por ellos. Se entenderá que el prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios; en caso contrario se atenderá al lugar en que se realice dicha gestión o dirección.

También será de aplicación esta Ley, a los servicios que sean prestados en España a través de un establecimiento permanente, por prestadores de servicios establecidos o domiciliados en otro Estado. Se entenderá que tiene un establecimiento permanente en territorio español, si dispone de forma continuada o habitual de instalaciones o lugares de trabajo, en los que realiza todo o parte de su actividad. No obstante, la utilización de medios tecnológicos situados en España, para la prestación o acceso al servicio, no bastan por sí solos para determinar el lugar de establecimiento. De la misma manera, se presumirá que está establecido en España cuando el prestador o alguna de sus sucursales se hayan inscrito en el Registro Mercantil u otro registro público español, en el que fuera necesaria su inscripción para la adquisición de la personalidad jurídica.

Finalizaremos lo concerniente a los prestadores de servicios establecidos en España, citando una obviedad de la LSSI, que más bien se utiliza en aras de clarificar el régimen jurídico de estos prestadores, ya que como es lógico, la LSSI dispone que a estos, les será de aplicación el resto del ordenamiento jurídico español que pudiera serles de aplicación, en función de la actividad que desarrollen.

En lo referente a los prestadores de servicios establecidos en otro E.E.M.M. u otro país del Espacio Económico Europeo (EEE)[210], sin perjuicio de lo dispuesto en los artículos 7.1 (libre prestación de servicios) y 8 (restricciones a la libre prestación de servicios), que se estudiarán más adelante, se aplicará la LSSI cuando el destinatario del servicio[211] radique en España y los servicios afecten a las materias siguientes:

a) derechos de la propiedad intelectual o industrial,
b) emisión de publicidad por instituciones de inversión colectiva,
c) actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios,
d) obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores,

[210] Es una zona de libre cambio que se encuentra formada por los países que pertenecían a la antigua EFTA, que fue quedando desfigurada al ingresar en la entonces CEE, Reino Unido, Dinamarca, Irlanda, Portugal y ya en la actual Comunidad Europea, Austria y Suecia. En la actualidad se encuentra formado por Suiza, Noruega, Islandia y Liechtenstein.

[211] De acuerdo con el punto d) del Anexo, éste es: "persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la S.I.".

e) régimen de elección por las partes contratantes de la legislación aplicable al contrato,
f) licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, no solicitadas.

Sin perjuicio de lo anterior, hágase saber que en cuanto a la constitución, transmisión, modificación o extinción de derechos reales sobre bienes inmuebles sitos en España, han de respetarse las normas formales para su validez y eficacia, así como todas las normas que afecten a una de las materias citadas anteriormente, salvo que de conformidad con las normas reguladoras de estas materias, no sea de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Por último, nos toca referirnos al supuesto que nos queda por analizar, que no es otro que el prestador de servicios establecido en un Estado que no pertenece ni a la U.E., ni al EEE. Para estos, baste decir que su sujeción a la ley derivará de lo dispuesto en los acuerdos y convenios internacionales, cuando el servicio se dirija específicamente a España.

Finalizaremos el epígrafe refiriéndonos a las materias que están excluidas del ámbito de aplicación de la LSSI, y que por ello estarán reguladas por su propia normativa:

a) los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas,
b) los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

En cuanto a los juegos de azar, estarán exceptuados de la LSSI, si proceden de un prestador de servicios establecido en un E.E.M.M. o en un país del EEE, pero no, si son prestados por un prestador de servicios establecido en España, si implican apuestas de valor económico, eso sí, sin perjuicio de lo establecido en la normativa estatal o autonómica en la materia. Puede lógicamente chocar al lector este supuesto, sobre todo en lo referente a la exclusión operada. Cabe responder indicando que en el Anteproyecto de Ley, los juegos de azar estaban totalmente excluidos, en consonancia con la Directiva 2000/31/CE como vimos en su momento. Pero durante su tramitación parlamentaria la Asociación de Usuarios de Internet lanzó una campaña en contra de su exclusión, ya que observaron que existían problemas de control de la publicidad que emitían los cibercasinos a través de los *banners* de publicidad, en lo referente a la protección de los menores. Al investigar la problemática pusieron de manifiesto que, a excepción de Ceuta y Melilla donde las competencias la ejerce la Comisión Nacional del Juego, en el resto son las Comunidades Autónomas las que han recogido la competencia. Desagraciadamente, éstas no han regulado la materia ya que argumentan que la realidad de Internet les sobrepasa y de ahí viene la conveniencia de realizar una

mención especial a este supuesto, eso sí, dejando claro que es necesario una normativa especifica en la materia, como se recoge en la enmienda que presentó el Grupo Parlamentario Popular y que fue aprobada en los términos indicados[212].

B) Materias Reguladas. Relación con la Ley 47/2002 y el R.D. 1906/1999.

Comenzaremos este epígrafe, refiriéndonos al principio que ha de regir en cuanto a la prestación de servicios de la S.I., que no es otro que el de no autorización previa. De esta manera, éste principio se aplicará sin perjuicio de los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto exclusivo y específico la prestación por vía electrónica de estos servicios.

Este principio, rige también para los prestadores de servicios establecidos en un E.E.M.M. o país del EEE, para las materias reguladas por el ámbito coordinado, con la excepción de los supuestos del artículo 3, (ya estudiado) y artículo 8.

Para los prestadores de servicios no establecidos en la U.E. o EEE, habrá que estar, como ya se indicó, a lo dispuesto por los acuerdos y convenios internacionales que resulten de aplicación.

En cuanto a las restricciones que pueden hacerse de este principio (reguladas en el artículo 8), los órganos competentes[213] para su protección, en el ejercicio de las atribuciones que tengan legalmente establecidas, podrán adoptar medidas tendentes a interrumpir la prestación del servicio o retirar los datos que vulneran o pueden vulnerar uno de los siguientes principios:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social.
d) La protección de la juventud y de la infancia.

Como no podía ser de otra manera, en lo referente a la adopción de las medidas mencionadas, habrán de respetarse en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento español para proteger los derechos a la intimidad personal y familiar, la protección de los datos personales y a la libertad de expresión o información, cuando estos puedan verse afectados. De igual manera,

[212] Véase en este sentido, Diario ABC Tecnología de 24.4.2002, página 45 y ABC Tecnología de 21.3.2002, página 7.

[213] El Anteproyecto recogía al igual que la Directiva 2000/31/CE, el término autoridad competente. Término que fue sustituido por el actual debido a las críticas de los grupos de la oposición parlamentaria, para los cuales, el término poseía connotaciones preconstitucionales.

cuando el ordenamiento jurídico atribuya competencia a los órganos jurisdiccionales en las materias señaladas, sólo éstos podrán ejecutar la restricción a la libre prestación de servicios.

Las medidas de restricción deberán ser objetivas, proporcionales y no discriminatorias, pudiéndose adoptar de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a la normativa procesal o administrativa, según sea el caso.

Para garantizar la correcta aplicación de una resolución de interrupción de la prestación de un servicio o la retirada de datos de un prestador de servicios establecido en otro Estado, el órgano competente podrá ordenar a los prestadores de servicios de intermediación establecidos en España, directamente o por solicitud motivada del Ministerio de Ciencia y Tecnología, que tomen las medidas necesarias para impedir dicho acceso.

Por el contrario si el prestador de servicios está establecido en España, habrá que estar a lo dispuesto en el artículo 11, referente al deber de colaboración de los prestadores de servicios de intermediación, supuesto regulado de forma idéntica al que nos ocupa, por lo que omitiremos su estudio para no ser repetitivos. La única salvedad es que también se regula la posibilidad de que el órgano competente disponga que el prestador de servicios de intermediación ha de colaborar en la interrupción de un servicio prestado por un prestador establecido en España.

Al margen de los procesos judiciales, cuando se trate de interrumpir la prestación de un servicio suministrado por un prestador de servicios establecido en un E.E.M.M. o país del EEE, habrá de seguirse el procedimiento siguiente:

El órgano competente requerirá al E.E.M.M. en el que esté establecido el prestador del servicio afectado, a que adopte las medidas oportunas. Si no las adopta o lo hace de manera insuficiente, dicho órgano notificará con carácter previo, a la Comisión Europea, o en su caso, al Comité Mixto del EEE y al Estado en cuestión, las medidas que piensa adoptar. No obstante, en el supuesto de urgencia, este órgano podrá adoptar medidas al margen del procedimiento indicado, debiendo notificarlas en un plazo máximo de 15 días, , siendo requisito indispensable que justifique las razones de tal urgencia.
Las notificaciones aludidas anteriormente, deberán canalizarse por el órgano competente en la Administración General del Estado para la comunicación y transmisión de información a las Comunidades Europeas[214].

Avanzando en nuestro estudio de la regulación jurídica a la que se somete a los prestadores de servicios de la S.I., pasamos a continuación a referirnos a las obligaciones que se imponen a estos.

[214] Es obvio decirlo, pero indicaremos que dicho órgano es la Secretaria de Estado para Asuntos Europeos.

En primer lugar deben dejar constancia registral del nombre de dominio si están establecidos en España, debiendo comunicar en el plazo de un mes al Registro Mercantil en el que se encuentren inscritos o aquel otro registro público en el que lo estuvieran a efectos de obtener la personalidad jurídica o a los meros efectos de publicidad, al menos, un nombre de dominio o dirección de Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información ya conste en el registro. Para los actos mencionados, será de aplicación la normativa vigente en materia registral. En este supuesto se nos plantea que ocurre con los Profesionales Liberales y Autónomos que usen un dominio, ya que la inmensa mayoría de ellos no se encuentran inscritos en ningún Registro Público. Es por ello que estarán exentos de dicha obligación, en tanto en cuanto por vía reglamentaría no se establezca una solución a esta laguna legal.

Además, sin perjuicio de los requisitos ya establecidos en la legislación preexistente, los prestadores de servicios deberán poner al alcance de los destinatarios del servicio y de los órganos competentes, la siguiente información, de manera que puedan acceder a ella por medios electrónicos, de forma permanente, fácil, directa y gratuita:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
b) Los datos de su inscripción en el Registro Mercantil.
c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.
d) Si ejerce una profesión regulada[215], deberá indicar:

1º Los datos del colegio Profesional al que, en su caso, pertenece y número de colegiado.
2º El título académico oficial o profesional con el que cuenta.
3º El Estado de la U.E. o del EEE en el que se expidió dicho título, y en su caso, la correspondiente homologación o reconocimiento.
4º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.
f) Información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables, y en su caso, los gastos de envío.
g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

[215] Atendiendo al punto g) del Anexo, entendemos por ésta: "toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias".

Para el cumplimiento de estos requisitos de información, bastará con que el prestador de servicios los refleje en su página o sitio de Internet.

Como ya se reseñó en el capítulo primero, la LSSI impone a los operadores de redes y servicios de comunicaciones electrónicas, a los proveedores de acceso a redes de telecomunicaciones y a los prestadores de servicios de alojamiento de datos, la obligación de almacenar y retener los datos sobre el tráfico y la conexión relativos a las comunicaciones electrónicas por un periodo máximo de 12 meses. Estos datos deben ser los necesarios para facilitar la localización del equipo terminal empleado por el usuario para transmitir la información, en el caso de los operadores de redes y proveedores de acceso, y los imprescindibles para identificar el origen de los datos alojados y el momento en el que se inició la prestación en el caso de los servicios de alojamiento de datos, pero en ningún caso, podrá afectar al secreto de las comunicaciones.

Estos datos, sólo podrán utilizarse en el marco de una investigación criminal o para la salvaguarda de la seguridad pública o defensa nacional, poniéndose a disposición de los Jueces, Tribunales o Ministerio Fiscal cuando así lo requieran. Si por el contrario, son los Cuerpos y Fuerzas de Seguridad los que los requieren, deberá estarse a lo dispuesto en la normativa sobre protección de datos.

Corresponde a los encargados de la retención de los datos su custodia, debiendo impedir su acceso no autorizado, perdida o alteración, estando obligados a no usar esos datos para otros fines que los que expresamente se han indicado.

Para la aplicación de este artículo, en aspectos tales como, la categoría de datos que deben conservarse, el plazo de retención para cada supuesto, las condiciones de almacenaje, tratamiento, custodia o destrucción, así como la manera de entrega a los órganos competentes, habrá que estar a lo que se determine reglamentariamente.

Pasamos a continuación a centrarnos en el régimen de responsabilidad aplicable a los prestadores de servicios. Para éstos, la LSSI establece que, sin perjuicio de lo dispuesto en esta Ley, les será de aplicación además, las reglas de la responsabilidad civil, penal y administrativa establecidas con carácter general en el ordenamiento jurídico. Además de esta responsabilidad, pueden tenerla también en los casos que veremos a continuación.

Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en retransmitir datos, facilitados por el destinatario del servicio, por una red de telecomunicaciones, o en facilitar el acceso a ésta, no serán responsables por la información transmitida, salvo que ellos mismos la hayan originado, modificado o seleccionado los datos o los destinatarios de estos. No se entenderá por modificación la manipulación estrictamente técnica de los archivos que tienen los datos durante su transmisión. De igual modo, las actividades de transmisión y

provisión incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que se utilicen para permitir la transmisión y por el tiempo estrictamente necesario para ello.

Otro supuesto es el de la copia temporal de los datos facilitados por los usuarios, así de esta manera, los prestadores de servicio de intermediación, que con la única finalidad de facilitar la ulterior transmisión de datos facilitados por el destinatario, los almacenen de forma provisional, temporal y automática, no serán responsables por el contenido ni la reproducción temporal de los mismos sí:

a) No modifican la información.
b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.
c) Respeten las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.
d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información.
e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.
2º Que se ha imposibilitado el acceso a ella.
3º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

El tercer supuesto que nos ocupa, corresponde al alojamiento o almacenamiento de datos por parte de los prestadores de servicios de intermediación que presten el servicio de alojamiento de datos a petición del destinatario. Éstos no serán considerados responsables, siempre que:

a) No tengan conocimiento efectivo que la actividad o la información almacenada es ilícita o que lesiona bienes o derechos de un tercero susceptibles de indemnización o,
b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Para determinar cuando el prestador tiene conocimiento efectivo, servirá con que un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos o se hubiera declarado la existencia de la lesión y el prestador tuviera conocimiento de la correspondiente resolución, sin perjuicio de los procedimientos que los prestatarios apliquen a la detección y retirada de contenidos basados en acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Para que opere en todo caso esta exención de responsabilidad, el destinatario del servicio no deberá haber actuado bajo la dirección, autoridad o control del prestador.

El último supuesto regulado, es el de la responsabilidad de los prestadores que faciliten enlaces a contenidos o instrumentos de búsqueda. Éstos no serán responsables, siempre que:

a) No tengan conocimiento efectivo que la actividad o la información a la que remiten o recomiendan es ilícita o que lesiona bienes o derechos de un tercero susceptibles de indemnización o,
b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Para determinar cuando el prestador tiene conocimiento efectivo, se aplicarán las mismas reglas que en el supuesto anterior. De igual manera deberá actuarse para operar la exención de responsabilidad.

A continuación, veremos la regulación referente a los códigos de conducta, que se recoge en la LSSI. Corresponde a las Administraciones Públicas fomentar la creación voluntaria de estos códigos[216], por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas por esta Ley. Corresponde esta tarea a la Administración General del Estado, cuando estos códigos sean de carácter comunitario o internacional.

Podrán tratar en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como, de los procedimientos extrajudiciales de solución de conflictos.
Deberá garantizarse que, en el proceso de elaboración intervienen las asociaciones de consumidores y usuarios y las organizaciones representativas de las personas discapacitadas físicas o psíquicas cuando afecten a sus respectivos intereses.

[216] En este sentido, se ha constituido en Barcelona la Agencia de Calidad y Autorregulación de Internet. Este organismo está auspiciado por la Comisión Nacional del Mercado de las Telecomunicaciones, la Secretaria de Telecomunicaciones y S.I. de la Generalidad de Cataluña, el Consejo Audiovisual de Cataluña, corporaciones locales, colegios profesionales y el Consejo Audiovisual de Andorra, entre otros. Pretende elaborar un código de conducta entre todos los actores de Internet, para evitar una mayor regulación de la red. Para ello, se elaborarán una serie de principios a partir de los derechos de los ciudadanos, se fomentará la autorregulación de contenidos, se mediará en los conflictos, se crearán patrones contractuales, se elaborarán certificados de calidad, etc. Las empresas y organizaciones que se acojan a los principios establecidos, recibirán un sello de calidad. Cien organizaciones se han acogido ya a la elaboración de este código, que contará con una oficina de defensa de la audiencia, cuya finalidad será recibir quejas o sugerencias de los ciudadanos. Véase Diario ABC de 2.10.2002, página 45 y www.iqua.net . Otro Código de Conducta a destacar, es el de Confianza OnLine, que puede ser consultado en la dirección www.confianzaonline.org y en Diario ABC Tecnología de 4 de diciembre de 2002, pág. 50. Posteriormente han aparecido otros Códigos como el de la Asociación Española de Normalización (AENOR), que pueden ser consultados en la página Web del Ministerio de Ciencia y Tecnología: www.lssi.es .

Deberá tenerse en cuenta la protección de menores y de la dignidad humana, cuando el contenido pueda afectarles, siendo posible la elaboración de códigos específicos para la defensa de estos intereses.

Los códigos deberán ser accesibles por vía electrónica y se fomentará su traducción a otras lenguas comunitarias para facilitar su difusión.

Pasamos a continuación a uno de los temas que más polémica suscitó, por parte de las asociaciones del sector, antes y durante la tramitación parlamentaria de la LSSI, tema que no es otro, que el de las comunicaciones comerciales por vía electrónica, que han sido modificadas en parte por la Ley General de Telecomunicaciones, para adaptar su regulación a lo establecido en la Directiva 2002/58/CE, que como vimos en su momento, establece un régimen levemente diferente al regulado en la Directiva de Comercio Electrónico.

Éstas se regirán, además de lo dispuesto por la presente Ley, por su normativa propia y vigente en materia comercial y de publicidad. En todo caso, será de aplicación la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales[217]. Y es que este tipo de comunicaciones plantean dos problemas diferenciados, por un lado el de la protección de datos de carácter personal, en tanto en cuanto el destinatario sea una persona física en el sentido de dónde y cómo se ha obtenido su dirección de correo electrónico, y si media consentimiento del afectado, y el segundo problema es el del *spam*, práctica que como se vio en su momento, puede bloquear el servidor del receptor o del emisor.

Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y deberán indicar la persona física o jurídica en el nombre de la cual se realizan. Si ésta se realiza por correo electrónico u medio de comunicación electrónica equivalente, deberán incluir al comienzo del mensaje la palabra "publicidad[218]".

En los supuestos de ofertas promocionales, como las que incluyen descuentos, premios o regalos, además del cumplimiento de los requisitos anteriores, será necesaria la autorización correspondiente previa, así como, que las condiciones de acceso y participación se fijen de manera clara e inequívoca.

[217] Recuérdese que la Directiva 2002/58/CE establece un marco para las comunicaciones comerciales electrónicas, con lo que, cuando dicha Directiva sea transpuesta al ordenamiento jurídico español, afectará al régimen jurídico aplicable a éstas.

[218] Para el Ministerio de Ciencia y Tecnología, la palabra "Publicidad" debe ir en el Asunto del Mensaje, por lo que recomendamos que hasta que no se apruebe el Reglamento de Desarrollo de la LSSI y éste no disponga otra cosa, se cumpla la interpretación dada por el Ministerio a esta disposición.

En todo caso, estas comunicaciones publicitarias o promocionales estarán prohibidas si se envían a través de correo electrónico u otro medio de comunicación electrónica equivalente, salvo autorización o solicitación expresa por parte del destinatario[219], salvo que exista una relación contractual previa y el prestador haya obtenido de manera lícita los datos de contacto del destinatario, y los emplee para comunicaciones referentes a productos o servicios de su propia empresa que sean similares a los del objeto del contrato. No obstante, el prestador deberá ofrecer al destinatario la posibilidad de negarse a ese tratamiento por un procedimiento sencillo y gratuito, tanto en el momento de la recogida de datos, como en cada una de las comunicaciones comerciales que remita.

Es más, el destinatario podrá revocar en cualquier momento el consentimiento prestado, con la simple comunicación de esa voluntad al remitente. Para ello se le deberá poner a su disposición un mecanismo sencillo y gratuito e informarle por medios electrónicos sobre esos mecanismos.

Cuando los prestadores empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales (como el uso de identificadores o *cookies)*, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciendo la posibilidad de rechazar el tratamiento mediante un procedimiento sencillo y gratuito, salvo que se realice para efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas, o en la medida en que resulte necesario para la prestación de un servicio de SI expresamente solicitado por el destinatario.

Para finalizar el epígrafe, realizaremos el estudio del régimen jurídico de la contratación electrónica.

En primer lugar, hay que señalar que la LSSI dispone que los contratos celebrados por vía electrónica serán validos y eficaces, siempre que concurran los requisitos del consentimiento y demás necesarios para su validez, de acuerdo con el ordenamiento jurídico español, salvo los contratos relativos a derecho de familia y sucesiones o los contratos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran la intervención de notarios, registradores de la propiedad y mercantiles, autoridades públicas u órganos jurisdiccionales, supuestos que se regirán por su normativa específica.

[219] Como se ha indicado, este precepto causó polémica. En este sentido, cabe citar la opinión que al respecto tenían las tiendas virtuales. Éstas criticaron la prohibición del *spam*, salvo consentimiento expreso del usuario, ya que según ellos, las empresas de Estados Unidos pueden mandar a España comunicaciones comerciales no deseadas, en base a que la prohibición sólo afecta a las empresas españolas, con lo que les provocaría una desventaja competitiva. No obstante, cabe esperar y desear que se desarrollen convenios internacionales para que puedan aplicarse los supuestos regulados en los artículos 4 y 7.2 sobre prestadores de servicios establecidos en países que no son miembros de la U.E., ni del EEE. Para más información, véase El País de los Negocios de 10.2.2002, página 9.

Los contratos, aparte de los del inciso anterior, se regirán por lo dispuesto en la LSSI, Códigos Civil y de Comercio, así como el resto de disposiciones civiles y mercantiles sobre contratos, en especial, las normas de protección de consumidores y usuarios y de ordenación de la actividad comercial. Como vimos en su momento al explicar el mismo supuesto en la Directiva 2000/31/CE y la Directiva 97/7/CE, toda esta normativa completa a la LSSI, en la medida en que no exista regulación al respecto incluida en ésta. El supuesto de transposición al ordenamiento jurídico español de esta última Directiva, lo analizaremos al final del epígrafe.

No es requisito indispensable para la validez de los contratos electrónicos que las partes pacten anteriormente la utilización de estos.

Siempre que la Ley exija que el contrato o cualquier información relacionada con éste conste por escrito, se entenderá satisfecho este requisito, si estos se contienen en un soporte electrónico.

En lo referente a la prueba de estos contratos, se estará a lo dispuesto en el ordenamiento jurídico español y, en su caso, a lo establecido en la legislación de firma electrónica, como se verá mas adelante. No obstante, bajo ningún concepto podrá negarse el valor probatorio como prueba documental en un juicio, al contrato que conste en un soporte electrónico, cuestión que podría haberse omitido ya que, según el artículo 299.2 de la Ley de Enjuiciamiento Civil de 2000, éstos serían admisibles como prueba, amén del apartado 3 de dicho artículo que permite la admisibilidad de aquellos medios que no estén creados en el momento de aprobación de la Ley.

También el Tribunal Supremo en sus sentencias de 3 de octubre y 11 de noviembre de 1997 declaró la admisibilidad de éstos, siempre que pueda garantizarse la autenticidad y autoría del documento, en especial, la firma de quien asume su contenido y la efectividad de su clausulado y esto es posible, como ya se vio en su momento, por el uso de la F.D. y la criptografía.

Una de las grandes innovaciones de esta Ley con respecto a la Directiva 2000/31/CE, es que posibilita a las partes a que pacten que un tercero de confianza archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y hora en que dichas comunicaciones han tenido lugar, intervención que nunca podrá alterar ni sustituir, como se vio en su momento, a las personas facultadas por el ordenamiento jurídico para emitir fe pública. El tercero debe archivar las declaraciones por el tiempo estipulado por las partes sin que, en ningún caso, pueda ser inferior a 5 años (téngase en cuenta que es el plazo mínimo de prescripción de acciones en nuestro derecho)[220]. Al tratarse de una innovación de la LSSI con respecto a la Directiva, no hemos encontrado en las legislaciones de

[220] En virtud de esta disposición, ya poseemos en España una empresa que se dedica a esta práctica. Se denomina Terceros de Confianza. Puede encontrarse información sobre su actividad en www.tercerosdeconfianza.com.

transposición de los distintos E.E.M.M. una disposición semejante a la descrita. No obstante, el que no se encuentre expresamente admitida esta posibilidad, no impide su validez jurídica en las distintas legislaciones[221].

En cuanto a la ley aplicable al contrato, como no podía ser de otro modo, se estará a la normativa sobre derecho internacional privado vigente en nuestro ordenamiento, debiéndose tomar en consideración lo dispuesto en los artículos 2 y 3, que como ya se vio, regulan el ámbito de aplicación de esta Ley.

La LSSI regula igualmente la información que el prestador de servicios debe poner a disposición del destinatario, antes y después de la celebración del contrato.

En cuanto a la información anterior a la realización del contrato, debe ser puesta a disposición del destinatario de manera clara, comprensible e inequívoca la siguiente información:

a) Los distintos trámites que deben seguirse para celebrar el contrato.
b) Si el prestador va a archivar el documento electrónico donde se formalice el contrato y si éste va a ser accesible.
c) Los medios técnicos que se ponen a su disposición para identificar y corregir errores en la introducción de datos.
d) La lengua o lenguas en las que podrá formalizarse el contrato.

No obstante, el prestador no estará obligado a suministrar dicha información en los casos siguientes:

a) Si ambos contratantes así lo acuerdan y ninguno de ellos tiene la condición de consumidor.
b) El contrato se ha celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no son empleados con el exclusivo propósito de eludir la obligación.

En lo referente a las ofertas o propuestas de contratación realizadas por vía electrónica, hay que indicar que, sin perjuicio de lo dispuesto en la legislación específica, éstas serán validas durante el periodo que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios.

También deberán ser accesibles con antelación a la formalización del contrato las condiciones generales por las que se rige el contrato[222], de manera que puedan ser

[221] Según se desprende de las consultas realizadas a los 15 Euro Info Centros integrados en el Proyecto www.ebusinesslex.net .

[222] La definición de las condiciones generales de la contratación, la encontramos en el artículo 1º de la Ley 7/1998 de 13 de abril Sobre condiciones generales de la contratación, BOE 89 de 14.4.1998. Atendiendo a este artículo son condiciones generales de la contratación, las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes, con independencia de la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos. El hecho de que ciertos elementos de una cláusula o que una o varias cláusulas aisladas se hayan

almacenadas y reproducidas por el destinatario. En este apartado, tenemos que traer a colación al Real Decreto 1906/1999 de 17 de diciembre, sobre la contratación telefónica o electrónica con condiciones generales, en desarrollo del artículo 5.3 de la ley 7/1998 de 13 de abril, de condiciones generales de la contratación[223]. Este artículo establece que "en los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad e firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma". Para dar cumplimiento a esta disposición, el Real Decreto establece que previamente a la celebración del contrato y con antelación necesaria, como mínimo de 3 días naturales anteriores a aquella, el predisponente deberá facilitar al adherente información de modo veraz, eficaz y completo, sobre todas las cláusulas del mismo y remitirle, de modo adecuado a la técnica de comunicación a distancia empleada, el texto completo de las condiciones generales. Continua el Real Decreto imponiendo la obligación al predisponente de remitir al adherente, inmediatamente la justificación del contrato celebrado incluyendo toda la información pactada en el mismo, así como soportar la carga de la prueba en cuanto al cumplimiento de estas obligaciones. Concede igualmente un derecho de resolución al adherente de 7 días hábiles, sin penalización alguna, incluso en lo que se refiere a los gastos de devolución del bien. No entraremos en detalle en la regulación contenida en el Real Decreto, ya que, como dispone la disposición final quinta de la LSSI, el Gobierno en el plazo de un año deberá adecuarlo a lo dispuesto en la LSSI.

Realizado este inciso, volvemos a la información posterior a la celebración del contrato que debe facilitarse a tenor de la LSSI.

En virtud de ésta, el oferente está obligado a confirmar la recepción de la aceptación de la oferta al que la hizo por alguno de los medios siguientes:

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 un plazo de 24 horas siguientes a la recepción de la aceptación.
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 el destinatario.

---

negociado individualmente no excluirá de la aplicación de esta ley al resto del contrato si la apreciación global lleva a la conclusión de que se trata de un contrato de adhesión. Téngase también en cuenta el Real Decreto 1828/1999 de 3 de diciembre por el que se aprueba el Reglamento del Registro de Condiciones Generales de la Contratación, BOE 306 de 23 de diciembre de 1999, para dar cumplimiento al artículo 11 de la ley.

[223] BOE 313 de 31 de diciembre de 1999.

No obstante, si en algún caso fuera el destinatario del servicio el obligado a emitir la confirmación, el prestador debe facilitar su cumplimiento, poniendo a disposición del destinatario alguno de los medios indicados anteriormente. Esta obligación es exigible tanto si la confirmación ha de remitirse al prestador de servicios o a otro destinatario.

Para determinar cuando se han recibido la confirmación y la aceptación, habrá que aplicar la máxima de que la recepción se produce en el momento en que las partes tienen constancia de éstas. Esta constancia, se presumirá para el destinatario del servicio en los casos en que es obligatorio el acuse de recibo, cuando el acuse sea almacenado en el servidor en el que esté dada de alta su cuenta de correo electrónico, en el dispositivo utilizado para la recepción de comunicaciones.

No será necesario confirmar la recepción de la aceptación de la oferta cuando ambos contratantes así lo acuerden, siempre que ninguno posea la condición de consumidor o el contrato se realice exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, siempre que estos medios no se utilicen para eludir el cumplimiento de la obligación.

Finalizaremos este apartado refiriéndonos al lugar donde se celebra el contrato. A tenor de la LSSI, los contratos celebrados por vía electrónica en los que una parte sea consumidor, se presumirán celebrados en el lugar en el que éste tenga fijada su residencia habitual. Si por el contrario son celebrados entre empresarios o profesionales se presumirán, salvo pacto en contra, celebrados en el lugar donde esté establecido el prestador de servicios.

Un supuesto de especialidad en esta materia, lo introduce la Ley 47/2002 de 19 de diciembre, de reforma de la Ley 7/1996 de 15 de enero de Ordenación del Comercio Minorista (LOCM), para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE en materia de contratos a distancia y para la adaptación de la Ley a diversas Directivas comunitarias[224]. Como ya vimos en su momento cuando estudiamos la relación entre las Directivas 2000/31/CE y 1997/7/CE, la legislación a aplicar cuando se vendan o suministren bienes o servicios por medios electrónicos, será preferentemente la de Servicios de la Sociedad de la Información y del Comercio Electrónico (artículo 38.6 de la Ley 47/2002). No obstante en nuestra opinión, teniendo en cuenta que la prestación o suministro de bienes y servicios a través de Internet, siempre se realiza a distancia, entendemos que esta ley completará a la LSSI en lo no previsto por ésta, y en todo aquello que no le esté atribuido en exclusividad (por poner un ejemplo, el artículo 38.7 se remite a la normativa sobre comunicaciones electrónicas de la LSSI con carácter de exclusividad, aunque la LOCM dispone de normativa propia). Es por ello que sólo vamos a dar algunas pinceladas sobre la ley.

[224] BOE 304 de 20 de diciembre de 2002.

Comenzaremos indicando que esta Ley se aplica a los contratos de compraventa cuando el vendedor sea un comerciante y el comprador un consumidor[225] (artículo 1.2 de la LOCM).

Lo que realmente nos interesa de esta reforma, es lo que se refiere a la regulación jurídica de las "ventas a distancia", puesto que este supuesto se da en los servicios de la S.I.. Según el artículo 38 de esta ley, se entenderá por venta a distancia la celebrada sin la presencia física simultanea del comprador y el vendedor, siempre que su oferta y aceptación se realicen de forma exclusiva a través de una técnica cualquiera de comunicación a distancia y dentro de un sistema de contratación a distancia organizado por el vendedor.

Un elemento a destacar, es la exoneración del deber de registrarse en el Registro de Empresas de venta a distancia[226], que funciona en el Ministerio de Hacienda, para todas aquellas empresas cuyas ofertas de venta abarquen el territorio de más de una Comunidad Autónoma.

En otro orden de cosas, el artículo 40 dispone una serie de datos informativos que el vendedor debe suministrar al comprador previamente a la celebración del contrato, que a nuestro entender es conveniente suministrar conjuntamente con los que dispone la LSSI (artículo 27). Filtrando los que ya se contienen en el apartado estudiado de la LSSI, o bien ya debe disponer el comprador, por ser datos identificativos que aparecen en la página Web del Prestador de Servicios de la S.I. (artículo 10 de la LSSI), mencionamos los siguientes:

- Las características esenciales del producto.
- El precio, incluidos todos los impuestos.
- Los gastos de entrega y transporte, en su caso.
- La forma de pago y las modalidades de entrega y ejecución
- La existencia de un derecho de desistimiento o resolución (en virtud del artículo 44, el comprador dispone de 7 días –como regla general- para valorar el producto, sin penalización alguna y sin deber notificar los motivos de este desistimiento), o su ausencia en los contratos a que se refiere el artículo 45.
- El coste de utilización de la técnica de comunicación a distancia, cuando se calcule sobre una base distinta de la tarifa básica.
- El plazo de validez de la oferta y el precio.
- La duración mínima del contrato si procede, cuando se trate de contratos de suministro de productos destinados a su ejecución permanente o repetida.
- En su caso, si el vendedor está adherido o dispone de algún procedimiento de resolución extrajudicial de conflictos.

[225] Para una correcta definición de consumidor, véase nota 209.

[226] Creado a tal efecto por el Real Decreto 1133/1997 de 11 de julio, por el que se regula la autorización de las ventas a distancia y la inscripción en el Registro de empresas de venta a distancia previsto en el artículo 38.2 de la Ley 7/1996 de 15 de enero, de Ordenación del Comercio Minorista, BOE 177 de 25.7.1997, modificado por el Real Decreto 1976 de 18 de septiembre, BOE 239 de 6.10.1998.

Para evitar abusos, se establece con carácter imperativo que en ningún caso, la falta de respuesta a la oferta de venta a distancia podrá considerarse como una aceptación de ésta. En caso de producirse el envío, éste se tendrá por no solicitado, no estando el receptor obligado ni a pagar el precio, ni a devolver el producto.

Finalizaremos el breve estudio de la Ley 47/2002 indicando que, se prevé la posibilidad de anular pagos realizados mediante tarjeta, cuando el importe de una compra hubiera sido cargado fraudulenta o indebidamente al titular de la misma. Para evitar abusos por parte del Titular de la tarjeta, si se demuestra que efectivamente la compra fue realizada por él, además de soportar el importe de la misma, responderá por daños y perjuicios ocasionados por la anulación ante el vendedor.

C) Aplicación de la LSSI.

A continuación nos referiremos a un conjunto de preceptos, que pretenden otorgar eficacia a la LSSI, en materias, tales como, la solución judicial o extrajudicial de conflictos, procedimiento de información y control o el régimen sancionador por el incumplimiento de las disposiciones reguladas en la Ley.

Comenzaremos con la regulación referente a la acción de cesación, que podrá interponerse contra las vulneraciones de las disposiciones de la presente Ley, cuando lesionen los intereses colectivos o difusos de los consumidores[227].

Esta acción tendrá como finalidad conseguir una sentencia que condene al demandado a cesar en la conducta contraria a la LSSI y a prohibir su reiteración en el futuro. Podrá igualmente interponerse contra una vulneración ya finalizada cuando existan indicios suficientes que hagan pensar que su reiteración es probable a corto plazo. Sobre el procedimiento de este tipo de acciones, habrá que estar a la regulación que impone para éstas, la Ley de Enjuiciamiento Civil.

Están legitimados para interponerla los siguientes sujetos:

a) Las personas físicas o jurídicas titulares de un derecho o interés legítimo.

[227] Para dar cumplimiento a esta obligación legal, se ha promulgado la Ley 39/2002 de 28 de octubre, de transposición al ordenamiento jurídico español de diversas directivas comunitarias en materia de protección de los intereses de los consumidores y usuarios. BOE de 29.10.2002. En virtud de esta ley, se reforman varia leyes para posibilitar la acción de cesación. Las leyes reformadas son la Ley 1/2000 de 7 de enero de Enjuiciamiento Civil, Ley 7/1998 de 13 de abril, de Condiciones Generales de la Contratación, Ley 26/1984 de 19 de julio, General de Defensa de los Consumidores y Usuarios, Ley 26/1991 de 21 de noviembre, sobre contratos celebrados fuera de establecimientos mercantiles, Ley 21/1995 de 6 de julio, reguladora de los Viajes Combinados, Ley 42/1998 de 15 de diciembre, sobre derechos de aprovechamiento por turno de bienes inmuebles de uso turístico y normas tributarias, Ley 25/1990 de 20 de diciembre, del Medicamento, Ley 25/1994 de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552 CEE, sobre la coordinación de disposiciones legales, reglamentarias y administrativas de los Estados Miembros relativas al ejercicio de actividades de radiodifusión televisiva, Ley 34/1988 de 11 de noviembre, General de Publicidad y Ley 7/1995 de 23 de marzo, de Crédito al Consumo.

b) Los grupos de consumidores o usuarios afectados, en los casos y condiciones previstos en la Ley de Enjuiciamiento Civil.
c) Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la Ley 26/1984, de 19 de julio General para la Defensa de los Consumidores y Usuarios o, en su caso, en la legislación autonómica en materia de defensa de consumidores.
d) El Ministerio Fiscal.
e) El Instituto Nacional de Consumo y los órganos correspondientes de las Comunidades Autónomas y de las Corporaciones Locales competentes en materia de defensa de los consumidores.
f) Las entidades de otros E.E.M.M. de la U.E. constituidas para la protección de los intereses colectivos o difusos de los consumidores que estén habilitadas ante la Comisión Europea mediante su inclusión en la lista publicada a tal fin en el DOCE.
   Los jueces y tribunales aceptarán dicha lista como prueba de la capacidad de la entidad habilitada para ser parte, sin perjuicio de examinar si la finalidad de la misma y los intereses afectados legitiman el ejercicio de la acción.

En lo referente a la solución extrajudicial de litigios[228], se permite que el prestador y el destinatario del servicio puedan someterse a los arbitrajes previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación. En estos últimos, el uso de medios electrónicos deberá someterse a lo que prescriba su normativa específica.

Avanzando en la explicación nos referiremos a los mecanismos de información de los que disponen los prestadores y destinatarios de servicios. Estos podrán dirigirse, incluso por medios electrónicos, a los Ministerios de Ciencia y Tecnología, Justicia, Economía y Sanidad y Consumo, a los órganos que determinen las respectiva Comunidades Autónomas y Entidades Locales, con el propósito de:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica.
b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos.
c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia técnica.

[228] Existen gran cantidad de sistemas de Arbitraje. No obstante en España el más habitual es el Arbitraje, regulado en la Ley 36/1988 de 5 de diciembre de Arbitraje y El Arbitraje de Consumo, regulado en el Real Decreto 636/1993 de 3 de mayo, dictado en desarrollo de la Ley 26/1984 de 19 de julio, General para la Defensa de los Consumidores y Usuarios. Puede obtenerse más información sobre este sistema en la dirección siguiente: www.consumo-inc.es/arbitraje/arbitraje.htm . Recuérdese otros sistemas a nivel internacional como el de la Red extrajudicial europea: http://www.eejnet.org/ y el Centro de Arbitraje y medicación de la OMPI: www.wipo.int .

Para facilitar el cumplimiento de lo arriba indicado y siempre guardando las debidas cautelas para salvaguardar el derecho a la intimidad de la persona y la protección de los datos personales de las personas en ellos indicados, el CGPJ remitirá al Ministerio de Justicia, en la forma y periodicidad que fijará un Convenio que se elaborará entre ambos, todas las resoluciones judiciales que contengan pronunciamientos relevantes sobre la validez y eficacia de los contratos celebrados por vía electrónica, sobre su utilización como prueba en juicio, o sobre los derechos, obligaciones y régimen de responsabilidad de los prestadores y destinatarios de servicios.

De igual manera los órganos arbitrales y los responsables de los demás procedimientos de resolución extrajudicial de conflictos, comunicarán los laudos o decisiones que revistan importancia para la prestación de servicios de la S.I. y del C.E., en los mismos términos fijados en el supuesto anterior.

Por su parte, el Ministerio de Justicia enviará a la Comisión Europea la información remitida, y deberá facilitar el acceso a ésta, a cualquier interesado que la solicite.

Pasando a la actividad de supervisión y control, corresponde al Ministerio de Ciencia y Tecnología controlar el cumplimiento de las disposiciones de la LSSI, por parte de los prestadores de servicios. Para llevar a cabo dicho control, se habilita a este órgano expresamente a que lleve a cabo todas las labores inspectoras que considere oportunas. No obstante para algunas materias reguladas (las contenidas en los artículos 8, 10, 11, 15, 16, 17 y 18), la referencia que contienen al órgano competente, se entenderá para los órganos jurisdiccionales o administrativos competentes en función de la materia que se trate.

De igual forma, los funcionarios del Ministerio de Ciencia y Tecnología que desarrollen dicha actividad inspectora tendrán la consideración de autoridad pública en el desempeño de sus cometidos. No obstante, si las conductas del prestador estuvieran sujetas al control de otros órganos por razón de la materia o de la entidad de que se trate y con independencia de que se realicen por técnicas o medios electrónicos o telemáticos, los órganos que por la legislación sectorial tengan atribuidas las funciones de control, supervisión, inspección o tutela, ejercerán las funciones que les corresponden.

En cumplimiento de lo establecido en los supuestos anteriores, se establece un deber de colaboración de los prestadores de servicios hacia los funcionarios en el ejercicio de funciones inspectoras, debiendo facilitar toda la información y colaboración precisas, permitiendo incluso el acceso a sus instalaciones y a la consulta de cualquier documentación relevante para la actividad de control de que se trate, siendo de aplicación en su caso el artículo 8.5 de la ley 29/1998 de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

Si como consecuencia de la actividad inspectora, se tiene conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, ya sean estatales o autonómicas, se dará cuenta de los mismos (como no podía ser de otra manera) a los órganos u organismos competentes para su supervisión y control.

Finalizaremos este epígrafe refiriéndonos al régimen sancionador establecido para las conductas que contravengan las disposiciones establecidas en la LSSI. Para ello, se establece que los prestadores de servicios están sujetos al régimen sancionador, que se explicará a continuación, cuando la LSSI les sea de aplicación.

Para empezar la explicación de este régimen, señalaremos que las infracciones se catalogan en muy graves, graves y leves.

Tienen consideración de muy graves las siguientes:

a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 (restricciones a la prestación de servicios) en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.
b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio de intermediación, cuando un órgano administrativo lo ordene, en virtud de lo dispuesto en el artículo 11.
c) El incumplimiento de la obligación de retener los datos del tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la S.I., previsto en el artículo 12.
d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

Se considerarán infracciones graves a las siguientes:

a) El incumplimiento de lo establecido en los párrafos a) y f) del artículo 10.1, (suministro de la dirección del prestador y sobre el precio, según los términos que se establecieron en su momento, respectivamente).
b) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a destinatarios que no hayan autorizado su remisión, o se hayan opuesto a ella o el envío, en el plazo de un año, de mas de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando éste no hubiera autorizado o solicitado su remisión, o se hubiera opuesto a ella.
c) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato en la forma prevista por el artículo 27.
d) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo, con arreglo a la ley.

Por último se consideran infracciones leves:

a) La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la S.I.
b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo.
c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.
d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan autorizado su remisión, o se hayan opuesto e ella, cuando no constituya infracción grave.
e) No facilitar la información a la que se refiere el artículo 27.1 (obligaciones previas a la contratación), cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.
f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos por el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

Lógicamente, la LSSI impone una cuantía sancionadora, para dar carácter coercitivo a la imposición de sanciones. Ésta, está graduada de la siguiente manera:

- Por la comisión de infracciones muy graves se impondrá una multa de entre 150.001 y 600.000 euros. En caso de reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante el plazo máximo de dos años.
- Por la comisión de infracciones graves la multa oscilará entre los 30.001 y 150.000 euros.
- Para las infracciones leves la multa se pondrá hasta 30.000 euros[229].

Además, la comisión de infracciones muy graves y graves podrá llevar aparejada la publicación de la resolución sancionadora, a cargo del prestador del servicio, en el BOE o Diario Oficial de la Administración Pública que, en su caso, hubiera impuesto la sanción, en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la Administración sancionadora o en la página de inicio del sitio de Internet del prestador del servicio, una vez que la resolución sea firme, siendo

[229] En el Anteproyecto la horquilla iba de los 3.000 a los 30.000 euros, pero durante la tramitación parlamentaria se suprimió el límite inferior para flexibilizar el régimen sancionador.

necesario para la imposición de esta sanción, considerar previamente la repercusión social de la infracción cometida, el número de usuarios o de contratos afectados y la gravedad del ilícito.

Cuando se interponga una sanción a un prestador de servicios establecido en un Estado que no sea miembro ni de la U.E. ni del EEE, el órgano que dicta la sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a estos servicios, por un periodo máximo de dos años, un año y seis meses para infracciones muy graves, graves y leves respectivamente.

Para la graduación de las cuantías, la LSSI establece que se atenderá a los criterios siguientes:

a) La existencia de intencionalidad.
b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.
c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.
d) La naturaleza y cuantía de los perjuicios causados.
e) Los beneficios obtenidos por la infracción.
f) Volumen de facturación a que afecte la infracción cometida.

Es más, en los procedimientos sancionadores por infracciones muy graves o graves, se podrán adoptar las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales. Eso sí, estas medidas deberán ser las previstas por la Ley 30/1992 de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en su legislación de desarrollo, pudiendo en particular adoptarse alguna de las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.
b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.
c) Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

Para la adopción y cumplimiento de estas medidas, se deberá estar a lo dispuesto en el ordenamiento jurídico para asegurar la protección de los derechos a la intimidad familiar y personal, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran estar afectados.

De igual forma, cuando la Constitución o demás normas reguladoras de derechos y libertades, confieran la competencia a órganos jurisdiccionales, estos serán los únicos competentes para establecer dichas medidas.

Se impone igualmente en lo referente a la aplicación de medidas provisionales, que se utilice el Principio de Proporcionalidad para tomar la decisión.

En los casos de urgencia, la medida podrá imponerse antes de la apertura del proceso sancionador con la condición de que sean confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento que deberá iniciarse antes del decimoquinto día siguiente a la aprobación de estas medidas, acuerdo que podrá ser objeto del recurso que proceda. El incumplimiento del plazo o de la obligación de pronunciamiento sobre las medidas conllevará que éstas queden sin efecto.

En caso de incumplimiento de estas medidas, el órgano competente para resolver el procedimiento sancionador podrá imponer una multa coercitiva de hasta 6.000 euros por cada día de incumplimiento.

Volviendo a las sanciones por infracción de lo previsto en la LSSI, corresponde su imposición en el caso de las muy graves al Ministro de Ciencia y Tecnología y al Secretario de Estado de Telecomunicaciones y para la S.I. las graves y leves. No obstante, si la imposición de ésta es por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate, a los que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley, corresponderá su interposición al órgano que la dicte. Igualmente corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3.b) y 38.4.d).

Como es obvio, y en consonancia con la mayor parte de las cautelas mencionadas a lo largo de la LSSI, que podrían haberse omitido por ser obvias, no podrá interponerse una sanción si hubiera sido impuesta una sanción penal, en los casos en los que se aprecie identidad de sujeto, hecho y fundamento (o sea el Principio *non bis in ídem*). Si aún no hubiera sanción penal, se deberá suspender el proceso hasta que exista resolución penal firme impuesta por la autoridad judicial. Reanudado éste, deberá respetar la resolución que se dicte y, en su caso, los hechos probados en la resolución judicial.

La imposición de una sanción prevista en la LSSI, por el contrario, no es incompatible con otro proceso sancionador cuando la conducta infractora se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no exista identidad del bien jurídico protegido.

Para finalizar este epígrafe, nos referiremos a la prescripción de las infracciones y sanciones. La LSSI establece que será de tres años para las muy graves, dos años para las graves y seis meses para las leves.

D) Otras Disposiciones.

Finalmente, la LSSI contiene una serie de disposiciones adicionales, transitorias o finales que, a modo de cajón de sastre, o bien modifican disposiciones normativas de otras leyes o reglamentos, o bien completan las disposiciones que se encuentran en el articulado de la LSSI.

De esta manera, la primera disposición que nos encontramos es la disposición adicional primera, según la cual, las definiciones que se encuentran recogidas en el Anexo tendrán el significado que allí se les asigna.

La disposición adicional segunda se refiere al ámbito de aplicación de la LSSI, al imponer que la prestación de servicios de la S.I. relacionados con medicamentos o productos sanitarios, se regirá por su normativa especifica.

Relativa al sistema extrajudicial de conflictos, la disposición adicional tercera, permite que el prestador y el destinatario de servicios puedan someterse al Sistema Arbitral de Consumo para la resolución de sus litigios. La Junta Arbitral Nacional de Consumo y aquellas otras de ámbito territorial inferior, autorizadas para ello por el Instituto Nacional de Consumo, podrán dirimir los conflictos planteados por los consumidores de acuerdo con lo dispuesto en el Real Decreto 636/1993 de 3 de mayo, que regula el Sistema Arbitral de Consumo a través de medios telemáticos.

Por su parte, la disposición adicional cuarta reforma el Código Civil y el Código de Comercio, en lo que respecta a la regulación de estos referente a la prestación del consentimiento. De esta manera, el artículo 1262 del Código Civil queda redactado de la siguiente manera:

“El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y las causas 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 en el lugar en que se hizo la oferta.
En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación”.

Y el artículo 54 del Código de Comercio queda redactado de la manera siguiente:

“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 realizado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación".

Por su parte, la disposición adicional quinta impone a las Administraciones Públicas a que adopten las medidas oportunas antes de 31 de diciembre de 2005, para que los contenidos de sus páginas de Internet sean accesibles a personas discapacitadas o de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido, generalmente reconocidos. El mismo criterio podrá extenderse a las páginas de Internet cuyo diseño o mantenimiento financien. Finalmente, se promoverá la adopción de normas de accesibilidad por los prestadores de servicios y los fabricantes de equipos y software para facilitar el acceso de estas personas a los contenidos digitales.

Especial importancia tiene la disposición adicional sexta que regula el Sistema de asignación de nombres de dominio bajo el "es", código correspondiente a España. Esta disposición regula los principios inspiradores de este sistema, en cumplimiento de lo dispuesto en la disposición adicional decimosexta de la Ley 17/2001 de 7 de diciembre, de Marcas[230]. La asignación de los nombres de dominio será realizada por la entidad pública empresarial Red.es, según se recoge en la disposición adicional sexta de la Ley 11/1998 de 24 de abril, General de Telecomunicaciones. Se realizará de conformidad con los criterios que se establecen en esta disposición, en el Plan Nacional de Nombres de Dominio de Internet[231], en las demás normas específicas de desarrollo que se dicten por la autoridad de asignación y en la medida en que sean compatibles con ellos, las prácticas generalmente aplicadas y las recomendaciones emanadas de las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión de nombres de dominio de Internet, que será analizado en el siguiente epígrafe.

La disposición adicional séptima, dispone que el Ministerio de Ciencia y Tecnología deberá elaborar un Plan Cuatrienal para el desarrollo de la SI y la convergencia con Europa. Igualmente regula los principios, objetivos y áreas del Plan.

Tampoco entraremos en la disposición final segunda, que crea una tasa, a satisfacer a la entidad pública empresarial Red.es, por las gestiones realizadas para la asignación o renovación de un nombre de dominio. Para conseguir dicho fin se reforma la ya citada ley 11/1998 y recientemente se ha dictado la Orden PRE/2440/2003 de 29 de agosto, por el que se desarrolla la regulación de la tasa por asignación del recurso limitado de nombres de dominio bajo el código de país correspondiente a España (es). (BOE de 9.9.2003).

[230] BOE de 8 de diciembre de 2001.

[231] En virtud de esta disposición, el Ministerio de Ciencia y Tecnología, ha publicado la Orden CTE/662/2003 de 18 de marzo, por la que se aprueba el Plan Nacional de nombre de Dominio de Internet bajo el Código correspondiente a España ("es"). BOE de 26-03-2003.

Por su parte la disposición transitoria única, impone que los prestadores de servicios que anteriormente a la entrada en vigor de la LSSI, ya vinieran usando uno o más nombres de dominio o direcciones de Internet, soliciten al menos la anotación de uno de ellos en el registro donde se encuentren inscritos a efectos de publicidad o constitutivos, en el plazo de un año desde la referida entrada en vigor.

Otra de las aportaciones a destacar, es la regulada en las disposiciones final primera y tercera, que tienen su origen en una enmienda aprobada por el Senado, por las cuales se operan las reformas necesarias en la ya mencionada Ley 11/1998, con el objeto de declarar Internet servicio universal (de acuerdo con el artículo 2 de la Directiva 2002/22/CE[232], entendemos por servicio universal que el servicio debe llegar a todos los usuarios finales con igual calidad y precio, con independencia de la localización geográfica del usuario) tomando las medidas que se consideran oportunas para ello y fijando un calendario de obligado cumplimiento, que finaliza el 31 de diciembre de 2004, con la llegada de Internet al 100% de los usuarios.

Para finalizar el estudio de la LSSI, concluiremos con lo dispuesto en la disposición final octava, que otorga al Gobierno el plazo de un año, para que apruebe un distintivo que permita identificar a los prestadores de servicios que respeten los códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios y que incluyan, entre otros contenidos, la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respeten los principios establecidos por la legislación comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores[233], en los términos que reglamentariamente se establezcan.

Concluido el estudio de la LSSI, en lo que respecta a la regulación jurídica de las materias tratadas, sólo nos queda esperar que el Gobierno utilice la habilitación que le otorga la disposición final séptima, para desarrollar mediante Reglamento esta Ley.

E) Nombres de Dominio.

Comenzaremos intentando delimitar que debe entenderse por Dominio. Por Dominio podemos entender el nombre o conjunto de caracteres separados por puntos, que identifican a una empresa, organismo, institución etc. en Internet a través de un procedimiento sencillo, por el cual se puede comunicar con un ordenador a través de su localizador asignado (cada ordenador tiene un número propio y exclusivo que se denomina *Internet Protocol* o IP). Cada IP está formada por 4 números separados por puntos, cada uno de los cuales puede tomar valores

[232] Para su correcta citación, véase nota 54.
[233] Recuérdese lo que se indicó en esta materia en el epígrafe sobre protección de los consumidores del capítulo primero.

entre 0 y 225. Esta dirección es, por tanto, difícil de recordar por lo que esos números se traducen en el sistema de nombres de dominio.

Como ya hemos puesto de relieve[234], el organismo Internacional que establece la normativa internacional de asignación de Nombres de dominio, es el ICANN. El ICANN fue creado en 1998 por la OMPI, para que elaborara y diera forma a las distintas cuestiones que pudieran plantearse con los nombres de dominio, como veremos a continuación. La base de datos de dominios como com., org., y net la gestiona la empresa norteamericana *Network Solutions INC.* Por su parte existen una serie de empresas que por delegación del ICANN gestionan dominios bajo el com., org. y net., tales como: *123HostingIdeal.com, Acens, ActiveISP, Arsys, Interdomain, Internet Names Worlwide, Nominalia, Ubilibet, Dinahosting, Global Name,* etc[235].

El principio a aplicar a los nombres de dominio en cuanto a su asignación es el de la antigüedad (*first come, first served*), lo que puede dar lugar a disputas en caso de que piratas informáticos registren dominios que se correspondan con conocidas marcas, para posteriormente venderlos a entidades, es por ello que los nombres de dominio están íntimamente ligados al derecho de marcas y no al de propiedad intelectual, salvo en el caso de que el dominio fuera tan original que recibiera protección por la PI (aunque es raro este supuesto ya que por razones de Política Empresarial, se intenta que los dominios coincidan o bien con la marca, o bien con el nombre comercial, para facilitar su reconocimiento y conexión con la empresa, por parte de los usuarios y clientes). Por ello se ha dotado el ICANN de una normativa de resolución de conflictos que se traduce en la Política Uniforme de Solución de Controversias en materia de nombres de dominio, de 26 de agosto de 1999, y el Reglamento de Política Uniforme de solución de controversias en materia de nombres de dominio, aprobado el 24 de octubre de 1999[236]. Para poder solventar un litigio por este sistema, es necesario acudir a uno de los proveedores de servicios de resolución de controversias administrativas acreditados en el ICANN[237]

Por su parte la OMPI, como proveedor de servicios acreditado, ha elaborado un Reglamento Adicional del Centro de Arbitraje y Mediación de la OMPI, relativo a la Política Uniforme de solución de controversias en materia de nombres de dominio de 1 de diciembre de 1999 y ha constituido un centro de Arbitraje y Mediación[238]. Las decisiones tomadas por los Órganos de Arbitraje y Mediación del la OMPI son vinculantes, en tanto que las autoridades acreditadas de registro que acceden a este sistema están obligadas a dar cumplimiento a la Resolución.

---

[234] Véase nota 4.
[235] La lista completa de empresas registradoras se encuentra en la Web del ICANN: www.icann.org .
[236] Ambos pueden ser consultados en la dirección: http://www.icann.org/udrp/udrp.htm.
[237] La Lista de proveedores acreditados puede consultarse en www.icann.org/udrp/approved-providers.htm.
[238] Puede ser consultado en la siguiente dirección: http://arbiter.wipo.int/center/index-es.html

Pero no olvidemos que en virtud de la Política Uniforme, cabe la posibilidad de acudir a la jurisdicción competente antes del proceso, o finalizado éste. En ese supuesto la decisión tomada por el proveedor de servicios de resolución de controversias, quedará en suspenso, en tanto no haya resolución judicial firme que confirme la primera decisión[239].

Para la OMPI existen tres supuestos de registro abusivo de nombres de dominio, a saber, aquel que da lugar a confusión al ser idéntico al de una marca similar, aquel registro en el que el propietario no posee derechos o intereses legítimos sobre ese dominio, o que el dominio esté siendo utilizado de mala fe.

Existen diversos tipos de dominio, de primer, segundo y tercer nivel. Dentro de los dominios de primer nivel podemos encontrar dos clasificaciones, los dominios genéricos y los de código país. Los dominios genéricos están recogidos bajo el com. (reservado en principio a empresas comerciales), org. (reservado en un principio a organizaciones), net. (reservado a empresas relacionadas con Internet), edu., gov., mil., (reservados exclusivamente a empresas de los Estados Unidos), int., (reservado a Organizaciones Internacionales constituidas a raíz de un Tratado Internacional) etc. En cuanto a los dominios de código país son: es, uk, ad, it, etc., aunque también pueden encontrase un supuesto especial, el del dominio eu., creado por la Unión Europea, para todas las empresas y particulares de los países Miembros que lo deseen[240], aunque mostramos dudas sobre su éxito y utilidad, ya que entendemos que a nivel empresarial actualmente es mejor identificarse o bien con un genérico, o bien con el de un país. El registro de los dominios de primer nivel –eu-, será llevado a cabo por el Consorcio *European Registry for Internet Domains* (EURID)[241]Para este último tipo de dominios, cada país dispone de sus propias reglas, por lo que sólo atenderemos a la normativa española.

Mayor problema plantean a efectos de marcas, como mencionábamos anteriormente, los dominios denominados de segundo nivel o dominios recuperados. Por poner un ejemplo, podemos encontrarnos un dominio bajo "Microsoft.com, telefónica.com, repsol.com". Como el lector podrá imaginarse, pueden generarse problemas si alguien bajo el principio aludido anteriormente de "*first come, first served*" registra un dominio de una marca conocida. Si el dominio finaliza en com.,org, net, biz, info, o name, la controversia deberá ser resuelta partiendo de la normativa del ICANN, ante un organismo de resolución acreditado, como el Centro de Arbitraje y Mediación de la OMPI.

[239] Aunque a la vista de la multitud de reclamaciones presentadas ante la OMPI, este sistema se presenta como el preferido por la sociedad civil. Nosotros optamos por este procedimiento ya que el litigio se solventa en un Órgano y trámite único, lo que puede no ser así en el caso de optar por la vía jurisdiccional, que puede acarrear más de un procedimiento antes diferentes jurisdicciones.

[240] Véase nota 4.

[241] De acuerdo con la Decisión de la Comisión 2003/375/CE, de 21 de mayo de 2003, relativa a la designación del Registro del Dominio de primer nivel .eu. DOUE serie L 128 de 24.5.2003.

Pasando a continuación a las peculiaridades de los nombres de dominio bajo el "es", atendiendo a la normativa española ya mencionada[242], nos encontramos con un Plan Nacional de Nombres de Dominio, aprobado por la Orden CTE/662/2003. Esta Orden sustituye a la Orden de 21 de marzo de 2000 que fue a su vez sustituida por la Orden de 12 de julio de 2001.

Como ya se ha comentado anteriormente, el organismo competente para la asignación de estos nombres es la entidad pública empresarial Red.es. Esta labor conlleva la de gestionar el Registro de Dominios y la de tomar decisiones para la buena gestión del sistema, incluyendo la aceptación o denegación motivada de las peticiones de asignación de nombres de dominio, según se desprende del artículo segundo de la mencionada Orden.

Bajo el "es" se pueden registrar nombres de dominio de primer, segundo y tercer nivel, siendo clasificados a su vez en dos grupos:

- nombres de dominio regulares: son todos los nombres de dominio que se asignan conforme a las reglas establecidas en este Plan.
- Nombres de dominio especiales: son aquellos nombres de dominio de segundo nivel, que la entidad pública empresarial Red.es puede asignar sin sujeción a las reglas establecidas en el Plan (con excepción de las recogidas en el capítulo IV), cuando concurra un notable interés público. En estos supuestos la entidad Red.es podrá establecer las condiciones que estime oportunas, en lo que respecta a la utilización del nombre de dominio (art. 4 b.).

El criterio general de asignación de los nombres de dominio es el de la antigüedad. Si nos encontramos ante un dominio de segundo nivel, este criterio se combinará con el de tener derecho a este dominio y que se reúnan los requisitos recogidos en el Plan. Con ello se pretende evitar el supuesto aludido de ocupación de dominio de segundo nivel, ya que para asignarlo se estará al nombre tal cual aparece en la escritura de constitución y/o modificación, o a un nombre abreviado o marca o nombre comercial de la organización que lo identifique de manera inequívoca. Para ello se coordinará la entidad Red.es, con el Registro Mercantil. Con la Oficina Española de Patentes y Marcas, los demás Registros Públicos nacionales y la Oficina de Armonización del Mercado Interior (OAMI), que es una Agencia Comunitaria con sede en Alicante. Otro supuesto de apoyo a la ocupación de dominios se encuentra recogido en el artículo 17.2, en virtud del cual se podrá denegar la asignación de un nombre de dominio cuando este pueda generar un riesgo evidente de confusión entre los usuarios.

Para la asignación de dominios de tercer nivel, se estará al mismo criterio de la antigüedad. Los dominios de tercer nivel que pueden asignarse bajo el "es" son los siguientes:

[242] Véase páginas 94 y 95.

- com.es, para personas físicas o jurídicas y entidades sin personalidad que tengan intereses o mantengan vínculos con España.
- Nom.es, para las personas físicas que tengan intereses o mantengan vínculos con España.
- Org.es, las entidades, instituciones o colectivos con o sin personalidad jurídica y sin ánimo de lucro que tengan intereses o mantengan vínculos con España.
- Gob.es, las Administraciones Públicas españolas y las Entidades de Derecho Público de ella dependientes, así como cualquiera de sus dependencias, órganos y unidades.
- Edu.es, para las entidades, Instituciones o colectivos con o sin personalidad jurídica, que gocen de reconocimiento oficial y realicen funciones o actividades relacionadas con la enseñanza o la investigación en España.

Para finalizar el apartado, mencionaremos algunas disposiciones del Plan que por su interés, merecen al menos una breve reseña.

En primer lugar, atendiendo al artículo 18, podemos afirmar que los derechos de utilización del nombre de dominio no son transmisibles. No obstante, en los casos de sucesión universal ya sea “inter vivos” o “mortis causa”, y en los de cesión de la marca o el nombre comercial al que estuviera asociado el nombre de dominio, el sucesor o cesionario puede continuar con su derecho de utilización, siempre y cuando comunique a la entidad Red.es la modificación de los datos en el Registro de Nombres de Dominio.

En consonancia con la exención de responsabilidad analizada para los prestadores e intermediarios de servicios S.I., se establece la misma regla para todos aquellos que actúen como agentes registradores de dominio (esta figura de intermediación entre Red.es y los solicitantes es válida, aunque exige al agente acreditarse previamente ante la entidad Red.es, sobre todo en lo que respecta al acceso a las bases de datos del Registro de Nombres de Dominio), no respondiendo por el uso que el titular haga de él.

Finalmente, mencionaremos la habilitación a Red.es, para establecer un procedimiento de Resolución Extrajudicial de controversias originadas por la asignación de nombres de dominio, sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar.

F) Fiscalidad.

Como hemos tenido ya ocasión de comprobar, la fiscalidad del comercio electrónico tiene una regulación propia, debido a la preocupación de los Estados, por la considerable disminución de la recaudación impositiva, como consecuencia de la aparición de las TIC.

Al igual que ocurrió en el supuesto de la legislación comunitaria, nos vamos a referir sólo a las especialidades de la prestación de bienes y servicios por vía electrónica, en lo que atañe al IVA y a la regulación de la factura electrónica.

1º Impuesto sobre el valor añadido (IVA).

El régimen jurídico aplicable al IVA, como no podía ser de otra manera, es la Ley 37/1992 de 28 de diciembre del Impuesto sobre el Valor Añadido[243], cuyo artículo 70 ha sido modificado por la ley 53/2002 de 30 de diciembre, de medidas fiscales, administrativas y del orden social[244]. Como ya vimos en su momento, se trata de regular un régimen especial al que podrán acogerse todos los empresarios o profesionales no establecidos en la Comunidad[245], que presten servicios electrónicos[246] a personas que no tengan la condición de empresario o profesional y que estén establecidas en la Comunidad o que tengan en ella su domicilio o residencia habitual. Para posibilitar esta opción, se regula detalladamente las obligaciones formales del empresario o profesional que elija a España como Estado de identificación del impuesto[247], el derecho a la deducción de las cuotas soportadas, las obligaciones de los sujetos pasivos y se introducen reglas especiales de facturación. Para ello la reforma de la ley 53/2002 introduce nuevas redacciones en los artículos 163 bis, 163 ter, 163 quáter, 164 y 165

En virtud del artículo 70, que regula la prestación de servicios sometidas al territorio de aplicación del impuesto, es decir cuando se entiende que la prestación de un servicio se entiende sujeta al IVA en España, se plantea una especialidad para los servicios prestados por vía electrónica, según el cual, se establecen los siguientes supuestos:

- Si el destinatario del servicio es un empresario o profesional que actúa como tal, y radica en España la sede de su actividad económica, o tiene un establecimiento permanente o, en su defecto, el lugar de su domicilio, siempre que se trate de servicios que tengan por destino dicha sede, establecimiento permanente o domicilio, con independencia de donde se encuentre establecido el prestador de los servicios y el lugar desde el que los preste.

[243] BOE de 29.12.1992
[244] BOE 313 de 31.12.2002.
[245] Se entiende por empresario o profesional no establecido en la Comunidad, según el nuevo artículo 163 bis dos A) todo empresario o profesional que no tenga la sede de su actividad económica en la Comunidad ni posea un establecimiento permanente en el territorio de la Comunidad, ni tampoco tenga la obligación, por otro motivo, de estar identificado en la Comunidad, conforme al número 2º del apartado uno del artículo 164 de esta Ley o sus equivalentes en las legislaciones de otros E.E.M.M.
[246] Se entiende por servicios electrónicos o servicios prestados por vía electrónica los servicios definidos en la letra B) del número 4º del apartado uno del artículo 70 de esta Ley, y que mencionaremos más adelante.
[247] Según el artículo 163 bis dos C), el Estado Miembro por el que haya optado el empresario o profesional no establecido para declarar el inicio de su actividad como tal empresario o profesional, en el territorio de la Comunidad, de conformidad con lo dispuesto en el presente artículo.

- Si los servicios se prestan por un empresario o profesional y la sede de su actividad económica o establecimiento permanente desde el que se prestan los servicios se encuentran en territorio de aplicación del impuesto, siempre que el destinatario del mismo no tenga la condición de empresario o profesional actuando como tal y se encuentre establecido o tenga su residencia o domicilio habitual en la Comunidad Europea[248], así como cuando no resulte posible determinar su domicilio.
- Cuando los servicios son prestados desde la sede de la actividad, o establecimiento permanente de un empresario o profesional que se encuentra fuera de la Comunidad, y el destinatario no tenga la condición de empresario o profesional actuando como tal, siempre que este último se encuentre establecido o tenga su residencia o domicilio habitual en el territorio de aplicación del impuesto[249].

Por servicios prestados por vía electrónica, se entiende aquellos que consisten en la transmisión enviada inicialmente y recibida en destino por medio de equipos de procesamiento, incluida la comprensión numérica y el almacenamiento de datos, y enteramente transmitida, transportada y recibida por cable, radio sistema óptico u otros medios electrónicos[250] y, entre otros, los siguientes:

- El suministro y alojamiento de sitios informáticos.
- El mantenimiento a distancia de programas y equipos.
- El suministro de programas y su actualización.
- El suministro de imágenes, texto, información y la puesta a disposición de bases de datos.
- El suministro de música, películas, juegos, incluidos los de azar o de dinero, y de emisiones y manifestaciones políticas, culturales, artísticas, deportivas, científicas o de ocio.
- El suministro de enseñanza a distancia.

Para otro tipo de servicios, que pasaremos a analizar a continuación, puesto que estas actividades están muy introducidas en Internet, se encontrarán sometidos al impuesto si se dan los siguientes requisitos:

- Si el destinatario es un empresario o profesional que actúa como tal, y radica en el territorio de aplicación del impuesto la sede de su actividad económica, o tenga en el mismo un establecimiento permanente o, en su defecto, el lugar del domicilio, siempre que se trate de servicios que tengan por destinatarios a dicha

[248] Se entiende que el destinatario del servicio es residente en la Comunidad, cuando se efectúe el pago de la contraprestación del servicio con cargo a cuentas abiertas en establecimientos de entidades de crédito ubicadas en dicho territorio.

[249] Se presume que el destinatario del servicio se encuentra establecido o es residente en el territorio de aplicación del impuesto, cuando se efectúe el pago de la contraprestación del servicio con cargo a cuentas abiertas en establecimientos de entidades de crédito ubicadas en dicho territorio.

[250] A estos efectos, el hecho de que el prestador del servicio y su destinatario se comuniquen por correo electrónico, no implica por sí mismo que el servicio sea prestado por vía electrónica.

sede, establecimiento permanente o domicilio. Lo dispuesto en este párrafo se aplicará con independencia de dónde se encuentre establecido el prestador de los servicios y el lugar desde el que los preste

- Cuando los servicios se presten por un empresario o profesional y la sede de su actividad económica o establecimiento permanente desde el que se presten los servicios se encuentra en el territorio de aplicación del impuesto, siempre que el destinatario del mismo no tenga la condición de empresario o profesional actuando como tal, y se encuentre establecido o tenga residencia habitual o domicilio en la Comunidad, Canarias, Ceuta o Melilla, así como cuando no resulte posible determinar su domicilio.

Estos servicios, teniendo en cuenta que sólo mencionaremos aquellos que por sus características se adaptan mejor a Internet, son los siguientes:

- Las cesiones y concesiones de derechos de autor, patentes, licencias, marcas de fabrica o comerciales y los demás derechos de propiedad intelectual, industrial, así como cualesquiera otros derechos similares.
- La cesión o concesión de fondos de comercio, de exclusivas de compra o venta o del derecho a ejercer una actividad profesional.
- Los de publicidad.
- Los de asesoramiento, auditoria, ingeniería, gabinete de estudios, abogacía, consultores, expertos contables o fiscales y otros análogos, con excepción de los comprendidos en el número 1º de este apartado uno.
- Los de tratamiento de datos y el suministro de informaciones, incluidos los procedimientos y experiencias de carácter comercial.
- Los de traducción, corrección o composición de textos, así como los prestados por intérpretes.
- Los de seguro, reaseguro y capitalización, así como los servicios financieros, citados respectivamente por el artículo 20 apartado uno, números 16º y 18º, de esta ley, incluidos los que no estén exentos, con excepción del alquiler de cajas de seguridad.

2º Facturación Electrónica.

Como ya vimos en su momento, la Legislación Comunitaria da validez a las facturas electrónicas. En lo que se refiere a la legislación española, nos centraremos en la Orden HAC/3134/2002, de 5 de diciembre, sobre un nuevo desarrollo del régimen de facturación telemática previsto en el artículo 88 de la Ley 37/1992 de 28 de diciembre, del impuesto sobre el valor añadido, y en el artículo 9 bis del Real Decreto 2402/1985, de 18 de diciembre[251] y en la Resolución 2/2003 de 14 de febrero, de la Dirección General de la Agencia Estatal de la Administración

[251] BOE 298 de 13.12.2002.

Tributaria sobre determinados aspectos relacionados con la facturación telemática[252].

Comenzando por la primera, y en consonancia con la legislación comunitaria, la facturación electrónica[253] para que sea válida, ha de estar basada en sistemas de F.E. avanzada, o de cualquier otro sistema de intercambio electrónico de datos que permita garantizar la autenticidad del origen de las facturas expedidas por medios electrónicos y la integridad de su contenido. Cumpliendo estos requisitos, serán válidas a efectos fiscales, para acreditar la repercusión y deducción de las cotizaciones del IVA y de la justificación de los gastos necesarios para la obtención de ingresos o de las deducciones practicadas para la determinación de las bases o las cuotas tributarias.

Para que la factura surta plenos efectos legales, los profesionales y empresarios que deseen emitir o recibir facturas electrónicas, deberán acogerse previamente a este sistema. Se les plantea dos posibilidades:

- Pedir la autorización previa a la Agencia Estatal de la Administración Tributaria (AEAT), de un sistema de firma electrónica avanzada, basada en un certificado electrónico y generada por un dispositivo de producción de firma de entre los admitidos y publicados por la AEAT, que serán automáticamente concedidos. Eso sí, el contribuyente deberá ser el titular del certificado electrónico de identificación y éste debe estar en vigor, así como disponer de los mecanismos de producción y verificación de la firma, conforme a los admitidos por la AEAT.
- Otros mecanismos de intercambio electrónico de datos. Para poder utilizar otros mecanismos, la AEAT deberá autorizarlos previamente, a raíz de la petición previa del contribuyente y la entrega de los elementos propuestos por el contribuyente.

Finalmente indicaremos que la Orden, establece que han de cumplirse ciertas normas, en lo que se refiere a la conservación de las facturas electrónicas durante el periodo de prescripción del impuesto. No vamos a entrar a detallarlas, pero queremos dejar constancia de las mismas.

Por su parte la Resolución 2/2003 establece una serie de normas de carácter técnico, para la validez de las facturas electrónicas, sus dispositivos de generación y conservación, que desarrollan las disposiciones normativas reguladas en la Orden 3134/2002. Todas aquellas firmas electrónicas avanzadas que cumplan estos requisitos, se entenderán en el sistema de dispositivos de facturación electrónica, admitidos por la AEAT, que vimos anteriormente.

[252] BOE 51 de 28.2.2003

[253] Se considera factura electrónica, cualquier documento electrónico que cumpla las condiciones de emisión y de contenidos exigidos en el Real Decreto 2402/1985.

Para finalizar, mencionaremos la Orden ECO/2579/2003 de 15 de septiembre, por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Ministerio de Economía y sus Organismos adscritos (BOE 225 de 19.9.2003). Aunque no regule directamente la factura electrónica, al estar basada ésta como acabamos de ver en sistemas de autenticación entre lo que se encuentra la F.E., deberemos tener en cuenta las disposiciones contenidas en la presente Orden.

G) Dinero Electrónico.

La incorporación al derecho español de las Directivas que tuvimos ocasión de estudiar en el capítulo primero, se produce a través de la Ley 44/2002 de 22 de noviembre, de medidas de reforma del sistema financiero (BOE 281 de 23.11.2002).

Esta ley poco viene a innovar las disposiciones ya estudiadas en cuanto a la materia que nos ocupa, aunque aún con riesgo de ser reiterativos, daremos algunas pinceladas de la normativa que nos ocupa.

En primer lugar, definiremos que se entiende por entidad de dinero electrónico. Atendiendo al artículo 21 son aquellas entidades de crédito distintas de las definidas en el párrafo a), apartado 1 del artículo 1 del Real Decreto Legislativo 1298/1986 de 28 de junio, cuya actividad principal consista en la emisión de medios de pago en forma de dinero electrónico.

Por dinero electrónico se entiende un valor monetario representado en un crédito exigible a su emisor:

- Almacenado en un soporte electrónico.
- Emitido al recibir fondos de un importe cuyo valor no será inferior al monetario exigido.
- Aceptado como medio de pago por empresas distintas del emisor.

Para poder emitir dinero electrónico, se deberá ser una entidad de crédito y hallarse autorizada para ello e inscrita en los oportunos Registros, existiendo la posibilidad de actuar en territorio español si la entidad se encuentra autorizada en otro E.E.M.M., salvo que medie una de las exenciones previstas en el artículo 8 de la Directiva 2000/46/CE.

Para finalizar esta breve exposición indicaremos que, el Titular del dinero electrónico podrá solicitar durante el periodo de validez del mismo, el reembolso de la cantidad en billetes y monedas de banco, o por transferencia a una cuenta, sin otros gastos que los necesarios para realizar la operación.

II) Normativa española sobre Firma Digital.

Entrando en la normativa que transpone la Directiva 1999/93/CE[254], nos encontramos, por un lado con el Real Decreto-Ley 14/1999 de 17 de septiembre, sobre F.E.[255] y, por otro con el Proyecto de Ley de F.E.[256]. Lógicamente nos vamos a centrar en la legislación en vigor y cuando se finalice su estudio, se mencionarán las innovaciones que aporta el borrador, sin perjuicio de que en algún momento durante la explicación del Real Decreto-Ley, consideremos necesario compararlo con el Proyecto de Ley.

No quiero empezar su explicación, sin destacar un hecho que posiblemente, ya haya percibido el lector, y que no es otro que la normativa de transposición de la Directiva, es dos meses anterior a su aprobación, y esto es así, porque el Gobierno tenía prisa por regular la disciplina para garantizar su creación y posterior despegue. Para ello y con el objeto de no vulnerar a la Directiva que estaba por llegar, se redactó conforme a la Posición Común lograda en el Consejo de Telecomunicaciones de la U.E. de 22 de abril de 1999, sobre la propuesta de Directiva en cuestión.

A) El Real Decreto-Ley 14/1999.

Comenzaremos el estudio de la materia, refiriéndonos al ámbito de aplicación de la presente norma. Lo que se pretende regular es el uso de la F.E.[257], el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación[258], así como regular la actividad de los prestadores de servicios de certificación establecidos en España[259].

La aprobación de esta disposición no alterará las disposiciones relativas a la celebración, la formalización, la validez y la eficacia de los contratos y de otros

[254] Para su correcta citación, véase nota 3.
[255] Para su correcta citación, véase nota 7.
[256] Puede ser consultado en la siguiente dirección de la página *Web* del Ministerio de Ciencia y Tecnología: www.mcyt.es/grupos/grupo_setsi.htm.
[257] De acuerdo con el artículo 2-a), ésta es: "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge".
[258] Por prestador de servicios de certificación entenderemos, de acuerdo con el artículo 2-k): "la persona física o jurídica que expide certificados, pudiendo prestar además, otros servicios en relación con la F.E.".
[259] El borrador de Anteproyecto de Ley va mas allá de la presente regulación, al establecer los principios, en base a los cuales, se entenderá que un prestador de servicios de certificación está establecido en España. No vamos a mencionarlos pero si indicaremos que es a imagen y semejanza de lo dispuesto en la LSSI para entender cuando un prestador de servicios de la S.I,. está establecido en España.

actos jurídicos, ni al régimen aplicable a las obligaciones. De igual modo, las disposiciones relativas a la prestación de servicios de certificación de F.E., ni sustituyen ni modifican las que regulan las funciones que corresponden a las personas facultadas para dar fe pública.

Como ya sucediera con la Directiva 1999/93/CE, se apuesta por la tecnología más avanzada y segura, en la actualidad, la F.E.A.[260], siempre que esté basada en un certificado reconocido[261] y que haya sido producida por un dispositivo seguro de creación de firma[262]. Cumpliendo estos requisitos los datos consignados en forma electrónica tendrán el mismo valor jurídico que la firma manuscrita en relación con los datos consignados en papel y será admisible como prueba en juicio. Se presumirá que se cumplen los requisitos anteriores, cuando el prestador de servicios de certificación que emite el certificado esté acreditado[263] y el dispositivo seguro de creación de firma, se encuentre verificado, de acuerdo con lo dispuesto en el artículo 21. El Proyecto de Ley opera una novedad en este supuesto, al declarar la equivalencia con la firma manuscrita de la firma electrónica reconocida, que no es mas que una F.E.A., basada en un certificado reconocido y generada por un dispositivo seguro de creación de firma.

La firma que no reúna los requisitos antes mencionados, no obstante, no podrá ser excluida como prueba en un juicio y tampoco se le podrán negar sus efectos jurídicos por el mero hecho de presentarse en forma electrónica.

La prestación de servicios de certificación se realizará bajo los principios de no autorización previa y libre competencia, sin que puedan establecerse restricciones a los que procedan de algún E.E.M.M. de la U.E.

No obstante, podrán supeditarse por parte de la normativa estatal o autonómica, el uso de la F.E. en el seno de las Administraciones Públicas y sus entes públicos y en las relaciones que cualesquiera de ellos mantengan con particulares, a las

---

[260] Atendiendo al artículo 2-b), ésta es: "la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los qué se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos".

[261] Atendiendo al artículo 2-j) este es: "el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12". Y por certificado, según el mismo artículo, punto i) entendemos: "la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad". Estos datos de verificación son aquellos, tales como, códigos o claves criptográficas públicas que se utilizan para crear la F.E. (punto g). Además, éstos serán verificados por un programa o aparato informático denominado dispositivo de verificación de firma, (punto h). Finalmente, por signatario entendemos: "la persona física que cuenta con un dispositivo de creación de firma y que actúa en su propio nombre o en el de una persona física o jurídica a la que representa", (punto c).

[262] Por éste entenderemos, de acuerdo con el artículo 2-f): "el dispositivo de creación de firma que cumple los requisitos enumerados en el artículo 19" y por dispositivo de creación de firma atendiendo al punto e) entenderemos: "un programa o aparato informático que sirve para aplicar los datos de creación de firma". Éstos últimos son, según el punto d): "los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la F.E.".

[263] Como indica el punto ll) del artículo 2, los prestadores de servicios de certificación podrán acreditarse voluntariamente, para ello deberán obtener una Resolución favorable por parte del organismo público de supervisión, en la que se establezcan sus derechos y obligaciones específicos para la prestación del servicio.

condiciones adicionales que se consideren necesarias para la salvaguarda del procedimiento, como la prestación de un servicio de consignación de fecha y hora[264], respecto de los documentos electrónicos integrados en un expediente administrativo. Estas condiciones deberán respetar el procedimiento y los principios regulados en el artículo 5, en los que no vamos a entrar.

Como se indicó en su momento, los prestadores de servicios de certificación, pueden someterse a un régimen de acreditación voluntaria. Para la creación de este régimen es competente el Gobierno, que podrá crearlo por Real Decreto, debiendo en todo caso crear un régimen que tenga un adecuado nivel de seguridad y sea protector de los derechos de los usuarios. Los órganos competentes serán aquellos a los que se refiere la legislación vigente en la materia, en particular los designados por la Ley 21/1992 de 16 de julio de Industria y a la ya mencionada Ley 11/1998 General de Telecomunicaciones.

Las normas que rijan este sistema, deberán ser objetivas, razonables y no discriminatorias, debiendo otorgar a los prestadores de servicios que se sometan voluntariamente a éste, la correspondiente acreditación de su actividad, o en su caso, la certificación del producto de F.E.[265] que empleen. Para la emisión de la acreditación, los órganos competentes tendrán en cuenta los informes técnicos que emitan las entidades de evaluación[266] sobre los prestadores de servicios que soliciten la acreditación o los productos para los que se pide la certificación. También tomarán en cuenta el cumplimiento de los requisitos que se determinen reglamentariamente para ser acreditado. Sobre el funcionamiento del sistema de acreditación y los datos que se han de consignar en él, debemos indicar que para dar cumplimiento a estas disposiciones se dictó la Orden de 21 de febrero de 2000, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, que ha provocado una situación compleja. En su articulado se recoge la necesidad de que se constituya una entidad de evaluación que reconozca a los prestadores de servicios de certificación, y esta entidad no se ha constituido, por lo que ningún

[264] El Proyecto de Ley recoge la fecha electrónica entre su articulado. La finalidad de este servicio, no es otro que saber cuando los datos fueron emitidos por el remitente o recibidos por el destinatario.

[265] De acuerdo con el punto l) del artículo 2, éste es: "un programa o aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de F.E. por el prestador de servicios de certificación o para la creación o verificación de F.E.".

[266] Téngase en cuenta que, en la normativa vigente, para ser entidad de evaluación hace falta haber sido acreditada ante el organismo independiente al que se le haya atribuido esa facultad. El Proyecto de Ley da un paso adelante en su artículo 2-n), al posibilitar que la acreditación la lleve a cabo un organismo público o privado, con el único fin de fomentar la autorregulación de la industria del sector, para que ésta sea quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación, destinados a mejorar los niveles técnicos y de calidad en la prestación de estos servicios, impulsando consiguientemente la creación de nuevos servicios. Además en este sentido, tenemos que añadir el supuesto regulado en el artículo 2-q) del Proyecto de Ley, que crea un nuevo instrumento denominado Declaración de Prácticas de Certificación que consiste en la emisión de un documento actualizado en el que se especifican por parte del prestador de servicios de certificación los aspectos relevantes de la gestión del ciclo de vida de los certificados, incluyendo las condiciones para la solicitud, emisión, uso, suspensión y perdida de vigencia de los certificados.

prestador ha podido ser reconocido. Esta problemática trata de salvarla el Proyecto de Ley en los términos explicados en la nota 266.

Al margen del sistema mencionado, se crea en el Ministerio de Justicia un Registro de Prestadores de Servicios de Certificación, en el que deberán inscribirse con carácter previo al inicio de su actividad, todos los que estén establecidos en España. Debemos entender que esta inscripción es sólo a efectos de publicidad, argumento que se ve reforzado a tenor de lo dispuesto en el artículo 6 del Proyecto de Ley, al recoger que esta inscripción lo será sólo a estos efectos.

Pasando a la regulación de los certificados, nos centraremos en primer lugar en los requisitos que han de contener los certificados reconocidos. Éstos son los siguientes:

a) La indicación de que se expiden como tales.
b) El código identificativo del certificado.
c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y en su caso, sus datos de identificación registral.
d) La F.E.A. del prestador de servicios de certificación que expide el certificado.
e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquel de su consentimiento.
f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.
g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo control del signatario.
h) El comienzo y fin del período de validez del certificado.
i) Los límites de uso del certificado, si se prevén.
j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Para la consignación de cualquier otro tipo de información referente al signatario, se requerirá su consentimiento expreso.

Estos certificados quedarán sin efecto si concurre alguna de las siguientes circunstancias:

a) Expiración del período de validez del certificado. Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.
c) Pérdida o inutilización por daños del soporte del certificado.
d) Utilización indebida por un tercero.
e) Resolución judicial o administrativa que lo ordene.
f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida total o parcial de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
g) Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.
h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

La perdida de eficacia de éstos, en los supuestos de expiración de su periodo de validez y cese de la actividad del prestador de servicios, tendrá lugar desde que las circunstancias se produzcan. Para el resto de los casos, surtirá efecto desde la fecha en la que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11-e). Para todos los supuestos será necesaria la inscripción por parte del prestador de servicios de la perdida de eficacia en el citado Registro, respondiendo de los posibles perjuicios que cause al signatario o a terceros de buena fe por el retraso de la publicación. En todo caso, corresponderá al prestador de servicios la prueba de que los terceros conocían las causas invalidantes del certificado.

También cabe la suspensión temporal del certificado, que se producirá por petición del signatario o sus representados u orden judicial o administrativa.

Para finalizar lo referente a los certificados, señalaremos bajo qué condiciones un certificado expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente a la U.E., es válido en España. Es necesario que los certificados, además de ser conformes a la legislación de ese país y ser reconocidos, cumplan alguna de las siguientes condiciones:

a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre F.E. y haya sido acreditado conforme a un sistema voluntario en un E.E.M.M..
b) Que el certificado éste garantizado por un prestador de servicios de la U.E. que cumpla los requisitos establecidos en la normativa comunitaria sobre F.E..
c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

Pasando a continuación al régimen jurídico establecido para los prestadores de servicios de certificación, comenzaremos indicando las obligaciones que deben cumplir todos los prestadores de servicios de certificación, que no son otras que las siguientes:

a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y cuenta suya, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados, relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquellos.
b) Poner a disposición del signatario los dispositivos de creación y de verificación de F.E..
c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.
d) Informar antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.
e) Mantener un registro de certificados en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o pérdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.
f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el artículo 13.1, a los titulares de los certificados por ellos emitidos y si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.
g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.
h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-Ley y en sus normas de desarrollo.

Pero si el prestador de servicios de certificación, además expide certificados reconocidos, aparte de las ya mencionadas, le será exigible el cumplimiento de los siguientes requisitos:

a) Indicar la fecha y hora en las que se expidió o se dejó sin efecto al certificado.
b) Demostrar la fiabilidad necesaria de sus servicios.
c) Garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta al registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de estos de forma segura e inmediata.

d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la F.E. y los procedimientos de seguridad y gestión adecuados.
e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
f) Tomar medidas contra la falsificación de certificados y en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.
g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en el Real Decreto-Ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.
   Inicialmente la garantía cubrirá al menos un 4% de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno por Real Decreto podrá reducir el citado porcentaje, hasta un 2%.
   En el caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir cubrirá al menos, su responsabilidad por un importe de 6.010.121,04 euros[267], importe que podrá ser modificado por Real Decreto.
h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante 15 años. Esta actividad de registro podrá realizarse por medios electrónicos.
i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.
j) Utilizar sistemas fiables para almacenar certificados de tal modo que:
   1º Solo personas autorizadas puedan consultarlos, si éstos sólo están únicamente disponibles para verificación de F.E..
   2º Únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.

[267] El Proyecto de Ley, impone la obligación de constituir una garantía a través de un contrato de fianza o seguro de caución por un importe de, al menos, 3.000.000 de euros.

3º Pueda comprobarse la autenticidad de la información.
4º El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-Ley y sus disposiciones de desarrollo, durante el ejercicio de su actividad.

Continuando con el estudio del régimen jurídico de los prestadores de servicios de certificación, pasamos a continuación a las obligaciones que tienen en el caso de que cesen en la actividad. De esta manera estarán obligados a comunicar, con una antelación mínima de dos meses, el cese en su actividad a los titulares de los certificados expedidos por ellos y a transferir, con consentimiento expreso del titular, los que sigan siendo válidos en la fecha en que el cese se produzca, a otro prestador de servicios que los asuma o dejarlos sin efecto.

Si el prestador estuviera inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar a éste, en los mismos términos que en el apartado anterior, el citado cese y el destino que se va a dar a los certificados. Deberá asimismo comunicar la concurrencia de cualquier otra circunstancia relevante en el cese de su actividad, como la existencia de un procedimiento de quiebra o suspensión de pagos. Producido el cese, el Ministerio de Justicia cancelará de oficio la inscripción en el Registro e igualmente se hará cargo de la información relativa a los certificados que se hubieran dejado sin efecto, en aras del cumplimiento de la obligación de conservación de toda la información y documentación relativa a un certificado reconocido durante 15 años, que ya vimos en su momento.

En lo referente a la responsabilidad de los prestadores de servicios de certificación, están obligados a responder por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone el Real Decreto-Ley o actúen con negligencia, debiendo soportar la carga de la prueba de que actuaron con la debida diligencia.

Sólo responderán por los daños y perjuicios causados por el uso indebido de un certificado reconocido, cuando no hayan consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que puedan realizarse en su empleo.

Esta responsabilidad se regirá, aparte de las especialidades ya mencionadas, por las normas generales sobre culpa contractual o extracontractual, según proceda. En el caso de que la garantía establecida por el prestador no resulte suficiente para cubrir el montante total de la indemnización, responderá de la deuda con sus bienes presentes y futuros.

En lo que respecta a la protección de los datos personales de los usuarios que aportan al prestador de servicios de certificación para la emisión del correspondiente certificado, así como los que se anoten en el Registro de Prestadores de Servicios de Certificación, deberán estar sujetos a lo que dispone la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo (hoy Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal).

Para la emisión de los certificados, los prestadores únicamente podrán recabar datos personales directamente de sus titulares o con su consentimiento expreso. Estos datos serán los imprescindibles para la expedición y el mantenimiento del certificado. No obstante, si a petición del signatario han consignado un seudónimo, deberán cerciorarse de su verdadera identidad y conservar la documentación que la acredite. En este supuesto los prestadores de servicios estarán obligados a revelar la identidad del titular del certificado siempre que un órgano jurisdiccional así lo acuerde y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, sin perjuicio de lo previsto en la legislación específica en tributación, defensa de la competencia y seguridad pública.

Para la supervisión y control de lo dispuesto para los prestadores de servicios de certificación, se establece un procedimiento de supervisión y control, que corresponde Ministerio de Ciencia y Tecnología. No vamos a entrar en el procedimiento, pero sí indicaremos que se impone a los prestadores de servicios de certificación un deber de colaboración, en los mismos términos que los que se vieron en su momento en la LSSI.

Para finalizar, veremos los dispositivos de F.E. y la evaluación de su conformidad con la normativa aplicable.

Comenzaremos por los requisitos que se exigen para que se considere a un dispositivo de creación de firma seguro, éstos son:

1º Que se garantice que los datos utilizados para la generación de la firma puedan producirse sólo una vez que se asegure razonablemente su secreto.
2º Que exista seguridad razonable que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y que la firma no pueda ser falsificada con la tecnología existente en cada momento.
3º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.
4º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

Estos dispositivos podrán ser evaluados por los órganos de certificación, a los que nos referimos en su momento, previo examen de los informes técnicos emitidos

sobre los mismos por las entidades de evaluación acreditadas (también mencionadas anteriormente) o serán reconocidos si han sido emitidos por los organismos designados para ellos por los E.E.M.M., cuando estos dispositivos cumplan lo dispuesto en la Directiva 1999/93/CE.

En otro orden de cosas y con el único objeto de otorgar seguridad jurídica, se establece que los productos de F.E. que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el DOCE (recuérdese lo que en este sentido se estableció durante la explicación de la Directiva 1999/93/CE) son conformes a lo previsto para los dispositivos seguros de creación de firma y la obligación de los prestadores de servicios de certificación que emiten certificados reconocidos, en lo referente al uso de sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica.

Sin perjuicio de esta presunción, los números de referencia de estas normas se publicará en el BOE.

El último apartado a tratar es el referente a las garantías que deben ofrecer los dispositivos de verificación de F.E.A.; éstas son los siguientes:
1º Que la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente.
2º Que el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.
3º Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo.
4º Que se verifica de forma fiable un certificado.
5º Que puede detectarse cualquier cambio relativo a su seguridad.

Finalizando ya lo que respecta a la normativa vigente de F.E., sólo mencionaremos que se crea una tasa por el servicio que prestan los órganos de acreditación competentes, en los supuestos que se han visto a lo largo de la explicación y que se establece un régimen de infracciones y sanciones por el incumplimiento de las disposiciones contenidas en el Real Decreto-Ley, en el que tampoco vamos a entrar. Sólo indicaremos que el borrador de Anteproyecto de Ley crea un régimen de infracciones y sanciones muy similar al que establece la LSSI. Al llegar a imponer la misma graduación y cuantía en las multas, el lector puede hacerse una idea de esa similitud.

B) El Proyecto de Ley de Firma Electrónica.

A lo largo del epígrafe anterior ya se han ido citando algunas de las novedades que contiene este Proyecto de Ley. Proyecto que en líneas generales mantiene la misma

regulación que el Real Decreto-Ley, pero que aspira a incorporar innovaciones a la vista de la experiencia recogida a través de la aplicación de este Real Decreto-Ley.

Ya vimos que una de las tres novedades más destacables es la posibilidad de que los prestadores de servicios de certificación utilicen la autorregulación, en lo que a la acreditación voluntaria de prestación de servicios de certificación concierne, pero además queremos destacar la creación del Documento Nacional de Identidad Electrónico y la posibilidad de expedir certificados a personas jurídicas.

Comenzando por el primer aspecto, entendemos por Documento Nacional de Identidad Electrónico, según los artículos 2-o), 25 y 26, el Documento Nacional de Identidad expedido por el Estado, que acredita electrónicamente la identidad de la persona y que permite la firma electrónica de documentos.

Éste surtirá plenos efectos para la acreditación de la identidad y de los demás datos personales del titular que, conforme a la normativa reguladora del D.N.I. consten en el mismo. De esta manera, será suficiente para acreditar en un procedimiento administrativo la identidad y demás datos personales que consten del titular, así como para comprobar la integridad de los documentos firmados haciendo uso de los instrumentos de firma incluidos en él, según lo previsto en los artículos 45 y 70.1 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Éste, a tenor de lo dispuesto en el artículo 26, deberá en lo que a la F.E. del mismo se refiere, utilizar el mecanismo de la F.E.A. basada en un certificado reconocido[268]. Es por ello que si además de lo anterior, se ha utilizado un dispositivo seguro de creación de firma en su elaboración, el documento firmado electrónicamente, tendrá los mismos efectos que la firma manuscrita en soporte de papel.

Finalmente se dispone que, en la medida de lo posible, éste debe ser compatible con el resto dispositivos y productos de firma electrónica generalmente aceptados.

Pasando a la posibilidad de emisión de certificados a las personas jurídicas, empezaremos señalando que esta novedad tiene su origen en la demanda del sector de los servicios de certificación.

Según se pretende regular, podrán solicitarlo los administradores, representantes legales y apoderados de la persona jurídica para la cual se solicita, que tengan poder bastante a estos efectos.

De la regulación de este supuesto, sólo vamos a resaltar una cuestión que nos parece significativa y que no es otra que la custodia de los datos de firma y del

[268] El apartado primero del artículo 26 dispone que el órgano público de la Administración del Estado que elabore este documento deberá, cumplir las condiciones previstas en esta Ley para la expedición de certificados reconocidos.

certificado corresponderá a una sola persona física o factor por certificado, cuyo nombre y apellidos o cualquier otro dato adicional que resulte necesario para su identificación, figurarán en el certificado emitido a nombre de la persona jurídica. Si esta persona perdiera la autorización para custodiar estos datos, debe ser la persona jurídica la que solicite la revocación del certificado.

III) La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

A) Antecedentes.

Los antecedentes a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), los encontramos en la Ley Orgánica 5/1992 de 29 de octubre, Reguladora del Tratamiento Automatizado de Datos (LORTAD).

La LORTAD fue publicada como consecuencia de la ratificación por el Reino de España del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, firmado en Estrasburgo por el Plenipotenciario de España el 28 de enero de 1982[269], el cual dispone que los estados signatarios quedan obligados a desarrollar una ley que proteja los datos de carácter personal[270].

Posteriormente, la ley fue derogada con la entrada en vigor de la LOPD, ya que como habrá podido apreciar el lector, la LORTAD es anterior a la Directiva 1995/46/CE, y es por ello que se hacia necesario o bien adecuar la norma a lo dispuesto en la Directiva, o bien, como al final fue el caso, aprobar una nueva disposición.

Al tratarse de una norma ya derogada, no vamos a estudiar su régimen jurídico, ni siquiera con vistas a compararlo con el actual. Nuestra intención es centrarnos en la legislación vigente, dejando constancia de la norma precedente, ya que al amparo de esta norma se dictaron, como se verá en su momento, dos Reglamentos que continúan aún vigentes, al amparo de la disposición transitoria tercera de la LOPD.

B) Objeto de la Ley.

Recogido en el artículo 1º de la ley, se establece que el fin pretendido es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Esta manifestación se ha visto reforzada por la Sentencia del Tribunal Constitucional –STC 292/2000 de 30 de noviembre- la cual establece que el

[269] BOE 274 de 15.11.1985.

[270] No ha sido éste el único acto del Consejo de Europa, puesto que ha elaborado una larga serie de Recomendaciones y Resoluciones en la materia. Éstas pueden ser consultadas en: Davara Rodríguez, Miguel Angel. "Manual de Derecho Informático" Aranzadi 2002. Pág. 56 y ss.

derecho a la protección de datos es un derecho, que sin estar recogido expresamente en la Constitución, goza del rango de derecho fundamental autónomo, que tiene su justificación en la llamada libertad informática y el derecho a impedir o restringir el uso de datos personales para un uso diferente al que justificó su obtención, es decir, atribuye a la persona un derecho de uso y destino sobre sus datos. Como bien señala algún sector de la Doctrina, lo que se establece es un derecho de autodeterminación de la persona, que reconoce a su titular, la facultad de decidir cuándo y cómo está dispuesta a permitir que sea difundida su información personal o a difundirla ella misma, esto es, la facultad de la persona de controlar y conocer los datos que sobre ella se encuentran en soportes físicos[271].

Como consecuencia de estas afirmaciones, no debemos entender el derecho a la protección de datos, como así continua rezando la sentencia del Constitucional, como una vertiente del derecho a la intimidad, sino que esa protección se extiende a cualquier tipo de dato personal, intimo o no, público o privado, ya que por el hecho de que un dato personal sea público, no escapa del poder de disposición de su titular. Es más, ese derecho se amplia a todos los datos que identifiquen o permitan identificar a una persona, pudiendo servir para la confección del perfil ideológico, racial, sexual, económico o de cualquier índole.

Continuando con el planteamiento de la situación, el artículo 2.1 establece que la ley será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Para entender esta disposición, se hace ya necesario definir "dato de carácter personal", y "tratamiento". Por dato de carácter personal entendemos, según el artículo 3 a): cualquier información concerniente a personas físicas identificadas o identificables[272]. Por tratamiento entendemos, según el artículo 3 c): operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como, las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

De lo anteriormente dicho se puede establecer que prácticamente nada escapa al control de esta ley (salvo las excepciones que veremos más adelante), ya que entran dentro del ámbito de aplicación legal, los tratamientos de datos no automatizados (por ejemplo en soporte papel, aunque hasta el 24 de octubre de 2007 están exentos de cumplir ciertas obligaciones de la ley, según reza la disposición adicional primera) y la ley se aplica tanto a los tratamientos de titularidad pública como privada (en este concepto deben agruparse las empresas y profesionales liberales).

[271] Davara Rodríguez, Miguel Ángel. Ob. Cit. Página 58.

[272] Se plantearon dudas sobre sí la dirección de correo electrónico o *e-mail* constituye un dato de carácter personal. En este sentido se pronuncia la APD en su Memoria de 2000, página 338 indicando que, si la información está constituida por un conjunto de signos que permiten la vinculación directa o indirecta con una persona física, debe entenderse que constituye un dato de carácter personal. .

Es más, aunque la LOPD extiende su ámbito de protección a las personas físicas, se planteó la duda de sí un empresario o profesional liberal que no revistiera su actividad bajo la forma de empresa, estaba o no protegido por la LOPD. Tras una serie de vaivenes iniciales, la APD ha entendido a raíz de la Resolución que dictó el 27 de septiembre de 2001, que habrá que analizar cada caso concreto, viendo si cabe diferenciar entre la actividad empresarial o profesional, y la propiamente privada de ese individuo en cuestión, es decir ver si los datos personales han sido tratados sólo por su consideración de empresario o profesional liberal[273]. En esta misma línea se encuentra la Sentencia de la Audiencia Nacional de 11 de octubre de 2002, que obliga a diferenciar si el dato se refiere a la persona-empresa o a la persona, estando protegidos si es imposible diferenciar su actividad mercantil de su propia esfera de actividad.

A continuación, mencionaremos las reglas que otorgan competencia a la LOPD, es decir cuando se entiende que es de aplicación la legislación española. No olvidemos que en un mundo internacionalizado, los datos de las personas fluyen por todo el globo terráqueo (pensemos en una transferencia de fondos de un banco a otro, sólo por poner un ejemplo). Estas reglas son las siguientes:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento[274].
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de derecho internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la U.E. y utilice en el tratamiento de datos medios situados en el territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Por su parte se establecen una serie de excepciones a la aplicación de la LOPD, unas de exención y otras de remisión a la normativa específica. Empezando por las primeras, no se aplicará la LOPD a:

a) A los ficheros[275] mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domesticas.

[273] Para más información, véase Memoria de la APD de 2001 y Aparicio Salom, Ob. Cit. Páginas 41 y ss.

[274] Entendemos por responsable del tratamiento, de acuerdo con el artículo 3 d): a la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. No obstante, existen dos supuestos en los que se establecen especialidades en cuanto a quien se entiende que es el responsable de tratamiento. En la Instrucción de la APD 1/1996, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, la APD entiende que el responsable será aquel por cuya cuenta se efectúe el servicio de seguridad, pero mediante el correspondiente contrato de prestación de servicios cabe entender que el responsable es la empresa que presta los servicios de seguridad. Estos datos serán destruidos en el plazo de 1 mes desde su obtención y no podrán ser cedidos salvo consentimiento del afectado o por disposición legal. Por otro lado tenemos la Instrucción 2/1996 de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo. El responsable en estos casos será la sociedad que explota el casino o la sala de bingo. Los datos serán cancelados en el plazo de seis meses desde el último acceso y no podrán ser utilizados para otros fines.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de la delincuencia organizada. No obstante, en esos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos (APD)[276].

Se regirán por su normativa específica y por lo especialmente previsto, en su caso, por esta ley, los siguientes tratamientos de datos personales:

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

C) Principios de la Protección de Datos.

Adentrándonos en la regulación jurídica de la LOPD, vamos a pasar a exponer una serie de principios que deben regir toda actividad de tratamiento de datos de carácter personal.

El primero, aunque parezca de perogrullo, es el principio de calidad de los datos. En virtud de esta disposición, los datos de carácter personal sólo se podrán recoger y someter a tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. De la misma manera, una vez obtenidos no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido obtenidos. La única excepción es su mantenimiento posterior por fines históricos, estadísticos o científicos. A la vista de esta disposición, se puede plantear el lector la tremenda ambigüedad de ésta, ya que habrá que delimitar caso por caso y sector por sector,

[275] Atendiendo al artículo 3 b), entendemos por este: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización o acceso. El concepto que utiliza la APD de fichero implica que debe estar organizado de modo que permita su acceso y consulta conforme a un criterio lógico y determinado (numérico, alfabético...) Memoria de la APD del 2000, página 54.

[276] La Agencia 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. No vamos a entrar en su regulación jurídica, órganos y funciones, aunque señalaremos que esta regulación se contiene en los artículos 35 y ss de la LOPD y en el Real Decreto 428/1993 de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. BOE 106 de 4.5.1993.

qué datos son pertinentes, adecuados y no excesivos. Pero en aras de intentar clarificar esta norma, indicaremos que en la práctica se ha demostrado que puede salvarse con picardía. Por poner un ejemplo, una agencia inmobiliaria puede pensar que al tomar los datos de una persona identificada e identificable a la hora de buscarle un inmueble, necesita indicar en el apartado del fichero en el que aparece esa persona, que es un minusválido (lo cual acarrea otra serie de problemas al ser considerado como dato de salud); y basa esa necesidad en que de esa manera sólo buscará inmuebles con ascensor, pisos en planta baja y que no tengan escalones de acceso al portal, o en su defecto, que posean rampa. Analizando la situación, hemos llegado a la conclusión de que es conveniente salvar esa situación indicando en vez de que el cliente es minusválido, que el cliente solicita un piso con esas características, al igual que podría solicitar un piso exterior o con mucha luz, ya que si una persona quiere un bajo o piso con ascensor, bien puede ser minusválido, pero también puede ser un anciano o un matrimonio joven con niños pequeños.

Continuando con ese principio de calidad de los datos, la LOPD establece que los datos deben ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado[277]. En el caso de resultar inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correctos. En virtud de esta apartado, pueden plantearse multitud de dudas y problemas prácticos, aunque nosotros sólo vamos a plantearnos dos. El primero es qué ocurre si se trata algún dato erróneo de una persona física identificada o identificable, cuando ese dato en cuestión no responde a la finalidad y uso de ese tratamiento. Como ya ha tenido ocasión de comprobar la APD, si en un fichero de morosos, cuya finalidad es informar sobre si una persona física lo es, o no, que aparezca el DNI erróneo no constituye una infracción del principio de calidad de los datos[278]. El segundo consiste en el supuesto de que el afectado no actualice al responsable del tratamiento sus datos. Como bien señala Aparicio Salom[279], no puede entenderse que el responsable del tratamiento deba ejercer una actividad de investigación sobre los datos que posee, es el afectado el que debe comunicárselos. El deber establecido de actuar de oficio que establece la ley, debe entenderse desde el momento en el que el responsable tenga conocimiento de la inexactitud de los datos. Sólo en el caso de que los datos procedan de fuentes accesibles al público (serán estudiadas más adelante), y se produzca una actualización de esta fuente, el responsable estará obligado a rectificar de oficio sin necesidad de comunicación por parte del afectado.

Para finalizar este principio indicaremos que los datos deberán ser cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la que hubieran sido requeridos o recogidos, que los datos deberán ser almacenados de manera que

[277] Según el artículo 3 e), afectado o interesado es: la persona física titular de los datos que sean objeto del tratamiento al que se refiere el apartado c) del presente artículo.
[278] Para más información, véase Aparicio Salom, Ob. Cit. Páginas 57 y ss.
[279] Ob. Cit páginas 112 y ss.

permitan el ejercicio del derecho de acceso, salvo que legalmente sean cancelados, y que la LOPD prohibe expresamente que se recojan datos por medios fraudulentos, desleales o ilícitos.

Continuando con nuestro estudio, nos encontramos con otro de los deberes que impone la LOPD, el derecho de información en la recogida de datos. En virtud de este derecho, los interesados deberán ser previamente informados a la recogida de sus datos personales, de modo expreso, preciso e inequívoco en los siguientes aspectos:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante[280].

Solamente deberán constar las advertencias primera y última, si el resto de advertencias se deducen claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Se establece igualmente que esta información deberá constar de manera claramente legible, si para la recogida de datos se utilizan cuestionarios u otros impresos.

Eso sí, si los datos no se han obtenido directamente del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del fichero o por su representante[281], dentro de los tres meses siguientes al registro de los datos, salvo que ya hubiera sido informado con anterioridad en los términos analizados anteriormente. De esto se deduce que si por ejemplo un familiar facilitó los datos de carácter personal y estos fueron recogidos en un cuestionario que informaba en los términos establecidos legalmente, y se entregó una copia del mismo al familiar, el interesado ya habrá sido informado previamente.

[280] Esta obligación adquiere gran relevancia si nos encontramos en el sector del C. E.. Como ha tenido ocasión de manifestar la APD en "Recomendaciones de la APD al sector del Comercio Electrónico, para la adecuación de su funcionamiento a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal", es necesario informar en todo momento de la identidad del responsable del tratamiento, sobre todo si se ha llegado a esa página a través de un hiperenlace. Por ello es necesario informar al usuario de modo inequívoco que el control va a transferirse a otra Web.

[281] Para garantizar el correcto cumplimiento del deber de informar al afectado, la LOPD establece que cuando el responsable de tratamiento no esté establecido en territorio de la U.E., y utilice en el tratamiento de datos medios situados en territorio español, deberá designar a un representante en España, salvo que tales medios se utilicen con fines de tránsito.

Lo anteriormente dispuesto no será de aplicación cuando así lo disponga una ley, el tratamiento tenga una finalidad histórica, estadística o científica o cuando la obligación de información resulte imposible o exija esfuerzos desproporcionados en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, eso sí, la interpretación de esta disposición queda al criterio de la APD u organismo autonómico equivalente. Si los datos proceden de fuentes accesibles al público y se destinan a la actividad de publicidad o prospección comercial, 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 los derechos que le asisten.

Esta obligación de información, tiene su origen en la intención de evitar vicios del consentimiento, y más en concreto un vicio en la prestación del consentimiento[282], ya que como veremos a continuación, el consentimiento es otro de los derechos que asisten a los afectados, y está íntimamente ligado al derecho de información. Nosotros vamos más adelante, ya que entendemos que la LOPD aparte de intentar evitar esos vicios, obliga a que el interesado esté en todo momento informado sobre el procedimiento de recogida de sus datos y cómo han sido obtenidos (véase párrafo anterior). Más adelante podremos argumentar con mas fuerza, ya que, como veremos, en el caso de que se pretendan ceder los datos personales, el interesado ha de ser informado previamente sobre el destino de sus datos. En definitiva la LOPD pretende a nuestro juicio crear un entramado tal, que investigando por parte del afectado consiga descubrir dónde y cómo ha obtenido sus datos una empresa a la que nunca se los ha facilitado. Y ese derecho de información puede ser en un caso de cesión de datos, una pieza importante de ese engranaje.

Como acabamos de manifestar, otro derecho íntimamente ligado al de información, es el del consentimiento. A tenor del artículo 6, se establece que el tratamiento de datos requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. Por consentimiento, a efectos de la LOPD entendemos: toda manifestación de voluntad, libre inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le concierna. Atendiendo a esta definición, se ha planteado la duda de cual es la forma en la que debe manifestarse ese consentimiento, si de forma expresa o si cabe también la presunta (se deduce de los propios actos del interesado; por ejemplo cumplimenta un cuestionario en el que se le informa en los términos previstos en el artículo 5) y la tácita (se desprende ese consentimiento de la no acción u omisión del interesado). La APD ha otorgado validez a estas formas de prestar el consentimiento, apoyándose en el artículo 7 que exige el consentimiento expreso para cierto tipo de datos, que serán analizados en breve. En suma la APD entiende que si para cierto tipo de datos, que gozan de la condición de especialmente protegidos, se requiere por la LOPD el consentimiento expreso, para el resto de

[282] Véase Aparicio Salom, Ob. Cit. Páginas 94 y ss.

datos valdrá cualquier forma de manifestación de la voluntad admisible en derecho[283].

Las excepciones a este derecho, vienen recogidas en el apartado siguiente del artículo 6, y son las siguientes:

- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Como bien señala Aparicio Salom[284], la LOPD permite una serie de tratamiento no consentidos, como el que puede establecerse ante la AEAT, ya que prevalece el deber público sobre la propia privacidad.
- 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. Se entiende para estos casos que el consentimiento se encuentra subsumido en el otorgado para la obligación principal.
- Cuando el tratamiento de los datos tenga la finalidad de proteger un interés vital del interesado, en los términos del artículo 7, apartado 6 de la presente ley (prevención y diagnostico medico, asistencia sanitaria...). En este caso prevalecen los derechos a la vida y a la salud sobre el de la privacidad.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Para estos casos, y siempre que una ley no disponga lo contrario, el afectado podrá oponerse al tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero viene obligado a excluir del tratamiento los datos relativos al afectado.

Con carácter general, indicaremos que el consentimiento podrá ser revocado cuando exista causa justificada para ello, no pudiendo atribuírsele efectos retroactivos.

Como ya hemos tenido la ocasión de comprobar, existe una categoría especial de datos, que se denominan datos especialmente protegidos. Esta diferenciación se apoya en el artículo 16.2 de la Constitución española, según el cual nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. De esta forma sólo podrán tratarse datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, si previamente se ha obtenido el consentimiento expreso del afectado[285] y se ha informado a éste de su derecho a no prestarlo. Se

[283] Para más información, véase Aparicio Salom, Ob. Cit. Páginas 70 y ss.
[284] Ob. Cit. Páginas 32 y ss.
[285] Si este tipo de datos se recogen a través de una Web, para que goce el consentimiento expreso de validez ante la APD, en el procedimiento de recogida se deberá articular algún procedimiento que permita al usuario de manera

exceptúan de este requisito los ficheros propiedad de los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de datos necesita el consentimiento expreso previo del afectado. Los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual, están radicalmente prohibidos (artículo 7.4).

Si los datos hacen referencia al origen racial o étnico[286], a la salud o a la vida sexual del afectado, sólo podrán ser recogidos, tratados y cedidos cuando, por razones de interés general, una ley así lo disponga o el afectado consienta expresamente.

En estos supuestos, sólo cabrá un tratamiento, cuando éste resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Esta habilitación se completa en el artículo 8, ya que se habilita a las Instituciones, centros sanitarios públicos y privados y a los profesionales correspondientes, para el tratamiento de datos relativos a la salud de las personas que a aquellos acudan, o hayan de ser tratados en los mismos, de acuerdo con la legislación sanitaria estatal o autonómica[287]. También podrá realizarse el tratamiento para salvaguardar el interés vital del afectado o de otra persona, si el afectado se encuentra física o jurídicamente incapacitado para dar su consentimiento.

Al no estar definidos estos conceptos en la LOPD, se han planteado dudas sobre su alcance y contenido, no obstante sólo nos vamos a referir a qué debe entenderse por dato de salud.

Teniendo en cuenta que como acabamos de indicar, el concepto no viene definido, ha obligado a la APD ha desarrollar una labor interpretativa de este concepto. En este sentido, y sin ánimo de ser exhaustivos, la APD en su Memoria de 2001, página 297 define dato de salud como "aquel que se desprenda de las normas nacionales e internacionales vigentes en España". La APD recoge expresamente el concepto de la Memoria Explicativa del Convenio 108 del Consejo de Europa, que los define como toda la información concerniente a la salud pasada, presente y

expresa y activa, prestar su consentimiento a que sus datos sean recabados y tratados. Véase Recomendaciones de la APD al sector del comercio electrónico... Ob. Cit.

[286] En relación a este tipo de datos, la APD entiende que no pueden considerarse como tales los datos relativos al aspecto externo de las personas, como el color de la piel o la apariencia física. Para que se dé este supuesto, el tratamiento deberá establecerse por motivo de la raza u origen. Para más información, véase Aparicio Salom, Ob. Cit, página 204.

[287] En este supuesto, deberá tenerse en cuenta la Ley 14/1986 de 25 de abril General de Sanidad. Un completo estudio de la materia se encuentra en Aparicio Salom, Ob. Cit. Páginas 196 y ss.

futura, física o mental, de un individuo. Con este concepto tan amplio, la APD ha tenido ocasión de considerar a los datos genéticos, como datos de salud, opinión no compartida por algún sector de la doctrina[288]. También ha considerado que el dato del porcentaje de minusvalía en relación con la retención a cuenta del IRPF, se considera dato de salud. Como bien manifiesta Aparicio Salom[289], en esta ocasión la APD no acierta, ya que una cosa es la salud, que se entiende como la existencia o ausencia de enfermedades, consistiendo la enfermedad en un desequilibrio orgánico que requiere cura para permitir la vuelta a la vida normal, y por otro lado se encuentra la discapacidad, que puede ser definida como una merma en las capacidades comunes de los individuos, que no tiene la característica de ser desequilibrante sino estable.

La última categoría de datos especialmente protegidos son los relativos a la comisión de infracciones penales o administrativas. En estos supuestos, los datos de carácter personal sólo podrán ser incluidos en los ficheros de la Administraciones Públicas competentes para ello, según las distintas normas reguladoras.

Especial mención merece el deber de seguridad de los datos. En virtud del artículo 9 se establece que el responsable del fichero, y en su caso el encargado de tratamiento (figura que analizaremos con detalle más adelante), deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico natural. En consecuencia, no se pueden registrar datos de carácter personal en ficheros que no reúnan las condiciones determinadas por vía reglamentaria con respecto a su integridad y a su seguridad y a la de los centros de tratamiento, locales, equipos y programas.

Para dar cumplimiento a esta disposición, y aprovechando la habilitación fijada en la ley, para que por reglamento se regulen estos requisitos de seguridad, ha podido mantenerse el Real Decreto 994/1999 de 14 de junio, de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal[290] (RMS). Este reglamento fue dictado en amparo de la LORTAD, pero a escasos meses de la aprobación de la LOPD, opción que no resulta muy lógica si tenemos en cuenta que la LORTAD sólo regulaba los tratamientos automatizados y, por el contrario la LOPD se ocupa de cualquier fichero recogido en soporte físico (por lo que cabe incluir también aquellos ficheros tratados en soporte papel, que como consecuencia de ello se encuentran excluidos del ámbito de aplicación del RMS).

[288] Véase Aparicio Salom, Ob. Cit. Páginas 205 y ss.
[289] Ob. Cit, página 206.
[290] BOE 151 de 25.6.1999.

En virtud del RMS se establecen tres niveles de protección, el Básico, el Medio y el Alto. El Básico es por defecto el nivel en el que se acogerán todos los datos que no se encuentren comprendidos en el Medio o Alto. El nivel Medio recoge todos los datos relativos a la comisión de infracciones penales y administrativas, datos de la Hacienda Pública, servicios financieros (a los que la APD ha añadido los de seguros) y los ficheros que contengan datos que sean suficientes para obtener una evaluación de la personalidad del individuo (para este supuesto no rigen las obligaciones de nombramiento de responsable de seguridad y creación del registro de incidencias que veremos a continuación, es por ello que algún sector de la doctrina lo denomina nivel medio atenuado[291]). Por último en el nivel Alto se encuentran los datos que calificábamos como especialmente protegidos que son los de salud, ideología, religión, creencias, origen racial o étnico, vida sexual y afiliación sindical. Estos tres niveles establecen diversas obligaciones de protección, siendo estas de carácter acumulativo, es decir, si poseemos datos de salud (nivel alto), deberemos adoptar las medidas del nivel básico, más las medidas del medio, más las medidas del alto.

Antes de comenzar a analizar las medidas a adoptar, dependiendo del nivel de seguridad en el que nos encontremos, debemos plantear una crítica general al RMS ya que, como se verá a continuación, impone un riguroso elenco de medidas a adoptar sin diferenciar si nos encontramos ante una empresa grande, pequeña o mediana. Para una gran empresa, estas medidas no suponen un gran esfuerzo económico y organizativo, pero para las pequeñas y medianas si lo es, ya que aparte del costo de las medidas técnico-informáticas a adoptar, exige que debido a la naturaleza de las obligaciones impuestas, una persona se dedique a estas cuestiones, y eso en una empresa de reducido tamaño, o para un profesional liberal es un costo inasumible, puesto que no se dedican a lo realmente importante, la facturación. Y no es tan difícil que una empresa se encuentre con ficheros de nivel medio o alto, ya que en un fichero de nóminas se pueden contener datos de minusvalías de sus trabajadores, altas y bajas laborales y datos de afiliación sindical. Y no pensemos en el nivel medio, que la experiencia demuestra que es el más común de los tres. Podemos preguntarnos en voz alta qué empresa no dispone de datos bancarios de sus clientes o trabajadores, o datos de transacciones realizadas a través de tarjetas de crédito.

Para cumplir con la obligación impuesta por el RMS, en los tres niveles de protección se debe establecer un Documento de Medidas de Seguridad. Este documento no se inscribe en la APD, pero debe estar disponible por si fuera requerido y debe mantenerse en todo momento actualizado. El documento establece una serie de medidas, que bien parecen un procedimiento de calidad, en cuanto al tratamiento de datos, que son de obligado conocimiento y cumplimiento por parte de todo el personal de la empresa.

[291] Aparicio Salom, Ob. Cit. Página 127.

Comenzando por las medidas a adoptar en el nivel de seguridad básico, son como mínimo, las siguientes:

A) Elementos que debe recoger el documento: Ámbito de aplicación del documento con especificación detallada de los recursos protegidos, medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido, funciones y obligaciones del personal, estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan, procedimiento de notificación, gestión y respuesta ante incidencias, procedimientos de realización de copias de respaldo y de recuperación de datos.

B) Medidas técnicas a adoptar: Definición de las funciones y obligaciones de cada una de las personas que acceden al fichero que contiene datos de carácter personal. Creación de un registro de notificación y gestión de incidencias en el que conste el tipo de incidencia, el momento en el que se produce, la persona que realiza la notificación, a quién se le comunica y los efectos que derivan de la misma. Creación de una relación actualizada del personal que tiene acceso autorizado al fichero y establecimiento un sistema de identificación y autenticación de acceso al mismo. Si ese procedimiento se basa en la creación de contraseñas, estas deberán cambiarse con periodicidad, y deberán ser asignadas distribuidas y almacenadas utilizando un procedimiento que garantice su confidencialidad e integridad. Este control de acceso de los usuarios del sistema, lo será para aquellos datos y recursos imprescindibles para el desarrollo de sus funciones. Esta asignación de recursos, así como su anulación o alteración, sólo podrá ser llevada a cabo por el personal expresamente autorizado para ello en el documento de seguridad. Creación de un registro de soportes informáticos, que permita inventariarlos y catalogarlos. Deberán ser almacenarlos en un lugar restringido para el personal que no esté autorizado a utilizar esos recursos. En caso de que salgan ficheros con datos de carácter personal fuera de los locales en los que esté ubicado el fichero, deberán obtener la autorización previa del responsable del fichero. La última obligación es la de realizar una copia de recuperación o de respaldo, al menos una vez por semana, de manera tal que permita garantizar la reconstrucción de los datos al estado en que se encontraban antes de su pérdida o destrucción.

Pasando a continuación a relatar las medidas de seguridad en el nivel medio, debemos indicar que la principal novedad es la obligación de nombrar, por parte del responsable del fichero, a uno o varios responsables de seguridad que coordinen y controlen las medidas definidas en el documento de seguridad, sin que pueda considerarse esta designación una delegación en las responsabilidades atribuidas al responsable del fichero. También es novedad la obligación de realizar una auditoria, interna o externa, al menos cada dos años. Ésta analizará los sistemas de información e instalaciones de tratamiento de datos y su adecuación a lo

establecido en el presente reglamento (lo que se trata de evitar con la auditoria, es, por ejemplo, que la ciencia avance tanto que una persona con escasos conocimientos informáticos pueda burlar el sistema de control de acceso establecido). El informe deberá dictaminar sobre la adecuación de las medidas y controles al presente reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Analizado el informe por parte del responsable de seguridad, elevará las conclusiones que estime oportunas al responsable del fichero para que éste adopte las medidas que considere necesarias. El informe quedará a disposición de la APD.

En cuanto a los mecanismos de identificación y autenticación, además de lo indicado ya para el nivel básico, deberán basarse en un sistema que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y verificar que está autorizado. De igual forma, se limitarán el número de intentos no autorizados al sistema. Los locales donde se encuentren ubicados los sistemas de tratamiento de información, se encontrarán restringidos al personal de la empresa, siendo necesario para su acceso encontrarse autorizado en el documento de seguridad. En lo relativo a la gestión de soportes, se debe establecer un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y la hora, el emisor, el número de soportes, el tipo de información que contiene, la forma de envío y la persona responsable de la recepción, que deberá estar debidamente autorizada. De la misma manera se creará un registro de salidas de soportes que contenga los mismos apartados que el de entrada. Cuando el soporte vaya a ser desechado, se deben adoptar todas las medidas necesarias que impidan la recuperación posterior de la información contenida en él, previamente a la baja del inventario. Si el soporte sale de los locales por operaciones de mantenimiento, se deberán adoptar las medidas necesarias para evitar la recuperación indebida de la información que contengan. En cuanto al registro de incidencias, se deberá consignar además, los procedimientos realizados en la recuperación de la información, indicando la persona que ejecutó el proceso, los datos restaurados, y en su caso, qué datos ha sido necesario grabar manualmente. Para estos procedimientos de recuperación de datos, será necesaria la autorización escrita del responsable del fichero. Finalmente se establece que si se realizan pruebas de un sistema de tratamiento de información con datos reales, para que estén permitidas se deberán realizar adoptando las medidas de seguridad aplicables al fichero tratado.

Para finalizar, indicaremos qué medidas han de adoptarse si el fichero posee datos que están calificados como de nivel de seguridad alto.

La primera medida a adoptar, consiste en cifrar los datos o utilizar cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulable cuando se distribuyan o transporten los soportes. Esa misma medida se establece

cuando se transmitan datos de carácter personal a través de redes de telecomunicaciones. Las copias de respaldo deberán almacenarse en lugar diferente a aquel en el que se encuentren los equipos informáticos que los tratan, cumpliendo en todo caso, las medidas de seguridad exigidas. Finalmente se endurecen las exigencias del sistema de autenticación e identificación, ya que de cada acceso se debe guardar en un registro creado a tal efecto, la identificación del usuario, la fecha y la hora en que accedió, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Estos mecanismos de registro estarán sometidos al control directo del responsable de seguridad, sin que quepa articular un procedimiento que pueda desactivarlos. El periodo de conservación de los datos consignados en el registro será como mínimo, de dos años. Por último el responsable de seguridad viene obligado, al menos una vez al mes, a elaborar un informe con los problemas detectados y las revisiones realizadas.

Finalizado este apartado, pasamos a mencionar otro de los deberes que establece la LOPD, deber que no es otro que el de secreto. En virtud de éste, el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal (entre los que podemos incluir al encargado de tratamiento, figura que se analizará a continuación), están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Estas obligaciones subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. De lo anteriormente dicho se deducen dos cosas, la primera es que a tenor de esta disposición el personal que trabaje para el responsable del fichero está sujeto a las obligaciones mencionadas, y segundo, que esa obligación persiste inclusive finalizada la relación laboral o mercantil que los unía.

Terminaremos las exposiciones referentes a este epígrafe, refiriéndonos a dos figuras que presentan gran relevancia en la LOPD. Nos estamos refiriendo a la comunicación de datos, y al acceso a los datos por cuenta de terceros.

Comenzando por la comunicación de datos, que según la definición que da la LOPD es, toda revelación de datos realizada a persona distinta del interesado, mencionaremos que para que esta comunicación de datos a un tercero sea válida, debe realizarse para cumplir los fines directamente relacionados con las funciones legítimas del cedente y cesionario, previo consentimiento del cedente. No obstante, este consentimiento no será necesario si la cesión está autorizada por una ley, si los datos están recogidos de fuentes accesibles al público y cuando el tratamiento responde 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. Para que sea válida en este caso, la cesión ha de limitarse a la finalidad que se justifique. Tampoco será necesario prestar consentimiento cuando la comunicación deba efectuarse al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen encomendadas. Tampoco será necesario cuando la

comunicación se dirija a instituciones autonómicas análogas al Defensor del Pueblo y Tribunal de Cuentas. Estarán exentas igualmente las comunicaciones entre Administraciones Públicas que tengan por objeto el tratamiento posterior con fines históricos, estadísticos o científicos, ni cuando los datos sean relativos a la salud, y esa cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

El consentimiento será nulo cuando la información facilitada al interesado no le permita conocer la finalidad a la que se destinan sus datos, o el tipo de actividad de aquel a quién se pretenden comunicar. Para la APD[292], para que sea válido se debe informar claramente al interesado sobre el destino de sus datos, siendo nulas las fórmulas genéricas (entre las cuales cabe incluir las de cesión de datos al grupo de empresas, para los cuales, se entiende que aunque integrados en un grupo, cada empresa goza de personalidad jurídica propia). Este consentimiento tiene, como no podía ser de otra manera, carácter revocable. No obstante, todo lo dicho no será aplicable si previamente a la comunicación de datos, se lleva a la practica un procedimiento de disociación de datos. Este procedimiento, según queda definido por la ley, consiste en todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. Para dar cuerpo a esta previsión, la APD en su Memoria de 2000 página 100, manifestó que si los datos personales van unidos a un Código, y ese Código puede a posteriori ser asociado a una persona identificada o identificable, no estamos ante datos disociados. De esto se deduce que si queremos disociar los datos, el procedimiento ha de ser tal que no puedan volver a asociarse.

Para los ficheros de titularidad privada, se plantea una especialidad, ya que según dispone la LOPD, el responsable del fichero deberá informar a los afectados en cuanto se produzca la primera cesión de datos. Este deber de información abarcará la finalidad del fichero, la naturaleza de los datos que han sido cedidos y la dirección el cesionario. El responsable del tratamiento no vendrá obligado a cumplir esta disposición cuando la cesión venga impuesta por una ley, cuando los datos hayan sido previamente disociados, y 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 ese caso la cesión será legítima, si se limita a la finalidad que la justifica. También estará el responsable de tratamiento exento si la comunicación tiene por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas u organismos autonómicos equivalentes, en el ejercicio de sus funciones. La última excepción es la que se fundamenta en una cesión de datos entre Administraciones Públicas con el objeto del tratamiento posterior de datos con fines históricos, estadísticos o científicos.

[292] Véanse Memorias de la APD de 2000 y 2001.

Las cesiones de datos son muy comunes en las actividades de publicidad o marketing directo, existiendo diversas modalidades de contratos, tales como: el arrendamiento de datos por el cual una empresa arrienda los datos que posee a una tercera empresa para que los utilice para una o varias campañas publicitarias, y que en nuestra opinión deberá formalizarse por escrito indicando los usos y finalidades del arrendamiento, así como las obligaciones y limites del arrendatario. Otra modalidad es la ejecución de campañas de marketing, por la cual una empresa ofrece a terceros la posibilidad de utilizar los ficheros que posee para la ejecución de la campaña, en este caso la empresa arrendataria debe ser diligente a la hora de elegir a la empresa arrendadora, ya que atendiendo a la doctrina de la APD, la arrendataria es la que ordena el tratamiento y por ende, puede ser sancionada si no se obtuvo el consentimiento por parte de la arrendataria, de los interesados a los que se dirija la publicidad, postura refrendada por la Sentencia de la Audiencia Nacional de 21 de junio de 2002, que establece en un caso similar al descrito que el responsable de tratamiento es aquel que decide sobre la finalidad y usos del fichero y del tratamiento, es decir, además del que decide y trata, se entiende responsable al que teniendo poder de decisión encomienda la materialidad del tratamiento a un tercero, lo que sucede cuando se contrata a otra empresa para que realice una campaña publicitaria. La tercera modalidad es la impresión de etiquetas y entrega posterior a la arrendataria, para que las pegue y las envíe. Esta actividad, en lo que se refiere a quién se considera responsable del fichero, no es pacífica, existiendo opiniones contradictorias entre la APD y la jurisprudencia[293]. Por último se encuentra el alquiler de espacio publicitario. En virtud de este contrato una empresa que envía regularmente documentación a sus clientes, con vistas a amortizar los costes de envío, remite publicidad de terceros. En ese supuesto, debe requerirse el consentimiento del afectado, ya que se produce una desviación de la finalidad de uso de los datos, para la cual el interesado prestó su consentimiento.

Para el tercero al que se comunican los datos, cabe decir que queda sometido, aunque no sea el responsable del fichero, a todas las obligaciones que impone la ley.

Entrando a continuación en el apartado del acceso a los datos por parte de un tercero, comenzaremos distinguiéndola de la comunicación de datos. Para que no se considere comunicación, el acceso ha de ser necesario para la prestación de un servicio al responsable del fichero. Este acceso para ser legal, ha de constar por escrito o de alguna manera que permita hacer constar su celebración y contenido, en un contrato, estableciéndose expresamente que ese tercero, denominado encargado de tratamiento[294], únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin

[293] Para más información, véase Aparicio Salom, Ob. Cit. Páginas 191 y ss.

[294] La definición que le otorga el artículo 3 g) de la LOPD, es la siguiente: 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.

distinto al que figure en el contrato, ni los comunicará, ni siquiera para su conservación a otras personas, en cuyo caso sería considerado a todos los efectos como responsable del fichero. En el contrato se estipularán las medidas de seguridad que correspondan al fichero en cuestión, que el encargado de tratamiento está obligado a poner en práctica. Una vez finalizada la relación contractual, el encargado de tratamiento viene obligado a la devolución o destrucción de los datos de carácter personal que posea.

Vista la regulación, el lector podrá preguntarse en qué casos puede considerarse un acceso a datos por cuenta de un tercero, y debemos indicar que se da en más supuestos que los que podemos pensar. Así por ejemplo, una empresa puede delegar en una Gestoría sus obligaciones laborales, respecto del fichero de personal de la empresa y fiscales, entre las que se encuentran la contabilidad y facturación del posible fichero de proveedores. Es más, incluso puede que toda la información se encuentre en la Gestoría y no en la empresa, pero ésta primera es a todas luces un mero encargado de tratamiento. O pensemos en un Administrador de Fincas, que posee datos de las Comunidades de Propietarios (entre la que puede encontrarse la de propietarios, empleados, proveedores...), o en una empresa de prevención de riesgos laborales, que actúe en la rama salud, accediendo a datos de los trabajadores de la empresa cliente.

Para finalizar el apartado, mencionaremos una variedad de contrato de arrendamiento de servicios, denominado *outsourcing*, que consiste en que el responsable del tratamiento encarga a un tercero la custodia, mantenimiento y conservación de los datos. Esta variedad puede presentar diversas modalidades prácticas, como los contratos estrella en Internet: el *hosting* y el *housing*. El primero consiste en que el operador sólo presta al responsable las herramientas necesarias para la gestión del fichero (emplazamiento, *hardware*[295] y líneas de comunicación). En el segundo además de prestar esas herramientas, el prestador facilita el *software*[296], y lo explota, por lo que sería el responsable de los accesos no autorizados al sistema.

D) Derechos de las personas.

En este epígrafe, nos disponemos a analizar los derechos que la ley otorga a los particulares. Debemos manifestar que en lo que respecta a los derechos de acceso, rectificación y cancelación, además de la normativa recogida en la LOPD, debemos acudir al Real Decreto 1332/1994 de 20 de junio, por el que se desarrollan diversos aspectos de la ley orgánica (reglamento LORTAD)[297] y a la Instrucción de la APD 1/1998 de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación

[295] Entendemos por éste, todos los componentes del ordenador en sí.
[296] Es el programa informático que da todas las ordenes de funcionamiento al ordenador.
[297] BOE 147 de 26.6.1994.

y cancelación[298]. Ambos fueron promulgados bajo la vigencia de la LORTAD, pero en virtud de la disposición transitoria tercera de la LOPD, se encuentran vigentes.

La primera aclaración que, sobre estos derechos debemos realizar, es que se trata de derechos personalísimos, es decir, que sólo pueden ser ejercitados por el titular del derecho, salvo que se encuentre en situación legal de incapacidad o minoría de edad, en cuyo caso podrán ser ejercitados por su representante legal. No obstante, la APD en su Memoria de 2001, página 311, se manifestó favorable a que pueda ejercerse el derecho por parte de una persona distinta del titular, siempre que exista un poder o mandato, que no podrá ser genérico, sino que debe referirse concretamente al ejercicio de uno de esos derechos.

Al estar considerados como derechos independientes, se entiende que es el titular el que elige cual ejercita, no estando subordinado el ejercicio de alguno de estos, al ejercicio anterior de ninguno de los mismos. Para poder ser ejercitado deberá remitirse al responsable del fichero una comunicación que debe contener los siguientes extremos: nombre y apellidos del interesado y fotocopia de su DNI (o cualquier otro medio que acredite la identidad, que sea válido en derecho). Si se trata de representante legal deberá adjuntarse igualmente su fotocopia del DNI y copia del documento acreditativo de la representación. Deberá igualmente incluirse la petición en la que se concreta la solicitud, designar un domicilio a efectos de notificaciones, fecha y firma del solicitante y en su caso, documentos en los que se acredita la solicitud. El método de envío de la solicitud deberá acreditar el envío y la recepción.

El responsable del fichero viene obligado a cursar la solicitud, aunque no posea datos de carácter personal del solicitante, debiendo utilizar de la misma manera un método que acredite el envío y la recepción.

Entrando a analizar el primero de estos derechos, definiremos el derecho de acceso como aquel por el cual el interesado tiene derecho a solicitar y a obtener información gratuita de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones que se han realizado o se prevén realizar de los mismos. Solicitado el acceso, el responsable tiene el plazo de un mes para cursarlo y el de 10 días para materializarlo en caso de que la solicitud resulte aceptada. El interesado no podrá ejercitar este derecho en espacios inferiores a 12 meses, salvo que se acredite un interés legítimo. El ejercicio del derecho se dará por cumplido si se proporciona información legible e inteligible por alguno de los siguientes medios: visualización en pantalla, escrito, copia o fotocopia remitida por correo, telecopia o cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

[298] BOE 25 de 29.1.1998.

En lo que respecta a la rectificación o cancelación de datos, se dispone que deberá procederse a ejecutar estos derechos cuando el tratamiento de datos no se ajuste a lo establecido en la LOPD, cuando los datos resulten inexactos o incompletos, o sean inadecuados o excesivos para la finalidad para la que se obtuvieron.

En caso de producirse la cancelación de los datos, se producirá el bloqueo de estos datos[299], conservándose únicamente por si fueran requeridos por las Administraciones Públicas, Jueces y Tribunales, para la atención de posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. También deberán mantenerse durante los plazos que indiquen las disposiciones aplicables, o en su caso, las relaciones contractuales. Una vez finalizado el plazo de procederá a su supresión. Esta disposición lo que quiere decir es que por ejemplo, ante la solicitud de cancelación de datos por parte del afectado, los datos deberán de salir del tratamiento del que eran objeto, pero si el responsable de tratamiento tiene la obligación legal de guardar la factura de la operación por cuatro años o, mantener los datos durante el periodo de prescripción de acciones, ya sean reales (5 años) o personales (15 años), estos datos deberán mantenerse, aunque no tratarse.

Además, si los datos cuya rectificación o cancelación se solicita, hubieran sido comunicados a terceros, el responsable del fichero viene obligado a comunicarles la rectificación o cancelación de los datos, viniendo el tercero obligado de la misma manera a proceder a tal rectificación o modificación.

El plazo establecido para cursar la solicitud, es de 5 días desde su recepción.

Si el responsable del tratamiento no atiende a la solicitud cursada por el afectado, sobre cualquiera de estos derechos, al que añadiremos el de oposición que fue estudiado en su momento, podrá solicitar amparo ante la APD u organismo autonómico competente, que deberá resolver sobre la procedencia o improcedencia de la denegación de la solicitud en el plazo de 6 meses. Iniciado el procedimiento de tutela, la APD entiende que no cabe el sobreseimiento del asunto por renuncia del titular, amparándose en el artículo 18.1 del R-D. 1332/1994, que dispone que el procedimiento sancionador se inicia de oficio. Es por ello que aunque se produzca la renuncia, si la APD observa una posible vulneración de la LOPD continuará con el expediente[300].

Continuando con los derechos de las personas, pasamos a continuación a estudiar el derecho de impugnación de valoraciones. En virtud de este derecho, los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. De la misma manera, podrán impugnar los actos administrativos o

[299] El Reglamento LORTAD lo define como la identificación y reserva de datos para impedir su tratamiento.
[300] Véase Memoria APD de 2000, página 280.

decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fin sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad, teniendo derecho a obtener del responsable del fichero información sobre los criterios de valoración y el programa utilizado a tales efectos. En este supuesto, pueden plantearse dudas si en el tratamiento de datos personales, se utiliza la actividad de almacenamiento de datos o *datawarehousing*. En virtud de esta actividad, el responsable del fichero almacena todo tipo de información relativa a una persona, incluso la que en principio no es relevante para el uso y finalidad del tratamiento, para después emitir las correspondiente conclusiones de perfil psicológico y sociológico del afectado. De acuerdo con Aparicio Salom[301], esta actividad será legal siempre que los datos obtenidos sean destinados a mejorar o innovar el servicio o producto contratado con el afectado, estando el resto de las posibilidades de uso de esta información (inclusive las de ofertar otros productos o servicios por parte del mismo responsable del fichero) fuera del marco legal de la LOPD.

Para poder facilitar el ejercicio de todos estos derechos, se dispone en el artículo 14 de la LOPD un procedimiento de consulta público y gratuito ante el Registro General de Protección de Datos, que verse sobre la existencia de tratamientos de datos personales, sus finalidades y la identidad del responsable del fichero.

El último derecho reconocido a las personas, es el derecho de indemnización. En virtud de éste, los interesados que a consecuencia de incumplimientos de las disposiciones de la LOPD, por parte del responsable o del encargado del tratamiento, sufran daño o lesión en sus bienes y derechos, tendrán derecho a solicitar una indemnización. Esta indemnización deberá solicitarse ante la jurisdicción ordinaria, en caso de tratarse de ficheros de titularidad privada, o de acuerdo con la legislación reguladora de la responsabilidad de las Administraciones Públicas, en el caso de que nos encontremos ante un fichero de titularidad pública. La indemnización, al no disponer la ley otra cosa, vendrá determinada por la responsabilidad que establece nuestro derecho. En caso de que entre el afectado y el responsable o encargado de tratamiento medie una relación contractual, la responsabilidad se entenderá contractual. En el caso de que no exista tal relación, la indemnización traerá causa de la responsabilidad extracontraltual o Aquiliana, del artículo 1902 del Código Civil.

E) Naturaleza y Obligaciones respecto de los ficheros.

En primer lugar debemos distinguir dos tipos de ficheros, según la catalogación efectuada por la LOPD. Los ficheros pueden ser de titularidad pública o privada. Ambos se encuentran regulados en la LOPD y el R.D. 1332/1994, aunque hay que señalar que para los ficheros de titularidad pública puede crearse por ley un

[301] Ob. Cit, páginas 85 y ss.

organismo autonómico equivalente a la APD, y regular legalmente los aspectos que afecten a este tipo de ficheros. En este sentido, en la Comunidad Autónoma de Madrid, se ha promulgado la Ley 8/2001 de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid[302], cuyo ámbito se extiende a todas las Administraciones e Instituciones de la Comunidad, a todas las Corporaciones Locales de la Comunidad y a los entes que representen los intereses económicos y profesionales en ese ámbito. Otras legislaciones de ámbito autonómico son el Decreto 67/2003 de 22 de mayo, por el que se aprueba el reglamento de desarrollo de la APD de la Comunidad Autónoma de Madrid de tutela de los derechos y de control de los ficheros de datos de carácter personal, la Ley 5/2002 de 19 de abril, de la Agencia Catalana de Protección de Datos, el Decreto 48/2003 de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, o el Decreto 53/2002 de 23 de abril, de Protección de Datos de Carácter Personal en la Junta de Comunidades de Castilla La Mancha.

En lo que respecta a los de titularidad pública, sólo mencionaremos que en la LOPD se recogen una serie de especialidades en lo que atañe al ejercicio de los derechos de acceso, rectificación y cancelación y se establece un supuesto especial para los ficheros creados por las Fuerzas y Cuerpos de Seguridad, que se ve completado por la Orden INT/1751/2002 de 20 de junio, por el que se regulan los ficheros informáticos de la Dirección General de la Policía, que contienen datos de carácter personal.

Los ficheros de las Administraciones Públicas deben notificarse, cancelarse o modificarse ante el organismo autonómico equivalente a la APD, aunque se inscribirán en el Registro General de Protección de Datos, que depende de la APD.

Centrándonos a continuación en los ficheros de titularidad privada, mencionaremos que podrán crearse este tipo de ficheros cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular, siempre que se respeten las garantías que esta ley establece para la protección de las personas.

Previamente a la creación del fichero, el responsable del mismo deberá notificar a la APD la próxima existencia del mismo, así como notificar las modificaciones o cancelación del mismo. Los términos en los que debe basarse la notificación se encuentran recogidos en el R.D. 1332/1994 y a éste nos remitimos, aunque mencionaremos que en virtud de esa disposición, la APD ha elaborado un modelo de Formulario único, para las notificaciones, modificaciones y cancelaciones del fichero[303]. Si la notificación se ajusta a las disposiciones legales se inscribirá de oficio en el Registro General de Protección de Datos. En caso contrario, la APD podrá solicitar que los datos se subsanen o completen en el plazo de 10 días. El

[302] BOE 245 de 12.10.2001.

[303] Puede obtenerse el Formulario o presentarse directamente a través de Internet, a través de la página Web de la APD: www.agenciaprotecciondatos.org .

incumplimiento de este requerimiento dejará sin efectos la notificación. En el supuesto de que transcurra un mes desde la solicitud de la inscripción sin que la APD resuelva sobre la misma, se entenderá inscrito el fichero a todos los efectos. La notificación según se desprende de la ley, tiene un efecto declarativo y no constitutivo, y así lo entiende la APD en su Memoria de 2000, página 30. De hecho la APD se permite recordar en las resoluciones de inscripción de ficheros, que con ese trámite se cumple con la obligación de notificación del artículo 26.1, y se evitan las sanciones previstas por su incumplimiento, pero no exime del cumplimiento del resto de obligaciones que impone la LOPD.

Un problema práctico con el que pretendemos terminar el apartado referente a la notificación, es el de la creación, modificación o cancelación de ficheros dentro de un grupo de empresas, unión temporal de empresas, o en casos de fusión, absorción o excisión de empresas. La APD ha emitido ya su opinión sobre el asunto en su memoria del 2000, página 40, entendiendo que cada una constituye una persona jurídica independiente, y en los casos de fusión o absorción existe una perdida de personalidad jurídica de las empresas anteriores, en beneficio de la obtención de la personalidad jurídica a la resultante. Esta interpretación deberá ser tenida en cuenta no sólo en lo que respecta a la notificación, modificación y cancelación de ficheros, sino que deberá tomarse en consideración a la hora de aplicar otras disposiciones de la LOPD, como las que respectan a la cesión de datos.

Pasando a continuación a estudiar las especialidades que plantean los datos incluidos en fuentes accesibles al público, indicaremos que entendemos por fuente accesible al público, según el artículo 3 j), a aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de 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. Si el formato de esta fuente consiste en la edición en forma de libro o algún otro soporte físico, perderán la condición de fuente accesible cuando se publique una nueva edición. Si la copia de la lista se ha obtenido por vía telemática en formato de correo electrónico, perderá el carácter de fuente accesible en el plazo de un año, a contar desde la fecha de su obtención. En el supuesto del censo promocional, perderá tal carácter transcurrido un año desde que comenzó su utilización.

Lo primero que queremos mencionar de este tipo de datos, es que a tenor de la definición aportada, nos estamos moviendo en una categoría de *numerus clausus*, sólo los supuestos mencionados tienen tal catalogación. De los supuestos recogidos

como fuentes accesibles, el que más problemas prácticos ha originado es el censo promocional. Éste se encuentra definido en la LOPD como: "el formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral". La problemática suscitada con esta fuente radica en que muchos responsables de ficheros utilizaron para fines de publicidad y prospección comercial los datos recogidos en el censo electoral, concepto mucho más amplio que el censo promocional, y por ende no catalogado como fuente accesible al público. Esta misma postura ha sido la mantenida por el Tribunal Supremo en sus sentencias de 23 de septiembre de 2002 y 18 de octubre de 2000.

Los datos de carácter personal que conten en el censo promocional y en las listas de personas pertenecientes a grupos profesionales, para que sean considerados como fuente accesible al público, deberán ser los estrictamente necesarios para cumplir con la finalidad a la que se destina cada listado. Cualquier extralimitación en cuanto a la inclusión de datos adicionales, requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

Para los listados de Colegios Profesionales, se añade una especialidad, que consiste en la comunicación, por parte del responsable del fichero, que los datos de un interesado no pueden utilizarse con fines de publicidad o prospección comercial. En caso de que el interesado ejecute este derecho, se establece que se realizará de manera gratuita.

Si por el contrario, los datos a los que nos referimos están incluidos en el censo promocional, los interesados podrán solicitar gratuitamente la exclusión de la totalidad de sus datos personales. Si se produce una solicitud de exclusión de la información innecesaria o de la inclusión en la objeción de Venta a Distancia, ésta deberá realizarse en el plazo de diez días si la información se consulta o comunica por vía telemática o en la siguiente edición del listado, cualquiera que sea el soporte en el que se edite.

Directamente relacionado con las fuentes accesibles al público se encuentran las dos actividades que estudiaremos a continuación, que son la prestación de información sobre solvencia patrimonial y crédito y el tratamiento con fines de publicidad y prospección comercial.

Comenzando por la primera actividad, indicaremos que para que ésta sea válida, los datos tratados deberán haber sido obtenidos de los registros[304] y las fuentes accesibles al público establecidos al efecto[305] o procedentes de informaciones facilitadas por el interesado o con su consentimiento. El tratamiento de datos de carácter personal sobre el cumplimiento o incumplimiento de obligaciones

[304] Tradicionalmente se acude al Registro Mercantil y a los registros de la propiedad de bienes,

[305] Suele acudirse con frecuencia a los periódicos oficiales, los cuales publican información, actos o disposiciones, sobre la solvencia de las personas.

dinerarias, facilitado por el acreedor o por quien actúe por su cuenta e interés, es igualmente legal. Para ello será necesario que se informe a los afectados en el plazo máximo de treinta días desde su inclusión en el fichero, informándoles de la posibilidad de recabar información sobre el tratamiento, en los términos previstos por la LOPD. Esta información consistirá en la comunicación de los datos, las evaluaciones y apreciaciones que sobre el interesado hayan sido comunicadas durante los últimos seis meses y el nombre y la dirección de la persona o entidad a quien se hayan revelado los datos.

El registro y cesión serán válidos, si no se refieren, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos.

Teniendo en cuenta que el responsable del fichero únicamente realiza una anotación en el fichero con arreglo a las instrucciones que le da el acreedor, es éste segundo el obligado a cumplir con el principio de calidad de los datos, debiendo comunicar al responsable los cambios en la situación del deudor, y en especial la del pago. El pago constituye la obligación por parte del acreedor de comunicar al responsable del tratamiento esta circunstancia, de modo que éste último pueda cancelar los datos del deudor, ya que la APD no acepta el mantenimiento de los datos bajo el apunte de saldo 0, y para ello se basa en el deber de que los datos respondan con veracidad a la situación actual del afectado[306].

Un supuesto de especialidad en cuanto a los ficheros de morosos, se encuentra recogido en la ya mencionada Ley 44/2002 de Medidas de Reforma del Sistema Financiero. En los artículos 59 y siguientes, se define y regula la Central de Información de Riesgos (CIR), que es un servicio público gestionado y administrado por el Banco de España, que tiene por finalidad recabar de las entidades declarantes (las recogidas en el artículo 60.1), datos e informaciones sobre los riesgos del crédito. Y decimos que se plantea especialidad ya que en primer lugar los afectados por el tratamiento no podrán oponerse al mismo, y las entidades declarantes vienen obligadas a facilitar a la CIR los datos necesarios para identificar a las personas con quienes mantengan, directa o indirectamente, riesgos de crédito, que son la posibilidad de que la entidad declarante pueda sufrir una pérdida como consecuencia de un incumplimiento de alguna de las obligaciones de sus contrapartes o de los garantes de éstas, en contratos tales como, préstamos, créditos, descuentos emisiones de valores, contratos de garantía, etc. Otra especialidad es que para la declaración de los datos a la CIR, no se precisa del consentimiento del afectado y quedan autorizadas las cesiones de datos sin consentimiento del afectado para determinados supuestos. En todo caso, debido a la multitud de especialidades reguladas en esta ley (los datos serán guardados durante 10 años, por poner otro ejemplo), nos remitimos a la Ley 44/2002 dejando constancia de la misma.

[306] Véase Memoria de la APD de 2000.

Pasando a continuación a detallar la segunda actividad, mencionaremos que, para que las actividades de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, sean legales, los datos de carácter personal recopilados deberán constar en fuentes accesibles al público o haber sido facilitados por los propios interesados u obtenidos con su consentimiento.

Como ya vimos en su momento, 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 los derechos que le asisten (en particular el derecho a conocer el origen de los datos, sí ejercita el derecho de acceso).

Los interesados, podrán en estos supuestos, oponerse al tratamiento de sus datos. Para ello bastará con la remisión de una solicitud, sin gastos, al responsable instando la cancelación de datos, que en estos supuestos se producirá en el acto.

Para finalizar el apartado correspondiente a los ficheros de titularidad privada, mencionaremos la posibilidad de crear Códigos Tipo, mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, por parte de los responsables de tratamiento de ficheros de titularidad pública o privada y de las organizaciones en que se agrupen. Los Códigos tipo tendrán el carácter de código deontológico o de buena practica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos.

En dichos Códigos se podrán establecer las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad en el entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo. De igual forma, podrán contener o no, reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

Los Códigos tipo inscritos en el Registro General de Protección de Datos, a fecha 20 de marzo de 2003, son los siguientes:

- Código Tipo de Telefónica, de Telefónica de España S.A.
- Código Tipo del Fichero Histórico de Seguros del Automóvil, de UNESPA.
- Código Ético del Sector de Información Comercial, de la Asociación Multisectorial de la Información.
- Código Ético de Protección de Datos Personales informatizados en empresas y despachos profesionales, de la Asociación Nacional de Fabricantes.
- Código Tipo de UCH, de la Unión Catalana de Hospitales.
- Código Tipo de ACES, de la Asociación Catalana de Establecimientos Sanitarios.

- Código Ético de Comercio Electrónico y Publicidad Interactiva, de Confianza Online.

F) Movimiento Internacional de Datos.

Las transferencias internacionales de datos, son posiblemente, la especialidad en protección de datos que más cautelas han propiciado en la LOPD y en la Directiva 1995/46/CE, siempre que vayan dirigidas a terceros Estados que necesariamente no tienen por que disponer de un sistema de protección de datos de carácter personal tan avanzado y protector, como el dispuesto para los E.E.M.M. de la U.E. .

El principio general en esta materia, es la prohibición de transferencias internacionales de datos, ya sean temporales o definitivas, de datos de carácter personal que hayan sido objeto de tratamiento, o vayan a serlo, con destino a países que no proporcionen un nivel de protección equiparable al establecido en la LOPD, salvo que medie autorización previa del Director de la Agencia de Protección de Datos, cuando observe que se ofrecen las garantías adecuadas[307]. Los parámetros que deben inspirar a la APD a la hora de autorizar la transferencia en base a sí el país de destino ofrece un nivel adecuado de protección, o no, son todos aquellos que intervienen en la transferencia, y en particular la naturaleza de los datos, la finalidad y la duración del tratamiento, el país de origen y el de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país de destino, el contenido de los informes de la Comisión Europea y las medidas de seguridad en vigor en dichos países.

Planteado el principio general, debemos irlo matizando, en atención a las excepciones a este principio que se regulan en la LOPD.

La primera excepción que recoge la LOPD, a tenor de la Directiva 1995/46/CE, es la libre circulación de datos entre E.E.M.M. de la U.E., es decir, no se requiere autorización para transferir datos a estos países, ya que han adoptado una legislación que tiene la misma raíz que la LOPD. Baste decir que en el caso de que la LOPD hubiera dispuesto el principio contrario, se habría producido un incumplimiento del Derecho comunitario. También en consonancia con la normativa comunitaria, se podrán efectuar estas transferencias a terceros países sin necesidad de autorización previa, cuando la Comisión Europea declare que el país en cuestión dispone de un nivel adecuado de protección[308].

El resto de excepciones al principio de autorización previa son:

[307] En virtud de esta habilitación, la APD ha dictado la Instrucción 1/2000 de 1 de diciembre, de la Agencia de Protección de Datos, sobre las normas que rigen los movimientos internacionales de datos. BOE 301 de 16.12.2000.

[308] La lista de países sobre los que ha recaído una resolución favorable, ya fue vista en el apartado correspondiente a la protección de datos del capítulo primero.

- Cuando la transferencia internacional resulte de la aplicación de Tratados o Convenios de los que España sea parte.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento específico a la transferencia prevista.
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero, o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del afectado, por el responsable del fichero y un tercero.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración Fiscal o Aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquella sea acorde con la finalidad del mismo.
- Por su parte, la disposición final primera del R.D. 1332/1994, faculta al Ministro de Justicia a que, previo informe del Director de la APD, apruebe la lista de países que se consideren que proporcionan un nivel adecuado de protección. Como consecuencia de esta habilitación, se han publicado dos normas: La Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995[309] por la que se aprueba la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos y la Orden del Ministerio de Justicia de 31 de julio de 1998[310] por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencias internacionales de datos.

G) Infracciones y Sanciones.

Como en cualquier ley en la que se establecen derechos y obligaciones para las partes, la LOPD establece una serie de sanciones para disuadir a los responsables y

[309] BOE 35 de 10.2.1995
[310] BOE 200 de 21.8.1998.

encargados del tratamiento, de las tentaciones de actuar en contra de lo establecido legalmente.

Las infracciones se clasifican en leves, graves y muy graves, estando tasados los supuestos de cada tipo de infracción, atendiendo a la naturaleza de la misma.

Son infracciones leves:

- No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
- No proporcionar la información que solicita la APD en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con los aspectos no sustantivos de la protección de datos.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente ley.
- Incumplir el deber de secreto establecido en el artículo 10 de esta ley, salvo que constituya infracción grave.

Son infracciones graves:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el BOE o diario oficial correspondiente.
- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de 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.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan, cuando resulten afectados los derechos de las personas que la presente ley ampara.
- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de

infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad el individuo.

- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- No remitir a la APD las notificaciones previstas en esta ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.
- La obstrucción al ejercicio de la función inspectora.
- No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la APD.
- Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta ley, cuando los datos hayan sido recabados de persona distinta del interesado.

Son infracciones muy graves:

- La recogida de datos en forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7, cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7, cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en al apartado 4 del artículo 7.
- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la APD o por las personas titulares del derecho de acceso.
- La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcione un nivel de protección equiparable sin autorización del Director de la APD.
- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Las sanciones establecidas por la LOPD son de 601,01 euros a 60.101,21 euros para las leves, de 60.101,21 euros a 300.506,05 euros para las graves y, de 300.506,05 euros a 601.012,10 euros para las muy graves. Esta cuantía podrá ser actualizada periódicamente por el Gobierno, de acuerdo con las variaciones experimentadas en los índices de precios. La horquilla de sanciones, a nuestro juicio no se encuentra bien creada, sobre todo en lo que respecta a las sanciones leves. Debería no haberse introducido un límite mínimo de sanción, ya que para un profesional autónomo o para una PYME, una sanción mínima de 601,01 euros por no haber inscrito su fichero en la Agencia de protección de Datos, nos parece desproporcionada y en muchos casos podría originar un cierre de actividad.

Para establecer la sanción concreta, dentro de la horquilla que establece la LOPD, se atenderá a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y culpabilidad presentes en la concreta actuación infractora. En caso de que el órgano sancionador aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, aplicará una sanción en la escala de sanciones anterior a la infracción cometida, pero bajo ningún concepto podrá aplicarse el principio contrario, es decir sancionar según la escala posterior a la infracción cometida.

Para los supuestos de infracciones muy graves, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la APD podrá además requerir a los responsables de tratamiento, la cesación en la utilización o cesión ilícita de datos. En caso de que este requerimiento no sea atendido, la APD podrá por medio de resolución motivada inmovilizar los ficheros con el único fin de restaurar los derechos de los afectados.

También se establece otra especialidad cuando se produzca una infracción muy grave, y el responsable del fichero sea una Administración Pública. En este supuesto, el Director de la APD dictará una resolución en la que se recojan las medidas a adoptar con el fin de que cesen o se corrijan los efectos de la infracción. La resolución deberá ser notificada, a parte de al órgano infractor, a su superior jerárquico y a los afectados, si los hubiera. Se podrán establecer igualmente por parte del Director de la APD, la iniciación de actuaciones disciplinarias, que serán

resueltas por la legislación específica del régimen disciplinario de las Administraciones Públicas. Para finalizar con este supuesto indicaremos que se establece que el Director de la APD viene obligado a notificar al Defensor del Pueblo, todo lo que acontezca, en relación con lo expresado en líneas anteriores.

En lo que respecta a la prescripción de las infracciones, debemos estar a lo dispuesto en el artículo 47.1 que dispone que, las infracciones muy graves prescribirán a los tres años, las graves lo harán a los dos y las leves lo harán pasado un año. Los mismos periodos se establecen para la prescripción de las sanciones. Este plazo comenzará a computarse desde el día en el que se hubiera cometido la infracción, o desde el día siguiente a aquel en que la resolución que impone la sanción obtenga el carácter de firmeza. Pero como en todo trámite administrativo, la iniciación del procedimiento sancionador, con conocimiento del interesado, interrumpirá estos plazos. No obstante, si el expediente estuviera paralizado durante más de 6 meses por causas no imputables al presunto infractor, se reanudará este plazo. Si se trata de una sanción, la prescripción la interrumpirá la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a correr el plazo si este procedimiento se encuentra paralizado durante más de 6 meses, por causa no imputable al infractor.

El procedimiento sancionador, al que antes nos referíamos, se encuentra regulado en el R.D. 1332/1994. En virtud de éste, se inicia siempre de oficio por acuerdo del Director de la APD, ya sea por propia iniciativa de la APD o bien por denuncia del afectado o afectados. Este procedimiento se configura como un procedimiento sancionador administrativo tipo, y sus pasos se encuentran minuciosamente regulados en el artículo 18 y 19 del R.D.. Añadiremos que para todo lo no previsto en estos artículos, regirá el procedimiento general del ejercicio de la potestad sancionadora previsto en el R.D. 1398/1993 de 4 de agosto, que regula el Procedimiento para el Ejercicio de la Potestad Sancionadora, en desarrollo de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

H) Un supuesto especial: La Ley General de Telecomunicaciones.

Como hemos tenido ocasión de comprobar en líneas anteriores, los servicios de guías de telecomunicaciones, como fuente accesible a público, se rigen por su propia normativa. Es por ello que vamos a dar algunas pinceladas sobre esta Ley.

En primer lugar, la Ley trae causa de la necesidad de transponer la Directiva 2002/58/CE y del resto de Directivas que forman el paquete Telecom, que estudiamos en su momento. Es por ello que una primera parte del Capitulo III, que es el que nos afecta, se dedica al secreto de las comunicaciones, permitiendo entre otras cosas su cifrado.

Pero como mencionaba anteriormente, lo que realmente nos interesa es la regulación en lo que respecta a la protección de datos de carácter personal. De acuerdo con esta normativa, abonados disponen de los siguientes derechos:

- Derecho a la cancelación de sus datos de trafico, o a que se hagan anónimos, cuando dejen de ser necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios para la facturación, no podrán ser tratados cuando haya expirado el plazo para la impugnación de la factura telefónica o para que el operador pueda exigir su pago.
- Derecho a que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.
- A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos del tráfico, cuando se hallan hecho anónimos o previo consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.
- Derecho a no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.
- La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías y el de suministrar la información que consta en estas, por parte del operador de comunicaciones, conforme a la normativa sobre protección de datos de carácter personal vigente en cada momento. En la actualidad estas se encuentran reguladas en la Orden CTE/711/2002 de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.

Para finalizar este epígrafe y el capítulo, mencionaré un supuesto que aunque no se refiere a la protección de datos, si tiene que ver con la confidencialidad de las comunicaciones electrónicas, y que no es otro que el uso del correo electrónico con fines particulares por parte de los trabajadores de una empresa en horario laboral, y si sobre estos supuestos el empresario tiene, o no, una potestad de control y sanción.

Mencionaremos que en estos supuestos la doctrina y la jurisprudencia se encuentran divididos, entre ellos y entre sí, ya que los primeros se inclinan por la primacía de los derechos fundamentales, en particular el derecho a la intimidad, los segundos han optado por considerarlo como un fraude contractual y por ello calificarlo como causa de despido. Alegan además que no se vulnera el secreto de

las comunicaciones ya que los posibles espionajes se realizan sobre materiales propiedad del empleador. En este sentido cabe citar las sentencias de los Tribunales Superiores de Justicia de Cataluña (5-7-2000), País Vasco (31-10-2000), Galicia (4-10-2001) y Madrid (4-12-2001). Como pronunciamiento en contra cabe citar las sentencias de los Tribunales Superiores de Justicia de Andalucía (25-2-2002) y Madrid (31-2-2002), por lo que nos atrevemos a aventurar a la vista de lo poco pacificada que está esta disciplina, que veremos continuamente polémicas y decisiones encontradas sobre la calificación de este supuesto.[311]

[311] Para más información, véase ABC Tecnología, de 2.10.2002, página 44.

IV) Propiedad Intelectual.

A continuación, nos disponemos a destacar algunos problemas que se suscitan con la PI, en lo que respecta a las TIC, en particular los programas de ordenador, las bases de datos, el derecho de comunicación pública y el derecho de distribución. Para ello es necesario que demos, al menos, algunas pinceladas sin ánimo de exhaustividad, sobre la normativa general aplicable a la PI, que nos permita centrar, identificar y comprender los problemas a los que nos referíamos anteriormente.

La norma en vigor en esta materia, es el Real Decreto Legislativo 1/1996 de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia[312], en adelante TRPI. Este texto refundido basa su validez en la Disposición final segunda de la Ley 27/1995 de 11 de octubre, de incorporación al derecho español de la Directiva 93/98/CEE, en la que se habilitaba al Gobierno para que antes del 30 de junio de 1996 aprobara un texto que refundiese las disposiciones legales vigentes. Y es que en esa fecha, no sólo contábamos con la Ley 22/1987 de 11 de noviembre de propiedad intelectual (ya derogada), sino con multitud de leyes que transponían al derecho español las Directivas Comunitarias, que como se vio en el capítulo primero, fueron aprobadas en el ámbito de la PI. Posteriormente se ha incorporado al derecho español la Directiva 96/9/CE sobre protección jurídica de bases de datos, a través de la Ley 5/1998 de 6 de marzo, pero las reformas operadas en esta ley, se han incorporado al TRPI.

A) Principios Comunes de la PI.

No podemos comenzar nuestra exposición, sin indicar que la PI de una obra literaria, artística o científica corresponde al autor, por el sólo hecho de su creación. Con esto lo que se pretende dejar claro, es que no se requiere registrar una obra previamente, para el nacimiento de estos derechos. No obstante en nuestro derecho es posible registrar una obra, cuestión que abordaremos más adelante.

Pero podemos preguntarnos que creaciones son susceptibles de protección bajo el derecho de PI. De acuerdo con el artículo 10 del TRPI son objeto de protección todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en un futuro, comprendiéndose entre ellas:

[312] BOE de 24 de abril de 1996.

- Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza.
- Las composiciones musicales, con o sin letra.
- Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales.
- Las obras cinematográficas y cualesquiera otras obras audiovisuales.
- Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o comics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas.
- Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.
- Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia.
- Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía.
- Los programas de ordenador.

Los derechos sobre la PI se dividen en personales o morales, y patrimoniales. Los primeros atribuyen al autor un derecho de disposición sobre la creación, y los segundos confieren el derecho de explotación. Los morales, son derechos de naturaleza irrenunciable e inalienable. Se encuentran recogidos en el artículo 14 del TRPI, y son los siguientes:

- Decidir si la obra ha de ser divulgada y en que forma[313].
- Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente.
- Exigir el reconocimiento de su condición de autor de la obra.
- Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos interesas o menoscabo de su reputación.
- Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural.
- Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de los derechos de explotación.
- Acceder al ejemplar único o raro de la obra, cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.

[313] Atendiendo al artículo 4, se considera divulgación de la obra: toda expresión de la misma que, con el consentimiento del autor, la haga accesible por primera vez al público en cualquier forma. Este artículo l diferencia de la publicación, entendiendo por ésta, la divulgación que se realice mediante la puesta a disposición del público de un número de ejemplares de la obra que satisfaga razonablemente sus necesidades estimadas de acuerdo con la naturaleza y finalidad de la misma.

Por su parte, los patrimoniales, se recogen en el derecho exclusivo de explotación, y de sus modalidades. Estos derechos corresponden en exclusiva al autor, y no podrán ser realizados sin su autorización, salvo en los casos expresamente previstos por la ley. Los derechos duran, como regla general, durante toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento. Estas formas de explotación son las siguientes:

- Reproducción: es la fijación de la obra en un medio que permita su comunicación y la obtención, en todo o en parte, de copias de ella.
- Distribución: es la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma.
- Comunicación pública: todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas. A estos efectos no se entenderá que es pública, cuando se realice dentro de un ámbito estrictamente doméstico[314] que no esté integrado o conectado a una red de difusión de cualquier tipo. Un listado con algunos de los actos que se consideran comunicación pública, se encuentra recogido en el artículo 20. En todo caso, debemos mencionar que entendemos que es un listado bajo la catalogación de numerus apertus.
- Transformación: comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente. Los derechos de PI sobre la nueva obra, corresponderán al autor de la transformación, sin perjuicios de los derechos del autor de la obra preexistente de autorizar durante todo el plazo de protección de sus derechos sobre ésta, la explotación de esos resultados en cualquier forma y en especial, mediante su reproducción distribución, comunicación pública o nueva transformación.

La principal excepción a estos derechos, es la recogida en el artículo 31.2, en virtud del cual, para uso privado del copista y siempre que la copia no sea objeto de utilización colectiva o lucrativa, podrán realizarse copias privadas sin autorización del autor, si la obra ha sido previamente divulgada. No obstante, el artículo 25 establece un derecho a la remuneración por copia privada, o lo que es lo mismo, establece un canon, sobre los aparatos que hacen posible la reproducción (por ejemplo una fotocopiadora) o sobre los materiales en los que se realiza (por ejemplo un CD, entendiendo a estos en su sentido más amplio, ya que a tenor de la Sentencia del Juzgado de Primera Instancia 22 de Barcelona de 2 de enero de 2002, a tenor de la aplicación del canon previsto en el TRPI a los CDR informáticos, cuando existen CDR Audio. Entiende el juzgado que aunque el CDR informático está pensado para programas informáticos, son idóneos para reproducir música, por lo que deben estar grabados por el mencionado canon). Están excluidos de este canon los programas de ordenador que veremos más adelante.

[314] Por ámbito doméstico, como bien señala Rodríguez Pardo debe entenderse comunicación cara a cara o bis a bis, salvando de esta manera las comunicaciones privadas que se realizan por redes públicas como por ejemplo el envío de correos electrónicos.

Los derechos de explotación podrán ser transmitidos, como cualquier derecho, por procedimientos Inter. vivos o mortis causa.. Los segundos no plantean ninguna especialidad en cuanto a nuestro derecho, ya que serán los designados por el autor en su última voluntad, o en su defecto los herederos legales. Para los supuestos de transmisión inter vivos se establece la obligación de indicar la modalidad de explotación cedida, la duración y el ámbito territorial. La falta de mención de las últimas las circunscribe a 5 años y al país en el que se realiza la cesión. En todo caso la cesión deberá contar por escrito. En el caso de que sea realizada a título oneroso, otorgará un derecho a remuneración al autor, por los beneficios derivados de la explotación de la obra. Únicamente en los supuestos contemplados por la ley, se podrá pactar una remuneración a tanto alzado. Para finalizar la cesión de derechos de explotación, indicaremos que la cesión puede realizarse en exclusiva o en no exclusiva. La primera se utilizará principalmente cuando se trate de contratos entre el autor y una empresa que los comercialice (editorial, discográfica, productora), y los segundos pueden ser muy útiles para una empresa que diseñe programas de ordenador o bases de datos.

El TRPI confiere en consonancia con la legislación internacional en la materia, una serie de derechos, que podríamos denominar conexos, u otros derechos sobre la PI, entre los que se encuentran los artistas interpretes o ejecutantes, los productores de fonogramas, los productores de las grabaciones audiovisuales, derechos de las entidades de radiodifusión, derechos de los que queremos dejar constancia de su existencia.

Finalizaremos el epígrafe como lo comenzamos, para el reconocimiento del derecho del autor, no será necesario que sea registrado previamente. No obstante, como el TRPI prevé la creación de un registro de PI en sus artículos 144 y 145, el Gobierno ha ejercitado recientemente la habilitación reglamentaria, promulgando el Real decreto 281/2003, de 7 de marzo, por el que se aprueba el Reglamento del Registro General de la Propiedad Intelectual[315]. Este R.D. reforma en primer lugar el reglamento sobre el Registro, cuestión en la que no vamos a entrar. Lo único que nos interesa para esta materia, es la reforma operada en lo que respecta al registro de páginas electrónicas (páginas Web) o multimedia[316]. Anteriormente si se quería registrar una Web, se debía realizar inscribiendo cada uno de sus elementos por separado de acuerdo con el sistema que correspondiese, es decir, el texto como obra literaria, los sonidos como obra musical, las fotografías como tales..., y tras la reforma, es posible registrarla como entidad propia. No obstante, sigue manteniéndose uno de los inconvenientes mayores, que desincentivan su registro,

[315] BOE de 28.3.2003.

[316] Para Rodríguez Pardo, multimedia es la creación resultante de la conjunción de textos, imágenes fijas o en movimiento, sonidos y gráficos, por medio de la Tecnología digital, fijada en un soporte informático y dotada de un mayor o menor grado de interactividad. Pueden ser off line, como programas de ordenador, CD-ROM, CD-I o bases de datos, o obras multimedia on line, como las bases de datos y páginas Web. Para más información véase Rodríguez Pardo Julián: El derecho de Autor en la Obra Multimedia. Páginas 32 a 34.

las páginas Web son un elemento dinámico, cambian diariamente o incluso varias veces al día, por lo que habría que estar registrando las modificaciones constantemente. Al menos en algo hemos avanzado, ya que por lo menos podemos registrar las Web cuando nos interesen registrar determinados contenidos. El último problema a destacar es que el R.D. no define que es página Web, ni tampoco lo hace el TRPI, por lo que surgirán problemas a la hora de delimitar dónde se encuadra su protección. Con el sistema anterior se podía acudir a la protección y el registro de cada elemento de la Web por separado, cuestión que ahora no parece muy defendible, en tanto que se registra como un todo. En nuestra opinión, en tanto no se produzca la anunciada reforma del TRPI, y éste pueda regular algo al respecto, habrá que analizar caso por caso y ver esa Web en particular a que se asemeja más, si a una obra literaria, audiovisual... y aplicar la protección en cuestión. También deberían tenerse en cuenta los elementos que se tratan de proteger o que se han vulnerado, es decir, si el autor denuncia que se han vulnerado sus derechos de explotación sobre un video que se encontraba en su Web, entendemos que habrá que proteger al autor según las normas establecidas en el TRPI para las obras audiovisuales, y así sucesivamente.

Por dar alguna característica mas sobre los derechos de autor, en lo que se refiere a la creación de páginas Web, indicaremos que los contenidos de la misma, ya sean imágenes, textos, videos, audiciones..., corresponderán al titular de la misma, ya sea como creador o como titular de los derechos de explotación. Por su parte el diseñador de la Web, mas conocido como Webmaster, será el que ostente la titularidad de los derechos de autor en cuanto al diseño de la misma. La jurisprudencia ha tenido ya ocasión de pronunciarse en relación con los plagios de contenidos de una página Web, en la Sentencia del Juzgado de Primera Instancia de Madrid de 16 de marzo de 2001, considerando esta práctica contraria a los derechos de propiedad intelectual que son propiedad de la titular de la página Web, y considerando además esta conducta como competencia desleal, de acuerdo con la Ley de Competencia Desleal.

B) Programas de Ordenador.

Los programas de ordenador son tratados de manera diferente en el TRPI, como no podía ser de otra manera, ya que como vimos en su momento existe una Directiva específica en la materia que dispone que los programas de ordenador serán protegidos como derechos de autor, al quedar asimilados a las obras literarias, ya que utilizan el lenguaje escrito como medio de comunicación.

Por programa de ordenador, se entiende la secuencia de instrucciones o indicaciones destinadas a ser utilizadas directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

La protección otorgada al programa de ordenador abarca tanto al Código Fuente, como al Código Objeto. Por Código Fuente entendemos el lenguaje técnico en el que se realiza la escritura original del programa. Por el segundo entendemos la traducción de esa escritura original, llevándose a cabo por un mecanismo compilador de forma tal que el programa pueda ser ejecutado por la maquina.

El ámbito de protección también abarca el de toda la documentación preparatoria, así como la documentación técnica y los manuales de uso.

Al igual que el resto de obras susceptibles de protección, el programa de ordenador será protegido, si es original, en el sentido de ser una creación intelectual propia de su autor. No obstante , en los programas de ordenador, como bien señala Rodríguez Pardo[317], pueden intervenir en su elaboración varias partes, es por ello que la directiva sobre protección jurídica de programas de ordenador en su artículo 3 no habla de autor o titular, sino de beneficiarios en la explotación. Entre esos beneficiarios, el autor ve las siguientes partes:

- El promotor de la idea.
- El productor, entendiendo por éste el que realiza la aportación económica.
- El creador del contenido.
- El técnico encargado del ensamblaje de los elementos y contenidos.
- El coordinador general del proceso, que puede ser el productor o persona diferente.

Para delimitar a quien se entiende por autor, debemos estar al artículo 97 del TRPI, que establece las reglas que determinan al autor o autores y a los titulares de los derechos, en las que no vamos a entrar.

En cuanto al requisito de la originalidad requerido para poder acogerse a la protección establecida legalmente, tenemos que acudir al concepto que de ella se ha ido creado por la jurisprudencia, en particular la del Tribunal Supremo y de la regulación del TRPI, en particular la de las bases de datos. Siguiendo a Rodríguez Pardo[318], por originalidad entendida en sentido amplio, no sólo la derivada de los programas de ordenador, entendemos:

- Es un concepto que se aplica básicamente en la obra primera y no en sus reproducciones, bajo la idea de que la obra representa la personalidad y genialidad individual de su autor.
- Aparece como una cualidad predicable no sólo del contenido temático de una creación, sino de la creación en sí misma, debido al criterio de selección y ordenación de dicho contenido, pudiendo suceder que, no siendo susceptible de protección lo sea en cambio su continente.

[317] Ob. Cit. Página 122.
[318] OB. Cit. Páginas 305 y ss.

- Constituye el criterio definitivo para la protección que muestre sistemas originales y creativos.

Como tuvimos ocasión de comprobar en el capítulo primero, existe un debate sobre si los programas de ordenador deben ser protegidos por la PI o como patente a través de la Propiedad Industrial. A nivel internacional, tanto a nivel de Tratados Internacionales, como de legislación nacional comparada, las legislaciones de patentes vedan la posibilidad a patentar programas de ordenador, como así ocurre en España con la Ley 11/1986 de 20 de marzo de Patentes, cuyo artículo 4.2.C excluye expresamente a los programas de ordenador como invenciones susceptibles de ser patentadas. Esto choca con el artículo 96.3 que prevé la posibilidad de patente de ordenador. Por ello debemos entender que un programa de ordenador en sí mismo no puede ser patentado, pero si cabe que el programa entre a formar parte de una patente si forma parte de una invención que cumpla los requisitos legales para ser patentada.

Al igual que para el resto de modos de reproducción de una obra sujeta a los derechos de autor, se habilita al usuario legítimo a realizar una copia privada para su uso personal. El problema radica en la exención de este tipo de copias del canon por copia privada al que nos referíamos en su momento. Los programas de ordenador son copiados principalmente en CD-ROM por lo que se plantea la paradoja de que estos se encuentren grabados por el canon para soportes que almacenen o reproduzcan obras musicales o audiovisuales, estando exentos del mismo. Es por ello que nos encontramos ante una laguna legal de no difícil solución, ya que es imposible controlar en la compra de un CD el uso y la finalidad que le va a dar su legítimo adquirente, y los usos y las finalidades que les pudiera dar en un futuro, ya que originariamente le puede asignar una función, y posteriormente formatear el disco y darle otra distinta.

A continuación vamos a destacar una especialidad que se establece en los programas de ordenador, referida a la necesaria autorización del titular de los derechos de explotación en lo que respecta a la transformación de la obra. En virtud del artículo 100.5 no será necesario obtener la autorización del titular del derecho para la reproducción y traducción del Código del programa, cuando esa información sea imprescindible para lograr la interoperabilidad con otros programas informáticos, siempre que se cumplan con ciertos requisitos legales establecidos en el mismo artículo. Entendemos que es una buena medida en tanto que limita la acción de los monopolios y oligopolios, que no podrán crear programas que únicamente funcionen con programas diseñados por las mismas compañías.

Finalizaremos el epígrafe señalando algunos de los contratos que en relación con los programas de ordenador, pueden llegar a celebrarse. Atendiendo a la clasificación recogida por Rodríguez Pardo[319], tenemos los siguientes:

- Contrato de consultoría: se estudian las necesidades del cliente y se aportan las soluciones a estas necesidades.
- Contrato de desarrollo: Se encarga por parte del cliente el desarrollo de un programa.
- Licencia de uso: se transmiten los derechos de explotación autorizando su uso ya sea con carácter exclusivo, o no.
- Contrato de mantenimiento: La empresa ofrece al cliente la optimización del programa, su puesta al día y la corrección de errores.
- Contrato de auditoria informática: se revisa el software para analizar su funcionamiento y rendimiento.
- Contrato de outsourcing: en virtud de éste, una empresa independiente se responsabiliza del funcionamiento del sistema y del estudio de su idoneidad por parte del cliente.
- Contrato de escrow: se garantiza bajo determinadas circunstancias el acceso al Código Fuente.
- Contrato llave en mano: la empresa solventa al cliente todos los problemas informáticos que pueda tener, creando, instalando, readaptando los programas y asegurándose de su funcionamiento.

Esta clasificación es importante ya que, dependiendo del contrato firmado entre las partes, se entenderá o no, la obligación de suministrar al usuario del programa, las fuentes o llaves del mismo. Como reza la Sentencia del Tribunal Supremo de 17 de mayo de 2003, éstas se han de suministrar cuando el programa se haya confeccionado a medida del usuario. En caso contrario, el usuario quedaría en manos del programador inicial para la actualización o acomodación a las nuevas normativas o necesidades del usuario. Aunque éste último necesite de la autorización del programador inicial para transformar el programa, dicha transformación no debe quedar únicamente al interés, capricho o veleidad del programador, en lo que respecta al futuro del programa. Y esto es así porque el programa ha sido encargado y confeccionado a medida del cliente.

C) Bases de Datos.

Nuevamente al estar reguladas en una Directiva especial, debemos tratar separadamente las bases de datos, para poder destacar las innovaciones que sobre estas se establecen.

[319] Ob. Cit. Página 298.

Por base de datos debemos entender, atendiendo al TRPI, las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma. Con una definición tan genérica, debemos entender que comprende tanto a las recopilaciones de datos en soporte on line, como los soportes off line, como puede ser un CD-Rom.

Como parece lógico, se concede una protección a las bases de datos por los criterios de selección o disposición de sus contenidos (la simple reordenación de contenidos se considere transformación), sin perjuicio de los derechos que puedan subsistir sobre esos contenidos, pero en consonancia con la Directiva en la materia, se establece un derecho *sui generis,* que trata de proteger al fabricante de la base de datos, por la inversión en esfuerzo económico y de tiempo a la que ha tenido que hacer frente para introducir y recopilar los contenidos y datos en la misma. Para ello es necesario, en palabras del TRPI, que la inversión sea sustancial y sea evaluada cualitativa o cuantitativamente en inversión en recursos humanos, medios técnicos y financieros. Como bien aclara la Sentencia del Juzgado de Primera Instancia 13 de Madrid de 24 de julio de 2001, este derecho trata de evitar el daño comercial que pueden ocasionar a su creador las extracciones ya sean de un competidor o de un usuario de la misma, ciñéndose la cuestión a un mero análisis económico.

Por fabricante de la base de datos entendemos la persona natural o jurídica que toma la iniciativa y asume el riesgo de efectuar las inversiones sustanciales orientadas a la obtención, verificación o presentación de su contenido. Para protegerle se regula detalladamente, aunque no vamos a entrar en ello, las condiciones en las que el fabricante podrá denegar la extracción de partes no sustanciales del contenido de su base de datos y cuando el usuario legítimo estará autorizado a realizarlas sobre partes sustanciales o no sustanciales, tratando de limitar con ello, los posibles abusos que por parte del fabricante pudieran ocasionarse al usuario de la base de datos, es decir, se trata de limitar una posible práctica monopolística.

D) Problemas Específicos en Internet.

Un primer problema que puede plantearse desde la perspectiva de los derechos de autor, es la utilización masiva de hipertextos en Internet. Los hipertextos son creaciones que permiten el acceso a la información que contienen a través de un sistema de links o nudos de enlace, presentando la información de modo gradual, a medida que la solicita el usuario al pulsar con el puntero del ordenador en los nudos, o los sistemas hipermedia, que combinan el uso de hipertextos y sistemas multimedia. A raíz de estos sistemas se pueden planear dos problemas. El primero consiste en averiguar si es necesario el consentimiento expreso del titular de una Web cuando queremos utilizar links que conecten nuestros contenidos con los

suyos, y el segundo radica en el hecho de que en el momento en el que se introduce en la red un contenido, es accesible al público desde el lugar y el momento en el que lo desee, sin que por ello medie una autentica petición de difusión *on demand*.

Atendiendo al primer problema, para Rodríguez Pardo[320], se debe aplicar por analogía el derecho de cita regulado en el TRPI, y para Garrote Fernández-Díez son válidos siempre que el autor no manifieste los contrario, ya que los enlaces ni reproducen, ni transforman nada. Cuestión diferente es si al crear el enlace, se modifica el marco de la Web enlazada. Para el autor[321], se está de esta forma creando una obra transformada o derivada, ya que al introducir el marco se está cambiando el Código original, por lo que requiere el consentimiento del autor. Esta segunda opinión nos parece más afortunada, ya que el derecho de cita, según se encuentra regulado en el TRPI, requiere para su validez que sea utilizado con fines docentes o de investigación, requisito que no se da en la práctica totalidad de los enlaces creados en la actualidad. En todo caso creemos que es una buena costumbre intentar recabar la autorización del autor de la Web previamente a la creación del enlace, puesto que pudiera ocurrir que el autor no quiere verse relacionado con otros contenidos o personas físicas o jurídicas.

Cuestión ligada al supuesto anterior, es si interpretamos como derecho de cita el resumen que los buscadores realizan de las páginas Web, resumiendo su contenido, indicando la URL y el tamaño de ésta. Para Garrote Fernández-Díez[322], debe asimilarse a estas practicas el derecho de cita, salvo que el autor muestre su deseo de no ser resumido, estableciéndose la presunción de que sí lo desea. Como bien señala el autor, cuando se incorpore al derecho español la Directiva 2001/29/CE, el problema analizado tendrá mejor solución, ya que la Directiva establece en su artículo 5.3. i) que se pueden tomar prestados incidentalmente materiales ajenos. Por incidental el autor propone que se considere que supone un beneficio económico, aunque habrá que estar a lo que establezca el legislador en su momento.

Retomando a continuación el segundo problema planteado, vamos a manifestar que en los que se refiere a la divulgación de una obra a través de Internet, se produce ésta sin que, como veíamos anteriormente, se produzca una verdadera demanda de ejemplares por parte de los usuarios, por lo que de momento, y en espera de la próxima reforma de la PI en nuestro derecho, habrá que entender que por la naturaleza de Internet, se satisfacen razonablemente la demanda de ejemplares, puesto que Internet está al alcance de todos. Pero no es el único problema planteado, ya que a efectos de lo que se entiende por distribución de la obra, el TRPI lo vincula a transmisión de ejemplares materiales y no digitales. Es por ello

[320] Ob. Cit. Página 132
[321] Ob. Cit. Página 380.
[322] Ob. Cit. Página 459.

que se han planteado diversas opciones, que son recogidas por Garrote Fernández-Díez, que en resumen son las siguientes:

- O entendemos la distribución digital dentro del artículo 17 del TRPI, por el cual se otorga al autor el derecho a decidir sobre la explotación de su obra.
- O lo subsumimos dentro del artículo 20.1 del TRPI, comunicación pública.
- O bien creamos una nueva categoría.

Para el autor citado, la mejor opción es entenderlo como una variante del derecho de comunicación pública.

También se plantean problemas desde la perspectiva del derecho de reproducción, para ello analizaremos previamente como fluye la información por Internet. La información en Internet se introduce en códigos binarios (utilizando 0 y 1) y así fluye por la red. Al visualizar un documento en la red, éste no se recibe directamente sino que se obtiene la información mínima para reconstruirlo, por lo que el documento debe almacenarse previamente en la memoria del ordenador. Por lo que ya podríamos plantearnos si existe reproducción o no. Pero además, al introducir una obra analógica en la red, se podrían estar llevando a cabo otras dos reproducciones o transformaciones, de la obra analógica a la digital, y de la digital al servidor. En mi opinión, se trata de supuestos incluidos en el artículo 17 del TRPI, por el cual corresponde al autor el ejercicio exclusivo de los derechos de explotación en cualquier forma y en especial los de reproducción, distribución, comunicación pública y transformación. Por lo que si queremos incorporar una obra analógica a la red, necesitaremos el consentimiento del autor.

Otro problema ligado con la reproducción, es el de la copia temporal. Debido al funcionamiento de la red, y para mejorar su rendimiento, rapidez y funcionalidad, se almacenan en nuestro ordenador o en el del servidor las páginas visitadas. Aunque el almacenamiento en la RAM, memoria local o memoria sistema se produce temporalmente, la doctrina ha estudiado la problemática, que no debería ser tal cuando se adquiere la obra en línea, sino cuando se paga por una reproducción a modo de única visión, es decir se paga cada vez que se quiere visualizar o escuchar. En nuestro caso, la solución vendrá marcada por la transposición de la Directiva 2001/29/CE, ya que en su artículo 5.1 puede encontrarse la solución, al establecerse una excepción al derecho de reproducción, declarando exentas de éste los actos de reproducción provisional a los que se refiere el artículo 2 que sean transitorios o accesorios y formen parte integrante y esencial de un proceso tecnológico cuya finalidad consista en facilitar:

a) una transmisión en una red entre terceras partes por un intermediario o,
b) b) la utilización legal de una obra o prestación protegida, y que no tengan por sí mismos una significación económica independiente.

Directamente relacionado con el derecho de reproducción, se encuentra la copia privada. Como señala Garrote Fernández-Díez[323], la doctrina se encuentra dividida en este sentido, existiendo diversas posturas enfrentadas, que propugnan o no cobrar nada en concepto de derechos de autor en Internet, o cobrar según descarga o establecer algún sistema de cánones o licencias que proporcionen al autor una remuneración adecuada. En la medida en que se produzca la transposición al derecho español de la Directiva 2001/29/CE, se utilizarán u optarán por unas medidas u otras, existiendo grandes posibilidades en este campo, ya que en la actualidad no están sujetos a canon los escáner, impresoras o discos duros y tampoco se han desarrollado los contratos o licencias electrónicas que limiten las posibilidades de copia. Por otra parte, existen multitud de medidas tecnológicas que pueden limitar la explotación no autorizada de las obras. Cuando nos referíamos al supuesto del *P2P* en el capítulo primero ya mencionamos algunas, pero ahora indicaremos algunas más, como el tatuado de la obra o las *watermarks* que identifican la obra no original y avisan de que la que la lleva está protegida por derechos de autor, o bien se puede encriptar la obra (que no la transforma sino que la convierte en más segura), o recurrir al SCMS (*Serial Copyright Management Systems*) que sólo permite realizar una copia de la obra. Ni que decir tiene que en el derecho español las medidas que impidan las copias privadas en los supuestos autorizados por el TRPI serán o bien nulas, si se trata de condiciones generales incorporadas en un contrato, en virtud de la Ley de Condiciones Generales de la Contratación, o nulas si no son condiciones generales por limitar una norma imperativa, según reza el artículo 6.3 del Código Civil.

[323] Ob. Cit. Páginas 51 y ss.

CONCLUSIONES.

- El comercio electrónico afecta a un gran número de áreas y necesita el desarrollo de éstas para garantizar su éxito. Éstas serían, como se ha visto, la protección de consumidores, la protección de datos, la contratación a distancia con consumidores, los derechos de autor, el dinero electrónico, la fiscalidad, las tecnologías de seguridad de la información, el derecho de la competencia, la seguridad de redes y la coordinación y el consenso mundial en legislación y normalización.

- El comercio electrónico debido al carácter abierto y universal de Internet, se presta al comercio de carácter transfronterizo. Éste se ve incrementado ante la aparición de los productos digitalizados, que no necesitan entrega, sino que se descargan directamente por el usuario a través de una página *Web*. Por ello es necesario buscar el consenso a nivel internacional en materia de legislación y normalización. Difícilmente podrá implantarse éste, si la tecnología utilizada no está normalizada y no es interoperable entre sujetos de distintos países. De la misma manera, si no están regulados internacionalmente diversos aspectos de la vida del contrato, en especial, aquellos que protegen los derechos de los consumidores, los usuarios de Internet no utilizarán las posibilidades que les ofrece esta forma de comercio, debido a la incertidumbre que provoca la diferencia de legislaciones entre distintos países, que podrían incluso ser contradictorias.

- Por lo anteriormente dicho, los Estados pueden y deben actuar, pero lo que no deben hacer, es regular la materia sin tener en cuenta la normativa que existe en otros países. No se trata de crear clones, sino de tratar de armonizar, en la medida de lo posible, las diferentes legislaciones. Un buen sistema, es el adoptado por la CNUDMI en la elaboración de las dos leyes modelos estudiadas. La elección de éste sistema se debe a la convicción que, al dar unas pautas de por donde deberían ir las legislaciones nacionales, dejando eso sí, absoluta libertad al legislador nacional para adoptarlas, total o parcialmente, se pensó que en la practica, más Estados uniformarían sus legislaciones, que si se hubiera adoptado un Convenio Internacional.

- La necesidad de regular jurídicamente diversos aspectos del comercio electrónico, proviene de la conveniencia de otorgar a los usuarios que eligen esta forma de comercio, confianza en esta práctica. La red es impersonal, se suministran datos personales o lo más importante, se paga u ordenan pagos o el modo de conseguir dichos pagos, a personas físicas o jurídicas a las que no ves, no conoces. Salvo las grandes empresas que se benefician de la confianza que les otorga la marca, y aún así en principio no existiría seguridad de que sea

quien dice ser, los demás agentes económicos necesitan que se cree confianza de los consumidores en esta práctica.

- El marco jurídico que regule la materia ha de ser neutro y flexible. Esto no quiere decir otra cosa que deben tener cabida en su articulado, las soluciones y tecnologías existentes y futuras. De otra manera el marco jurídico se tendría que cambiar cada vez que hubiera una innovación tecnológica, lo que provocaría una tremenda inseguridad jurídica.

- Pero no sólo se debe actuar en lo que respecta a la protección de consumidores, en la creación de un marco jurídico sobre el comercio electrónico. Éste también se caracteriza por la posibilidad de realizar compras de pequeño valor económico, por lo que resulta aconsejable fomentar la autorregulación del sector, la elaboración de códigos de conducta por las partes intervinientes y la promoción de sistemas alternativos de solución extrajudicial de conflictos, que ofrezcan una solución rápida y barata al litigio en cuestión.

- Continuando con la autorregulación, también hay que tratar de lograrla en lo que respecta a la búsqueda de la normalización e interoperabilidad de las tecnologías de la sociedad de la información. La industria de este sector, ha de participar activamente en esta búsqueda y la máxima a aplicar es la utilización de soluciones y tecnologías aceptadas por un conjunto significativo del mercado, debiéndose basar preferentemente en normas internacionales abiertas.

- Las Administraciones Públicas tienen mucho que decir en cuanto a la generalización del uso de estas tecnologías. Utilizándolas en el desarrollo de sus relaciones con los particulares, dan ejemplo y levantan las reticencias e inseguridades que el uso de éstas pudieran ocasionar a los particulares. En definitiva, pueden generar confianza. También deben jugar un papel relevante en el desarrollo de estas tecnologías al poner en práctica, tecnologías, tales como, el uso de tarjetas inteligentes, métodos biométricos o sistemas criptográficos. Finalmente deben levantar las barreras legales que limiten el uso de estas tecnologías en sus relaciones con los particulares. Muchas ya se han levantado pero se hace necesario no bajar la guardia y continuar levantando las que aún quedan, o que se puedan originar en un futuro.

- El principio a aplicar en lo referente a la regulación de los contratos electrónicos, especialmente en lo que respecta a su validez y eficacia, es el Principio de Equivalencia Funcional, que no quiere decir otra cosa que el contrato electrónico no es una nueva modalidad contractual, sino un nuevo soporte de manifestación de la voluntad de las partes en los negocios jurídicos. Por ello, habrá que ver cuando se requiere un documento escrito y por qué motivos se optó por éste tipo. Si lo que se pretende es dejar constancia, lógicamente valdrá el documento electrónico, pero si lo que se pretende es

otorgar fe pública a través de un documento notarial, éste no será posible. Además, la aplicación de éste principio requiere dejar las normas preexistentes en materia contractual como estaban, sólo actuando puntualmente para introducir o regular, las especialidades que este *modus operandi* requiere.

- En materia de seguridad de tecnologías de la información, la máxima a aplicar es la económica, según la cual, hay que crear un sistema de seguridad cuya vulneración resulte más cara de lo que los piratas informáticos estén dispuestos a soportar.

- La firma digital de clave pública y basada en un certificado reconocido por un prestador de servicios de certificación, garantiza a través de sistemas criptográficos, la autenticidad, la integridad, la confidencialidad y la no repudiación del mensaje electrónico. Es decir, se garantiza la identidad de quien suscribe el mensaje, que éste no ha sido modificado o alterado, que no ha sido interceptado y leído y que una vez firmado, el firmante no puede decir que él no fue el que lo suscribió.

- El comercio electrónico reporta grandes ventajas a las empresas. Mejora su modelo de negocio y de gestión empresarial. También puede aumentar el valor añadido que las empresas ofrecen a sus clientes en todas las fases del contrato, como la información preliminar o el servicio postventa en línea. También las ofrece a los consumidores, que pueden acceder a una mayor oferta de productos, con precios más bajos y con libertad de horario.

- Se ha aprendido mucho de la crisis de las Puntocom. El modelo que deben seguir las empresas para aprovechar las ventajas que les ofrece el comercio electrónico, es un modelo mixto entre la empresa tradicional y la empresa virtual, denominado sistema de *bricks and clicks*. También debe tenerse presente la modalidad de comercio electrónico entre empresas *B2B*, por el ahorro que puede ocasionarles, en la compra de bienes y servicios indirectos.

- La LSSI, debido a las críticas que recibió en sus fases más tempranas de elaboración, es demasiado puritana y minuciosa en lo que respecta a la regulación de los derechos fundamentales y garantías de los ciudadanos, realizando menciones y regulando situaciones que, a tenor del ordenamiento jurídico español, resultan obvias, como la prohibición del *non bis in ídem* que se vio en su momento.

- Debido al carácter abierto y universal de Internet, los datos de carácter personal circulan libremente por la red, y se pueden introducir en ella. Es por ello que se deben armonizar a nivel internacional las distintas legislaciones en la materia, al igual que lo ha hecho la U.E., en aras a generar confianza en los usuarios. Pero no olvidemos que esa confianza comienza a generarse en el ámbito nacional, ya que continuamente se suministran datos de carácter personal a través de las

páginas Web, e incluso a veces esos datos se almacenan directamente en una base de datos ubicada en un servidor, gestionada o no, por un tercero. Es por ello que se requiere una mayor concienciación por parte de los afectados, en lo que respecta a sus derechos y el volumen de datos que están dispuestos a aportar. De la misma manera se requiere mayor concienciación por parte de las empresas, operen o no en la red, en cuanto a la necesidad de elaborar políticas de seguridad de datos y usar y recabar los datos necesarios para la prestación de sus servicios de acuerdo con la LOPD y códigos de conducta que pudieran establecerse. Aunque la protección de datos en Internet es importante, de momento las especialidades que plantea pueden ser solventadas por la normativa general sobre la materia.

- En materia de derechos de autor referentes al uso de las nuevas tecnologías, las soluciones a las vulneraciones de estos derechos pasan inevitablemente por la búsqueda del consenso a nivel internacional y por la creación de medidas tecnológicas antipiratería. Armonización para no dejar vía de escape a los infractores y medidas antipiratería para dificultar la copia ilegal. No obstante, somos pesimistas en esta materia, y aún discrepando con esta práctica, entendemos que a lo largo de los presentes años iremos viendo la aparición de nuevos cánones que graben los soportes donde puedan realizarse copias ilegales, pagando de esta manera justos por pecadores.

ANEXOS.

DISPOSICIONES NACIONALES COMUNICADAS POR LOS ESTADOS MIEMBROS Y RELATIVAS A:
Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, 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). A FECHA 17.6.2003.

Bélgica:
2. – Loi du 11 mars 2003 sur certains aspects juridiques des services de la sociétè de l'information visés à l'article 77 de la Constitution. Ref: MB Ed. 2 du 17/03/2003 p. 12960 (C – 2003/11126)

Dinamarca:
2. – Lov om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel ref: Lov nr 227 af 22/04/2002

Alemania:
2. – Gesetz über rechtliche Rahmenbedingungen für den Elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz (EGG)) ref: Bundesgesetzblatt, Jahrgang 2001, Teil I Nr. 70 vom 20/12/2001, Seite 3721
3. – Landesgesetz zu dem Sechsten Rundfunkänderungsstaatsvertrag und zur änderung des Landesrundfunkgesetzes vom 4/07/2002 ref : GVBl. Rheinland-Pfalz n° 10 du 12/06/2002 p. 255

Grecia:
SIN REFERENCIA

España:
2. – Ley 34/2002 de 11de julio, de servicios de la sociedad de la información y de comercio electrónico ref: BOE n° 166 de 12/07/2002 p. 25388

Francia:
SIN REFERENCIA

Irlanda:
2. – European Communities (Directive 2000/31/EC) Regulations 2003. Ref: SI n° 68/2003 of 24/02/2003

Italia:
2. – Decreto legislativo 09/04/2003 n. 70 – Attuazione delle direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della societa dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico ref: GURI Serie generale n° 87 du 14/04/2003

Luxemburgo:
2. – Loi du 14 août 2000 relative au commerce éléctronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers

Países Bajos:
SIN REFERENCIA

Austria:
2. – Regelung bestimmter rechtlicher Aspekte des elektronischen Geschäfts- und Rechtsverkehrs und Änderung des Signaturgesetzes sowie der Zivilprozessordnung ref: Bundesgesetzblatt n° 152, Jahrgang 2001, Teil I vom 21/12/2001, Seite 1977

Portugal:
SIN REFERENCIA

Finlandia:
2. – Laki tietoyhteiskunnan palvelujen tarjoamisesta ref: Suomen Säädöskokoelma n° 458 du 11/06/2002 p. 3039
3. – Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetun lain muuttamisesta ref: Suomen Säädöskokoelma n°459 du 11/06/2002 p. 3047
4. – Laki kuluttajansuojalain 2 luvun muuttamisesta ref: Suomen Säädöskokoelma n° 460 du 11/06/2002 p. 3048
5. – Laki sopimattomasta menettelystä elinkeinotoiminnassa annetun lain muuttamisesta ref: Suomen Säädöskokoelma n° 461 du 11/06/2002 p. 3049

Suecia:
2. – Lag om elektronisk handel och andra informationssamhällets tjänster ref: SFS 2002:562 du 14/06/2002 – SG(2002) A/6456 du 26/06/2002

Reino Unido:
2. – The Electronic Commerce (EC Directive) Regulations 2002 ref: SI n° 2013 du 31/07/2002 coming into force 21/08/2002 (Regulation 16 : 23/10/2002)

DISPOSICIONES NACIONALES COMUNICADAS POR LOS ESTADOS MIEMBROS Y RELATIVAS A:

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. A FECHA 17.6.2003.

Bélgica:
2. – Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électorniques et les services de certification ref: MB du 29/09/2001, page 33070
3. – Arrêté royal du 6/12/2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés ref: MB du 17/01/2003 p. 1541 (C – 2002/11524); (SG(2003)A/01676 du 13/02/2003)

Dinamarca:
2. – Lov nr. 417 om elektroniske signaturer af 31. Maj 2001
3. – Bekendtgorelse nr. 922 af 5. Oktober 2000 om noglecentres og systemrevisionens indberetning af oplysninger til Telestryrelsen.
4. – Bekendtgorelse nr. 923 af 5. Oktober 2000 om sikkerhedskrav m.v. til noglecentre

Alemania:
2. – Gesetz vom 16. Mai 2001 über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften ref: BGBl. Teil I Nr. 22, 21/05/2001 seite 876
3. – Gesetz vom 13. Juli 2001 zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr ref: BGBl. Teil I Nr. 35, 18/07/2001 seite 1542

Grecia:
2. – Instrument légal 150/2001 ref: FEK A n° 125 du 25/06/2001, page 2061

España:
2. – Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma electronica

Francia:
2. – Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ref: JORF n° 62 du 14/03/2000, page 3968 (NOR JUSX9900020L)
3. – Décret 2001-272 du 30 mars 2001 – Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, entrée en vigueur le 31/03/2001 ref: JORF du 31/03/2001, page 5070 (NOR JUSCO12O141D)
4. – Arrêté du 31/05/2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation ref: JORF du 08/06/2002 p. 10223 (NOR : ECOI0200314A) (SG(2003)A/47 du 09/01/2003)

Irlanda:
SIN REFERENCIA

Italia:
2. – Inserita nella Legge n. 422 del 29 dicembre 2000 (Allegato A – Legge comunitaria 2000) ref: GURI n. 16 del 20/01/2001 – S.O. n. 14/L
3. – Decreto legislativo 23 gennaio 2002 – Attuazione della direttiva 1999/93/CE relativa ad un quadro communitario per le firme elettroniche ref: GURI n° 39 du 15/02/2002

Luxemburgo:
SIN REFERENCIA

Países Bajos:
SIN REFERENCIA

Austria:
2. – Bundesgesetz über elektronische Signaturen (Signaturgesetz – Sig G) ref: BGBl. Teil I Jahrgang 1999 Nr. 190, 19/08/1999 page 145
3. – Bundesgesetz : Änderung des Signaturgesetzes ref: BGBl. Teil I Jahrgang 2000 Nr. 137, 29/12/2000 page 1353
4. – Verordnung : Signaturvervordnung – Sig V ref: BGBl. Teil II Jahrgang 2000 Nr. 30, 02/02/2000 page 93
5. – Verordnung : Feststellung der Eignung des Vereins “Zentrum für sichere Informationstechnologie – Austria (A-SIT)” als Bestätigungsstelle ref: BGBl. Teil II Jahrgang 2000 Nr. 31, 02/02/2000 page 105
6. – Bericht des Justizausschusses über die Regierungsvorlage (1999 der Beilagen) : Bundesgestz über elektronische Signature (Signaturgesetz – Sig G) und Regierungsvorlage : Bundesgesetz, mit dem das Signaturgesetz geändert wird ref: 065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. Et XXI. GP

Portugal:
2. – Decreto-Lei n° 62/2003 ref: Diario da Republica I Série A n° 79 du ¾/2003 p. 2170

Finlandia:
2. – Laki sähköisistä allekirjoituksista ref: Laki du 24/01/2003
3. – Laki viestintähallinnosta annetun lain 2 §:n muuttamisesta ref: Laki du 24/01/2003

Suecia:
2. – Lag om kvalificerade elektroniska signaturer; 02/11/2000 ref: SFS 2000:832
3. – Lagen om teknisk kontroll ref: SFS 1992:1119
4. – Förordningen om vissa skyldigheter för myndigheter vid ett medlemskap i Europeiska unionen ref: SFS 1994:2035)

Reino Unido:
2. – The Electronic Signatures Regulations, 2002 ref: S.I. n° 318 of 2002, coming into force on 08/03/2002

DISPOSICIONES NACIONALES COMUNICADAS POR LOS ESTADOS MIEMBROS Y RELATIVAS A:

Directiva 1995/46/CE de 24 de octubre de 1995, relativa a la protección de las personas físicas, en lo que respecta al tratamiento de sus datos personales y a la libre circulación de esos datos. A Fecha 5.8.2003. Fuente: Dirección General del Mercado Interior: http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm

Austria

Estado del Procedimiento Legislativo.

1. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 136/2001 of 17.08.1999 that applies to all processing by automatic means.
   Entrada en vigor: 01.01.2000.
2. Adopted ordinances: Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung – DSAV), Federal Law Gazette II Nr. 521/1999, about countries with adequate DP legislation (Switzerland and Hungary);

   Verordnung des Bundeskanzlers über das bei der Datenschutz- kommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2000 – DVRV), Federal Law Gazette II Nr. 520/1999, about the registration procedure; Verordnung des Bundeskanzlers über Standard- und Muster-anwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 – StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification.

   Seven Länder have adopted new DPLs to implement the Directive. These apply to processing otherwise than by automatic means. **Kärnten**
   Kärtner Landesdatenschutz-Gesetz (K-LDSG), LGBl. Nr. 59/2000 (Inkrafttreten: 01.01.2000)
   Niederösterreich
   NÖ-Datenschutzgesetz (NÖ DSG), LGBl. 0901-1 (Inkrafttreten: 01.01.2001)
   Oberösterreich
   Gesetz vom 1. Juli 1988 über die Auskunftspflicht der Organe des Landes, der Gemeinden, der Gemeindeverbände und der durch Landesgesetz geregelten Selbstverwaltungskörper (oÖ. Auskunftspflicht- und Datenschutzgesetz), LGBl. Nr. 46/1988; idF. LGBl. Nr. 41/2000
   Salzburg
   Gesetz über die Auskunftspflicht und den Datenschutz, LGBl. Nr. 73/1988, idF LGBl. Nr. 65/2001 (Inkrafttreten 01.07.2001)
   Steiermark
   Gesetz vom 20. März 2001 über den Schutz personenbezogener Daten in nicht automationsgestützt geführten Dateien (Steiermärkisches Datenschutzgesetz-StDSG), LGBl. Nr. 39/2001 (Inkrafttreten: 01.08.2001)
   Vorarlberg
   Vorarlberger Landes-Datenschutzgesetz, LGBl. Nr. 19/2000 (Inkrafttreten: 01.01.2000)
   Wien
   Wiener Datenschutzgesetz (Wr. DSG), LGBl. Nr. 125/2001

Belgica

Estado del Procedimiento Legislativo.

1. Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data
2. Modified by the implementation law of December 11, 1998 (O.J. 3.2.1999)

3. Secondary legislation adopted on 13 February 2001 and published in the Official Journal of 13 March 2001.
4. Entry into force: 01.09.2001 (exception for information when the data were not collected from the data subject then three years more).

Dinamarca

Estado del Procedimiento Legislativo.

1. The Act on Processing of Personal Data (Act No. 429) of 31 May 2000
2. Entrada en vigor 01.07.2000.

Finlandia

Estado del Procedimiento Legislativo.

1. The Finnish Personal Data Act (523/1999) was given on 22.4.1999
2. Entrada en vigor: 01.06.1999

Francia

Estado del Procedimiento Legislativo.

1. Law 78-17 of 6 January 1978
2. Draft implementation law of July 2001

Próximo paso

Debate en el Parlamento

Alemania

Estado del Procedimiento Legislativo.

1. The Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May English version : The Federal Data Protection Act applies to the federal publicsector and the private sector.
2. Entry into force: 23.05.2001.
   All Länder (except Sachsen and Bremen) adopted new DPLs to implement the Directive.These acts apply to the public sectorof the respective “Länder”. **Baden-Württemberg**
   Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) vom 27. Mai 1991, zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung des Landesdatenschutzgesetzes
   und anderer Gesetze vom 23. Mai 2000:
   Bayern
   Bayerisches Datenschutzgesetz (BayDSG) vom 23. Juli 1993, zuletzt geändert durch Gesetz zur Änderung des Bayerischen Datenschutzgesetzes vom 25.10.2000 (Inkrafttreten zum 01.01.2001):
   Berlin
   Berliner Datenschutzgesetz vom 17.Dezember 1990 (GVBl. 1991, S. 16, 54), geändert durch Gesetz vom 3.Juli 1995
   (GVBl. 1995, S. 404), zuletzt geändert durch Gesetz vom 30. Juli 2001(GVBl. I, S. 66) (Inkrafttreten zum 5.8.2001) :
   Brandenburg
   Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz – bgDSG)
   in der Fassung der Bekanntmachung vom 9. März 1999
   Hamburg
   Hamburger Datenschutzgesetz vom 5. Juli 1999, zuletzt geändert am 18. Juli 2001 (HmbGVBl. S. 216)
   Hessen
   Hessisches Datenschutzgesetz (HDSG) in der Fassung vom 7. Januar 1999

Mecklenburg-Vorpommern
Landesdatenschutzgesetz vom 28. März 2002 (GVOBl. M-V S. 154)
Niedersachsen
Niedersächsisches Datenschutzgesetz (NDSG) in der Fassung vom 29. Januar 2002 (Nds. GVBl. S. 22)
Nordrhein-Westfalen
Gesetz zum schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen-DSG NRW-)
idF. Der Bekanntmachung vom 9. Juni 2000
Rheinland-Pfalz
Landesgesetz zur Änderung datenschutzrechtlicher Vorschriften vom 8. Mai 2002 (GVBl. S. 177)
Saarland
Gesetz Nr. 1477 zur Änderung des Saarländischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 22. August 2001 (Abl. S. 2066)
Sachsen-Anhalt
Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA)
Schleswig-Holstein
Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000

Grecia

Estado del Procedimiento Legislativo.

1. Implementation Law 2472 on the Protection of individuals with regard to the processing of personal data
2. Entrada en vigor: 10.04.1997

Irlanda

Estado del Procedimiento Legislativo.

1. Data Protection (Amendment) Act 2003 enacted on 10 April 2003.
2. Entrada en vigor. 1.7.2003

Italia

Estado del Procedimiento Legislativo.

1. Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996.
2. Entry into force: 08.05.1997
3. Additional legal acts previewed by Act no. 676 of 31.12.1996 (in particular, the Legislative Decrees no. 123 of 09.05.97, no. 255 of 28.07.97, no. 135 of 08.05.98, no. 171 of 13.05.98, no. 389 of 06.11.98, no. 51 of 26.02.99, no. 135 of 11.05.99, no. 281 and no. 282 of 30.07.99 ; the Presidentials decrees No. 501 of 31.03.98, No. 318 of 28.07.99)

Próximo paso

Debate parlamentario sobre la renovación de la habilitación al Gobierno de la Ley 675

Luxemburgo

Estado del Procedimiento Legislativo.

1. DPL approved on 2 August 2002 and published in Memorial A 91 of 13 August 2002.
2. Entrada en vigor 1 Diciembre 2002

Paises Bajos

Estado del Procedimiento Legislativo.

1. DPL approved by the Senate on 06.07.2000 (O.J. 302/2000).
   Original and English version: Personal Data Protection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000
2. Entrada en vigor 1 Septiembre 2001.
3. Aprobada la legislación de desarrollo.

Portugal

Estado del Procedimiento Legislativo.

1. Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecçao de dados pessoais'
2. Entrada en vigor: 27.10.1998

España

Estado del Procedimiento Legislativo.

1. Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999).
   Entrada en vigor: 14.01.2000

Suecia

Estado del Procedimiento Legislativo.

1. Directive implemented by SFS 1998:204 of 29.4.98 and regulation SFS 1998:1191 of 03.09.98
2. Entrada en vigor: 24.10.1998.

Reino Unido

Estado del Procedimiento Legislativo.

1. Data Protection Act 1998.
2. Aprobada: 16.07.1998
3. Subordinate legislation passed on 17.02.2000.
   Entrada en vigor 01.03. 2000.

BIBLIOGRAFÍA.

Monografías.

- Contratos electrónicos y defensa del consumidor. Pinochet Olave, Ruperto. Marcial Pons. 2001.
- Derecho de la contratación electrónica. Illescas Ortiz, Rafael. Civitas. 2001.
- El Derecho de Autor en Internet. Garrote Fernández-Díez, Ignacio. Comares. 2003. 2ª Ed.
- El Derecho de Autor en la Obra Multimedia. Rodríguez Pardo, Julián. Dykinson. Madrid. 2003.
- Estudio sobre la Ley de Protección de Datos de Carácter Personal. Aparicio Salom, Javier. Aranzadi 2ª edición 2002.
- Firma electrónica y comercio electrónico. Consejo General de los Colegios Oficiales de Corredores de Comercio. Cuadernos de Derecho y Comercio. Monográfico 1999.
- La firma y el comercio electrónico en España. Álvarez-Cienfuegos Suárez, José María. Aranzadi. 2000.
- Los impuestos en el comercio electrónico. Cazorla Prieto, Luis María y Chico de la Cámara, Pablo. Aranzadi. 2001.
- Manual de Derecho Informático. Davara Rodríguez, Miguel Ángel. Aranzadi. 2002

Artículos en revistas especializadas.

- El comercio electrónico y la U.E.. Ferrer Ramírez, Raquel. Noticias de la Unión Europea. Nº 183. 2000.
- El documento electrónico y la firma digital. Su regulación en la U.E.. Díaz Fraile, Juan María. Noticias de la U.E.. Nº 177. 1999.
- Electronic Signatures: the technical and legal ramifications. Mason, Stephen. Computers&Law. December 1999 / January 2000. Volume 10. Issue 5.
- Is EU Competition Law the limit for the Internet?. Van Varissing, Paul. Computers&Law. December 2000 / January 2001. Volume 11. Issue 5.

Documentación y Normativa Comunitaria.

- Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, 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 comercio electrónico). DOL 178 de 17.7.2000.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. DOL 13 de 19.1.2000.
- Reglamento (CE) nº 377/2002 del Parlamento Europeo y del Consejo de 22 de abril de 2002, relativo a la aplicación del dominio de primer nivel "eu". DOL 113 de 30.4.2002.
- Comunicación de la Comisión: Estrategias para la creación de empleo en la sociedad de la información. Com. (2000) 48 final.
- Comunicación de la Comisión: El impacto de la economía electrónica en las empresas europeas. Com. (2001) 711 final.
- Comunicación de la Comisión: El informe de evaluación comparativa de la acción eEurope 2002. Com. (2002) 62 final.
- Comunicación de la Comisión: Iniciativa europea de comercio electrónico. Com. (1997) 157 final.

- Libro blanco sobre El crecimiento, la competitividad y el empleo. Retos y pistas para entrar en el siglo XXI. Com. (1993) 700 final.
- Comunicación de la Comisión: La sociedad de la información: nuevas prioridades surgidas entre Corfú y Dublín. Com. (1996) 395 final.
- Resolución del Consejo de 21 de noviembre de 1996, sobre las nuevas prioridades políticas en materia de la sociedad de la información. DOC 376 de 12.12.1996.
- Comunicación de la Comisión: Europa a la vanguardia de la sociedad mundial de la información. Plan de actuación móvil. Com. (1996) 607 final.
- Comunicación de la Comisión: eEurope. Una sociedad de la información para todos. Com. (1999) 687 final.
- Comunicación de la Comisión: eEurope. Una sociedad de la información para todos. Informe de avance. Com. (2000) 130 final.
- Comunicación de la Comisión: eEurope 2002. Una sociedad de la información para todos. Proyecto de plan de acción. Com. (2000) 330 final.
- Comunicación de la Comisión: Puesta al día sobre eEurope 2002. Com. (2000) 783 final.
- Comunicación de la Comisión: eEurope 2002. Impacto y prioridades. Com. (2001) 140 final.
- Comunicación de la Comisión: eEurope 2002. Accesibilidad a los sitios Web públicos y de su contenido. Com. (2001) 529 final.
- Resolución del Consejo de 25 de marzo de 2002, sobre el plan de acción eEurope 2002: accesibilidad a los sitios Web públicos y de su contenido. DOC 86 de 10.4.2002.
- Comunicación de la Comisión: Go Digital. Ayudar a las Pymes a pasar a la fase digital. Com. (2001) 136 final.
- Resultados de la reunión informal de ministros de telecomunicaciones y sociedad de la información. Documento de la Presidencia. Vitoria 22-23 de febrero de 2002. www.ue2002.es.
- Comunicación de la Comisión: eEurope 2005. Una sociedad de la información para todos. Plan de acción presentado para el Consejo Europeo de Sevilla. Com. (2002) 236 final.
- Consejo Europeo de Sevilla. Conclusiones de la Presidencia. Punto 54.
- Decisión del Consejo 98/253 de 30 de marzo de 1998, por la que se adopta un programa plurianual comunitario para estimular el establecimiento de la sociedad de la información en Europa. DOL 107 de 7.4.1998.
- Decisión del Consejo 2000/819/CE de 20 de diciembre de 2000, relativa al programa plurianual a favor de la empresa y el espíritu empresarial, en particular para las pequeñas y medianas empresas (PYME), 2001-2005. DOL 333 de 29.12.2000.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo, por la que se crea la Agencia Europea de Seguridad de las Redes y de la Información. Com. (2003) 63 final.
- Propuesta de Decisión del Consejo, por la que se adopta un programa plurianual (2003-2005) para el seguimiento de eEurope, la difusión de las buenas prácticas y la mejora de la seguridad de las redes y de la información (MODINIS). Com. (2002) 425 final.
- Resolución del Consejo de 27 de noviembre de 1995, sobre los aspectos industriales para la U.E., en el desarrollo de la sociedad de la información. DOC 341 de 19.12.1995.
- Resolución del Consejo de 19 de enero de 1999, sobre la dimensión de los consumidores en la sociedad de la información. DOC 23 de 28.1.1999.
- Resolución del Consejo de 25 de mayo de 2000, sobre una red comunitaria de órganos nacionales responsables de la solución extrajudicial de litigios en materia de consumo. DOC 155 de 6.6.2000.
- Recomendación de la Comisión de 4 de abril de 2001, relativa a los principios aplicables a los órganos extrajudiciales de resolución consensual de litigios en materia de consumo. DOL 109 de 19.4.2001

- Recomendación de la Comisión 98/257/CE de 30 de marzo de 1998, relativa a los principios aplicables a los órganos responsables de la solución extrajudicial de los litigios en materia de consumo. DOL 115 de 17.4.1998.
- Red extrajudicial europea. Documento de trabajo de la Comisión Sec. (2000) 405.
- Comunicación de la Comisión: mejorar el acceso a los consumidores a mecanismos alternativos de solución de litigios. Com. (2001) 161 final.
- Comunicación de la Comisión: el comercio electrónico y los servicios financieros. Com. (2001) 66 final.
- Directiva 1995/46/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 sus datos personales y la libre circulación de esos datos. DOL 281 de 23.11.1995.
- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y los Organismos comunitarios. DOL 8 de 12.1.2001.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, (directiva sobre la privacidad y las comunicaciones electrónicas). DOL 201 de 31.7.2002.
- Directiva 2002/77/CE de la Comisión de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas. DOL 249 de 17.9.2002.
- Directiva 1997/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. DOL 24 de 30.1.1998. Derogada por Directiva 2002/58/CE.
- Decisión 2001/497/CE de 15 de junio de 2001 de la Comisión, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE. DOL 181 de 4.7.2001.
- Decisión 2002/16/CE de 27 de diciembre, de la Comisión, relativa a cláusulas contractuales tipo para la transferencia de datos personales a los encargados de tratamiento establecidos en terceros países, de conformidad con la directiva 95/46/CE. DOL 6 de 10.1.2002.
- Directiva 1997/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia. DOL 144 de 4.6.1997.
- Directiva 2002/65/CE del Parlamento Europeo y del Consejo de 23 de septiembre de 2002, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, y por la que se modifican la Directiva 90/619/CEE del Consejo y las Directivas 97/7/CE y 98/27/CE. DOL 271 de 9.10.2002.
- Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores y por la que se modifican las Directivas 97/7/CE y 98/27/CE. Com. (1998) 468 final.
- Propuesta modificada de Directiva del Parlamento Europeo y del Consejo, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores y por la que se modifican las Directivas 97/7/CE y 98/28/CE. Com. (1999) 385 final.
- Propuesta modificada de Directiva del Parlamento Europeo y del Consejo, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores y por la que se modifican las Directivas 97/7/CE y 98/28/CE. Com. (2002) 360 final.
- Consejo Europeo de Barcelona. Conclusiones de la Presidencia. Punto 35.
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la coordinación de los procedimientos de adjudicación de los contratos públicos de suministro, servicio y obras. Com. (2000) 275 final.

- Propuesta modificada de Directiva del Parlamento Europeo y del Consejo relativa a la coordinación de los procedimientos de adjudicación de los contratos públicos de suministro, servicio y obras. Com. (2002) 236 final.
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la coordinación de los procedimientos de adjudicación de los contratos públicos en los sectores del agua, energía, transportes y telecomunicaciones. Com. (2000) 276 final.
- Propuesta modificada de Directiva del Parlamento Europeo y del Consejo relativa a la coordinación de los procedimientos de adjudicación de los contratos públicos en los sectores del agua, energía, transportes y telecomunicaciones. Com. (2002) 235 final.
- Directiva 2001/29/CE del Parlamento Europeo y del Consejo de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información. DOL 167 de 22.6.2001.
- Directiva 91/250/CEE del Consejo de 14 de mayo de 1991, relativa a la protección jurídica de programas de ordenador. DOL 122 de 17. 5.1991. Modificada por Directiva 93/98/CEE.
- Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la patentabilidad de las invenciones implementadas en ordenador. Com. (2002) 92 final.
- Directiva 92/100/CEE del Consejo de 19 de noviembre de 1992, sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual. DOL 346 de 27.11.1992. Modificada por Directiva 93/98/CEE.
- Directiva 93/83/CEE del Consejo de 27 de septiembre de 1993, sobre coordinación de determinadas disposiciones relativas a los derechos de autor y derechos afines a los derechos de autor en el ámbito de la radiodifusión vía satélite y de la distribución por cable. DOL 248 de 6.10.1993.
- Directiva 93/98/CEE del Consejo de 29 de octubre de 1993, relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines. DOL 290 de 24.11.1993.
- Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. DOL 77 de 17.3.1996.
- Tratado de la OMPI sobre derechos de autor Ginebra. 1996. DOL 89 de 11.4.2000.
- Tratado de la OMPI sobre interpretación o ejecución de fotogramas. Ginebra. 1996. DOL 89 de 11.4.2000.
- Directiva 2000/12/CE del Parlamento Europeo y del Consejo de 20 de marzo de 2000, relativa al acceso a la actividad de las entidades de crédito y a su ejercicio. DOL 126 de 26.5.2000.
- Directiva 2000/28/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000, por la que se modifica la Directiva 2000/12/CE. DOL 275 de 27.10.2000.
- Directiva 2000/46/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión cautelar de dichas entidades. DOL 275 de 27.10.2000.
- Comunicación de la Comisión: comercio electrónico y fiscalidad indirecta. Com. (1998) 374 final.
- Directiva 77/388/CEE del Consejo de 17 de mayo de 1977, en materia de armonización de las legislaciones de los Estados Miembros relativas a los impuestos sobre el volumen de negocios –sistema común del impuesto sobre el valor añadido: base imponible uniforme- (VI Directiva Iva). DOL 145 de 13.6.1977.
- Directiva 1999/59/CE del Consejo de 17 de junio de 1999, por la que se modifica la Directiva 77/388/CEE en lo que respecta al régimen del impuesto sobre el valor añadido aplicable a los servicios de telecomunicaciones. DOL 162 de 26.6.1999.
- Directiva 2002/38/CE del Consejo de 7 de mayo de 2002, por la que se modifica y se modifica temporalmente la Directiva 77/388/CEE, respecto del régimen del impuesto sobre el

valor añadido aplicable a los servicios de radiodifusión y televisión y a algunos servicios prestados por vía electrónica. DOL 128 de 15.5.2002.

- Reglamento (CE) nº 792/2002 del Consejo de 7 de mayo de 2002, por el que se modifica temporalmente el Reglamento (CE) nº 218/92 sobre cooperación administrativa en materia de impuestos indirectos (Iva), en cuanto a medidas adicionales relativas al comercio electrónico. DOL 128 de 15.5.2002.
- Directiva 2002/115/CE del Consejo de 20 de diciembre de 2001, por la que modifica la Directiva 77/388/CEE con objeto de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el impuesto sobre el valor añadido. DOL 15 de 17.1.2002.
- Reglamento (CE) nº 458/2002 del Consejo de 6 de marzo de 2001, por el que se modifica el Reglamento (CE) nº 1334/2000 con respecto a la lista de productos y tecnologías de doble uso cuando se exporten. DOL 65 de 7.3.2001.
- Reglamento (CE) nº 1334/2000 del Consejo de 22 de junio de 2000, por el que se establece un régimen comunitario de control de las exportaciones de productos y tecnologías de doble uso. DOL 159 de 30.6.2000. Modificado por Reglamento (CE) nº 2889/2000, DOL 336 de 30.12.2000.
- XXX Informe sobre la política de competencia 2000. Comisión Europea. OPOCE. 2001.
- Reglamento (CE) nº 1400/2002 de la Comisión de 31 de julio de 2002, relativo a la aplicación del apartado 3 del artículo 81 del TCE, a determinadas categorías de acuerdos verticales y prácticas concertadas en el sector de los vehículos de motor. DOL 203 de 1.8.2002.
- Comunicación de la Comisión: la transmisión electrónica de datos comerciales mediante redes de comunicación TEDIS y propuesta de Reglamento del Consejo, por el que se establece la fase preparatoria de un programa comunitario relativo a la transferencia electrónica de datos de uso comercial utilizando las redes de comunicación TEDIS. Com. (1986) 662 final.
- Decisión del Consejo 87/499/CEE de 5 de octubre de 1987, por la que se establece un programa comunitario relativo a la transferencia electrónica de datos de uso comercial utilizando las redes de comunicación TEDIS. DOL 285 de 8.10.1987.
- Decisión 1989/241/CEE del Consejo de 5 de abril de 1989, que modifica a la Decisión 89/499/CEE por la que se establece un programa comunitario relativo a la transferencia electrónica de datos de uso comercial utilizando las redes de comunicación TEDIS. DOL 97 de 11.4.1989.
- Decisión 1991/385/CEE del Consejo de 22 de julio de 1991, por la que se establece la segunda fase del programa TEDIS. DOL 208 de 30 de julio de 1991.
- Comunicación de la Comisión: la evaluación del programa de sistemas de intercambio electrónico de datos comerciales TEDIS. Com. (1997) 335 final.
- Recomendación de la Comisión 94/820/CE de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos. DOL 338 de 28.12.1994.
- Decisión 1992/242/CEE del Consejo de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información. DOC 123 de 8.5.1992.
- Comunicación de la Comisión: seguridad de las redes y de la información: Propuesta para un enfoque político europeo. Com. (2001) 298 final.
- Recomendación del Consejo de 25 de junio de 2001, sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología. DOC 187 de 3.7.2001.
- Propuesta de Decisión Marco relativa a los ataques de los que son objeto los sistemas de la información. Com. (2002) 173 final.

- Comunicación de la Comisión: creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos. Com. (2001) 890 final.
- Libro verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de la información. Com. (1996) 483 final.
- Recomendación 1998/560/CE del Consejo de 24 de septiembre de 1998, relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana. DOL 270 de 7.10.1998.
- Resolución del Consejo y de los Representantes de los Gobiernos de los Estados Miembros reunidos en el seno del Consejo, de 17 de febrero de 1997, sobre contenidos ilícitos y nocivos en Internet. DOC 70 de 6.3.1997.
- Decisión 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999, por la que se crea un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. DOL 33 de 6.2.1999.
- Comunicación de la Comisión: evaluación intermedia de la ejecución del plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Com. (2001) 690 final.
- Comunicación de la Comisión: sobre el seguimiento al plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales y Propuesta de Decisión del Parlamento Europeo y del Consejo por la que se modifica la Decisión 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Com. (2002) 152 final.
- Decisión 1151/2003/CE del Parlamento Europeo y del Consejo de 16 de junio de 2003, que modifica la Decisión 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos mundiales. DOUE serie L 162 de 1.7.2003.
- Conclusiones del Consejo de 17 de diciembre de 1999, sobre la protección de los menores ante el desarrollo de los servicios audiovisuales digitales. DOC 8 de 12.1.2000.
- Comunicación de la Comisión: la mundialización y la sociedad de la información, necesidad de reforzar la coordinación internacional. Com. (1998) 50 final.
- Reglamento (CE) nº 44/2001 del Consejo de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. DOL 12 de 16.1.2001.
- Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información. DOL 204 de 21.7.1998. Modificada por Directiva 98/48/CE, DOL 217 de 5.8.1998.
- Directiva 2003/33/CE del Parlamento Europeo y del Consejo de 26 de mayo de 2003, relativa a la aproximación de las disposiciones legales reglamentarias y administrativas de los Estados miembros en materia de publicidad y patrocinio de los productos del tabaco, DOUE serie L 152 de 20 de junio de 2003.
- Directiva 97/13/CE del Parlamento Europeo y del Consejo de 10 de abril de 1997, relativa a un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones. DOL 117 de 7.5.1997.

- Directiva 2002/20/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (directiva autorización) DOL 108 de 24.4.2002.
- Directiva 98/27/CE del Parlamento Europeo y del Consejo de 19 de mayo de 1998, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores. DOL 166 de 11.6.1998.
- Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa al servicio universal y los demás derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (directiva servicio universal). DOL 108 de 24.4.2002.
- Comunicación de la Comisión: Europa en marcha hacia la sociedad de la información. Plan de actuación. Com. (1994) 347 final.
- Comunicación del la Comisión: el fomento de la seguridad y la confianza en la comunicación electrónica. Com. (1997) 503 final.
- Decisión de la Comisión 2003/375/CE, de 21 de mayo de 2003, relativa a la designación del Registro del Dominio de primer nivel eu. DOUE serie L 128 de 24.5.2003.

Documentación y normativa internacional.

- Convenio de la Unión de Berna para la protección de obras literarias y artísticas de 9 de septiembre de 1886. BOE 81 de 4.4.1974 y 260 de 30.10.1974.
- Convenio de Roma sobre ley aplicable a las obligaciones contractuales, de 19 de junio de 1980. BOE 171 de 19 de julio de 1993; corrección de errores BOE 189 de 9 de agosto de 1993.
- Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, firmado en Estrasburgo por el Plenipotenciario de España el 28 de enero de 1982. BOE 274 de 15.11.1985.
- Directrices sobre criptografía de la OCDE. Recomendaciones del Consejo de 27.3.1997. www.oecd.org/EN/home/0,,EN-home-29-nodirectotate-no-no29,00htlm.
- Ley modelo de la CNUDMI sobre el comercio electrónico con la guía para su adaptación al derecho interno de 1996, con la adición del artículo 5 bis en la forma aprobada en 1998. www.uncitral.org/sp_index.htm.
- Política Uniforme de solución de controversias en materia de nombres de dominio de 26 de agosto de 1999 del ICANN. http://www.icann.org/udrp/udrp.htm
- Reglamento de Política Uniforme de solución de controversias en materia de nombres de dominio de 24 de octubre de 1999 del ICANN. http://www.icann.org/udrp/udrp.htm
- Reglamento Adicional de la OMPI relativo a la Política Uniforme de solución de controversias en materia de nombres de dominio de 1 de diciembre de 1999. www.wipo.org .
- Ley modelo de la CNUDMI sobre firmas electrónicas con la guía para su incorporación al derecho interno de 2001. www.uncitral.org/sp_index.htm.

Normativa española.

- Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones. BOE 264 de 4 de noviembre de 2003.
- Orden ECO/2579/2003 de 15 de septiembre, por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Ministerio de Economía y sus Organismos adscritos. BOE 225 de 19.9.2003.
- Orden PRE/2440/2003 de 29 de agosto, por el que se desarrolla la regulación de la tasa por asignación del recurso limitado de nombres de dominio bajo el código de país correspondiente a España (.es) BOE de 9.9.2003.
- Proyecto de Ley de Firma Electrónica. Boletín Oficial de las Cortes Generales. Serie A de 20 de junio de 2003. Núm. 158-1.
- Decreto 67/2003 de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad Autónoma de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.
- Orden CTE/662/2003 de 18 de marzo, por la que se aprueba el Plan Nacional de nombres de Dominio de Internet bajo el código de país correspondiente a España ("es"). BOE de 26-03-2003.
- Real Decreto 281/2003, de 7 de marzo, por el que se aprueba el Reglamento del Registro General de la Propiedad Intelectual. BOE de 28.3.2003.
- Decreto 48/2003 de 20 de febrero por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos.
- Resolución 2/2003 de 14 de febrero de la Dirección General de la Agencia Estatal de la Administración Tributaria, sobre determinados aspectos relacionados con la facturación telemática. BOE 51 de 28 de febrero de 2003.
- Ley 53/2002 de 30 de diciembre, de medidas fiscales, administrativas y del orden social. BOE 313 de 31 de diciembre de 2002.
- Orden HAC/3134/2002 de 5 de diciembre sobre un nuevo desarrollo del régimen de facturación telemática previsto en el artículo 88 de la Ley 37/1992 de 28 de diciembre del impuesto sobre el valor añadido y en el artículo 9 bis del Real Decreto 2402/1985 de 18 de diciembre. BOE 298 de 13 de diciembre de 2002
- Ley 47/2002 de 19 de diciembre, de reforma de la Ley 7/1996 de 15 de enero, de Ordenación del Comercio Minorista, para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE, en materia de contratos a distancia y para la adaptación de diversas Directivas Comunitarias. BOE 304 de 20 de diciembre de 2002.
- Ley 44/2002 de 22 de noviembre, de Medidas de Reforma del Sistema Financiero. BOE 281 de 23 de noviembre.
- Ley 39/2002 de 28 de octubre, de transposición al ordenamiento jurídico español de diversas directivas comunitarias en materia de protección de los intereses de los consumidores y usuarios. BOE de 29 de octubre de 2002.
- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE 166 de 12.7.2002. Corrección de error BOE de 8 de Agosto de 2002.
- Orden INT/1751/2002 de 20 de junio, por el que se regulan los ficheros informáticos de la Dirección General de la Policía que contienen datos de carácter personal.
- Ley 5/2002 de 19 de abril, de la Agencia Catalana de Protección de Datos.
- Decreto 53/2002 de 23 de abril, de protección de datos de carácter personal en la Junta de Comunidades de Castilla La Mancha
- Orden CTE/711/2002 de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.
- Ley 17/2001 de 7 de diciembre de Marcas. BOE de 8 de diciembre.

- Ley 8/2001 de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. BOE 245 de 12.10.2001.
- 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.
- Instrucción 1/2000 de 1 de diciembre, de la Agencia de Protección de Datos, sobre las normas que rigen los movimientos internacionales de datos. BOE 301 de 16.12.2000.
- Real Decreto 1906/1999 de 17 de diciembre, sobre contratación telefónica o electrónica con condiciones generales, en desarrollo del artículo 5.3 de la Ley 7/1998 de 13 de abril, de condiciones generales de la contratación. BOE 313 de 31.12.1999.
- Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. BOE 298 de 14.12.1999.
- Real Decreto 1828/1999 de 3 de diciembre, por el que se aprueba el Reglamento del Registro de Condiciones Generales de la Contratación. BOE 306 de 23 de diciembre de 1999.
- Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma electrónica. BOE 224 de 18.9.1999.
- Real Decreto 994/1999 de 14 de junio, de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. BOE 151 de 25.6.1999.
- Instrucción 1/1998 de 19 de enero de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. BOE 25 de 19.1.1998.
- Ley 7/1998 de 13 de abril, sobre condiciones generales de la contratación. BOE 89 de 14.4.1998.
- Orden del Ministerio de Justicia, de 31 de julio, por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. BOE 200 de 21.8.1998.
- Instrucción 1/1996 de 1 de marzo de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios.
- Instrucción 2/1996 de 1 de marzo, de la Agencia de Protección de Datos sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.
- Real Decreto Legislativo 1/1996 de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. BOE de 24.4.1996
- Orden del Ministerio de Justicia e Interior de 2 de febrero, por la que se aprueba la relación e países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. BOE 35 de 10.2.1995.
- Real Decreto 1332/1994 de 20 de junio, por el que se desarrollan algunos preceptos de la ley orgánica. BOE 147 de 26.6.1994.
- Real Decreto 428/1993 de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. BOE 106 de 4.5.1993.
- Ley 37/1992 de 28 de diciembre, del Impuesto Sobre el Valor Añadido. BOE de 29.12.1992.

Prensa.

- Diario ABC de 16.1.2002.
- Diario ABC de 7,2,2002.
- Diario ABC de 8.2.2002.
- Diario ABC de 9.2.2002.
- El País de los Negocios de 10.2.2002. Página 9.

- Diario ABC “Economía” de 17.3.2002. Páginas 5 y ss.
- Diario ABC “Tecnología” de 21.3.2002. Página 7.
- El País de los Negocios de 24.3.2002. Página 5.
- Diario ABC “Tecnología” de 24.4.2002. Página 45.
- Diario ABC “Economía” de 28.4.2002. Página 11.
- Diario ABC “Tecnología” de 1.5.2002. Página 35.
- El País de los Negocios de 2.6.2002. Página 7.
- Diario ABC de 21.8.2002. Página 21.
- Diario ABC de 25.8.2002. Página 29.
- Diario ABC de 2.10.2002. Páginas 44 y 45.
- Diario ABC “Tecnología” de 20.11.2002. Página 41.
- Diario ABC “Tecnología” de 4.12.2002. Página 50.
- Diario ABC “Tecnología” de 16.07.2003.

Direcciones de Internet.

- Agencia Española de Certificación www.ace.es .
- Agencia Española de Normalización. http://www.aenor-e.com
- Agencia Española de Protección de Datos: www.agenciaprotecciondatos.org
- Arbitraje de Consumo. www.consumo-inc.es/arbitraje/arbitraje.htm.
- Asociación Española de Comercio Electrónico. www.aece.org/
- Asociación de Internautas. www.internautas.org/
- Asociación Española de Tiendas Virtuales (ATIENDES) www.atiendes.com
- Asociación de Usuarios de Internet. www.aui.es
- Centro de Alerta Temprana de virus y seguridad informática http://www.alerta-antivirus.es/ .
- Comisión Europea: Dirección General Del Mercado Interior. http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm
- Comisión Europea. Sociedad de la información. europa.eu.int/comm/dgs/information_society/index_es.htm
- Confianza Online. http://www.confianzaonline.org/
- CNUDMI. www.uncitral.org/
- ETSI. www.etsi.org/
- Fabrica Nacional de la Moneda y Timbre. www.fnmt.es
- ICANN: http://www.icann.org/udrp/udrp.htm
- IQUA. www.iqua.net
- Ministerio de Ciencia y Tecnología. www.mcyt.es y www.lssi.es
- OCDE. www.oecd.org/
- OMPI: www.wipo.int
- Organización para la defensa de los derechos civiles *Statewatch*. www.statewatch.org/
- Presidencia Española de la U.E. 2002. www.ue2002.es
- Portal de e-comercio para la empresa. www.ebusinesslex.net
- Red.es. www.red.es
- Red Extrajudicial Europea (EEJNET): http://www.eejnet.org/
- Terceros de Confianza. www.tercerosdeconfianza.com
- Unión Europea. Europa.eu.int

Jurisprudencia.

- Las Sentencias reseñadas proceden de la Base de Datos de Datadiar.

ÍNDICE.

Págs.