RELACIONES COMERCIALES POR MEDIOS ELECTRÓNICOS

Mª ARÁNZAZU ALCAIDE DE LA FUENTE

ISBN-13: 978-84-692-5044-0

INDICE

1. INTRODUCCIÓN

En el origen de este trabajo de investigación está mi interés en el proceso de cambio global en el que la sociedad se encuentra inmersa y por el que las viejas estructuras están siendo transformadas a gran velocidad, así como por la importancia decisiva de una herramienta como Internet, que lo ha facilitado (incluso se podría decir que lo ha propiciado).

La década de los años ochenta marca el inicio de un espectacular fenómeno de globalización: supresión de fronteras, apertura de mercados, cambios sociales, interacción de culturas, universalización y estandarización de las economías, etc.

Uno de los grandes impulsores de este proceso ha sido, sin duda, el desarrollo de las nuevas tecnologías (en especial de las telecomunicaciones) y los cambios originados por el crecimiento de las

redes de comunicación en general y de Internet en particular, que han definido un nuevo entorno mundial, haciendo realidad el concepto de un mundo global interconectado.

En este contexto, la información ha adquirido una importancia vital para todos los aspectos de la sociedad, incluido el económico. La Red se ha configurado como una revolución en sí misma, que afecta, influye y modifica muchos de los aspectos sociales, culturales, económicos y empresariales de nuestra vida, cambiado nuestra forma de relacionarnos a todos los niveles.

Se han producido cambios en la forma de comunicarnos: las cartas escritas con letra redondilla y enviadas en un sobre con su sello ya han pasado a la historia, ¡hasta las felicitaciones de Navidad se envían por email o SMS!; ya no hay merendolas en las que te intercambias las fotos de las vacaciones: ahora se vuelcan en el PC y se envían electrónicamente en pocos minutos, y si quieres hacer un álbum de fotos eliges tus preferidas entre tus fotos digitales, las colocas en una página *web* arrastrándolas con el ratón, ... y en pocos días recibes un álbum precioso a todo color que te han preparado unas personas a las que no conoces, en un país que, igual, tampoco conoces. Se "chatea" con desconocidos, se "liga" a través de la *web* gracias a empresas de servicios que ponen en contacto a personas de todo el mundo. Es posible encontrar cualquier tipo de información en cualquier idioma y en tiempo real; ver el estado de las pistas de tu estación de esquí favorita para decidir si te vas allí a pasar el fin de semana; estudiar un máster *on-line*, leer, contratar las vacaciones, hablar por “teléfono” viendo la imagen en directo de tus interlocutores... y, por supuesto, comprar cualquier cosa. Las posibilidades parecen ilimitadas.

Un elemento claro que cambia en Internet es el tiempo: el mundo se vuelve instantáneo, se pasa a trabajar en tiempo real y se anulan las diferencias horarias, los tiempos entre la emisión y la recepción de un

mensaje; entre la operación, por ejemplo, bancaria, que realizamos y su registro en la contabilidad de la empresa. Otro elemento que cambia es el espacio: desde cualquier parte se puede estar en el centro de todo. Tiempo y espacio se convierten en inmediatez e instantaneidad en este entorno.

Internet es hoy una tecnología omnipresente. En poco tiempo se ha convertido en foco de atención por parte de las más diversas organizaciones, consumidores, gobiernos y medios de comunicación. Y no es de extrañar puesto que estamos evolucionando hacia una economía de servicios en la cual la habilidad de mover información es esencial.

Esta revolución, lógicamente, ha involucrado también al comercio.
Al igual que lo hicieron en su día el teléfono y el fax, Internet se configura como una herramienta que puede ser utilizada para mejorar la eficiencia del desarrollo de la actividad empresarial.
Centrada la cuestión desde el punto de vista del Derecho y más concretamente en el ámbito del Comercio Internacional (objeto de este Máster), los aspectos a analizar también se multiplican puesto que, si bien partimos del concepto milenario de "comercio", realizado éste a través de medios electrónicos, obliga a actualizar antiguos conceptos y a crear otros desde la nueva realidad virtual. Por ejemplo, la firma manuscrita de toda la vida tiene su "virtual" *alter ego* en la firma electrónica, la factura... su factura electrónica, el D.N.I. ... el DNI electrónico, y así sucesivamente.

La posibilidad de contactar y contratar con operadores desconocidos en una red abierta y la demanda de mayor seguridad en las transacciones nos lleva a estimar que estamos ante una nueva realidad: el "comercio electrónico en Internet", que se muestra, no sólo como una vía de comunicación, sino como un nuevo mercado donde realizar

actividades virtuales.

Esta nueva forma de realizar todo tipo de transacciones, comerciales o no, a distancia y por medios electrónicos presenta grandes ventajas de tipo práctico y económico, de ahí que se esté imponiendo a todos los niveles en relativamente pocos años. Abarca las transacciones comerciales electrónicas, compraventas de bienes y prestación de servicios, incluidas las negociaciones previas y posteriores a dichas transacciones.

Entre las ventajas de los nuevos escenarios de contratación: mayor competitividad, comodidad, rapidez y abaratamiento de costes..., que redundan en beneficio de las partes contratantes, sean éstas empresarios o consumidores.

Para las empresas: acceso al mercado mundial con una inversión mínima, pudiendo ofrecer productos-servicios a precios competitivos, pues reducen costes.

También encontramos desventajas: fallos y riesgos producidos por los propios equipos y sistemas electrónicos utilizados, problemática de carácter jurídico que demanda soluciones normativas *ad hoc*, de carácter global, en torno a cuestiones fundamentales como: la validez y eficacia de los contratos electrónicos sin el soporte del papel y sin el acompañamiento de la firma tradicional manuscrita (problema de la prueba), la determinación del momento y el lugar de perfección del contrato, la distribución de riesgos y la delimitación de responsabilidades entre los sujetos intervinientes, y la ley aplicable y la jurisdicción competente en caso de litigio, entre otras.

El comercio electrónico ha ido implantándose en los distintos ordenamientos jurídicos, en un primer momento sin regulación expresa, tanto de la mano de la interpretación doctrinal y jurisprudencial (así ha sucedido con la admisión de medios de comunicación electrónica -tales como el fax o el e-mail- para estipular el contrato o con los

documentos electrónicos como prueba del contrato), como el pacto entre las partes.

La coordinación del comercio electrónico con el Derecho ha vivido una segunda etapa con la creciente preocupación de distintas entidades y organizaciones por dotar a éste de reglas, que ha propiciado la progresiva aparición de regulación tanto a nivel nacional como supranacional.

La Unión Europea ha mostrado su preocupación por el comercio electrónico en épocas tempranas, bien de forma indirecta, a través de las Recomendaciones en materia de tarjetas de pago y medios de pago electrónicos, como de forma directa mediante la Comunicación sobre Iniciativa europea en materia de comercio electrónico; las Directivas sobre protección de los consumidores en los contratos estipulados a distancia, la Directiva sobre protección de los consumidores en los servicios financieros prestados a distancia, la Directiva sobre firma electrónica o la Directiva sobre comercio electrónico. [1]

También la Organización para la Cooperación y el Desarrollo, preocupada por la protección de los consumidores, y la Cámara de Comercio Internacional, son partícipes de esta disciplina. Especial relevancia ha jugado la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, primero con la regulación del EDI y posteriormente a través de la Ley Modelo sobre comercio electrónico y su Guía Jurídica, puesto que ha impulsado e inspirado la regulación nacional en distintos Estados. La regulación ha llegado a nuestro ordenamiento, plasmándose en el Real Decreto-Ley sobre firma

[1] Peces Barba, G. "Derecho del Comercio electrónico", La Ley, Biblioteca de los negocios, 2001

electrónica y su norma de desarrollo e, indirectamente, en la nueva Ley de Enjuiciamiento Civil.

En el campo del Derecho Privado, en particular del Derecho Mercantil, tales cambios son especialmente significativos por las importantes consecuencias que están llamados a producir; por ejemplo, una nueva concepción del comercio y la contratación.
La normativa vigente tiene carácter fragmentario pues, por lo general, contempla aspectos parciales del comercio electrónico y sólo resultan aplicables en ámbitos territoriales concretos (estrictamente nacionales o más extensos como la CE).

Los contratos mercantiles que se realizan a través de Internet, siendo en buena medida los mismos que se venían realizando por los medios tradicionales, presentan unas particularidades propias que dan lugar a un proceso especial del contratación, distinto de los hasta ahora conocidos por nuestra práctica comercial.
Como queda esbozado en los párrafos anteriores, estamos ante un fenómeno de la máxima relevancia, no solo por los resultados económicos que representa sino también por la amplia problemática que suscita su práctica y desenvolvimiento en este entorno virtual, en un ámbito intangible y desterritorializado, y en el que, a pesar de los avances, la materia adolece todavía de una regulación legal fragmentaria.

Siendo, como son, innumerables las virtudes y ventajas de este "mercado global", hace tan solo unos meses que nos ha presentado los inconvenientes más graves del sistema, pues la desestabilización de la economía a nivel mundial ha inmerso al planeta en una crisis profunda que está haciendo imprescindible replantear el Sistema económico mundial. Como explica con simplicidad y elocuencia Don Leopoldo Abadía en su libro “La crisis NINJA y otros misterios”, el dinero de un señor

de un pueblo perdido de Extremadura puede ser prestado en algunos segundos a un señor "poco solvente" en Idaho (EEUU) para que se compre una casa; y mientras que aquél pensaba que dejaba su dinero en un fondo garantizado que le iba a reportar algunos beneficios, se encuentra en estos momentos con que ha perdido todo su capital, y parece que nadie sabe dónde está.

La grave situación económica actual no hace "mala" en sí misma la globalización, ni las nuevas tecnologías, pero sí que deja en evidencia la necesidad de mayores controles de la actividad económica por parte de los Estados para contrarrestar las carencias y aspectos negativos que nos ha demostrado el nuevo sistema. Como afirmó Keynes “los mercados no se autocorrigen, o al menos, no lo hacen en un marco temporal relevante”. Subsiste, pues, la necesidad de que el legislador intervenga imponiendo soluciones que sean más eficientes que las del mercado[2]. Evidentemente, esas limitaciones exigen una coordinación entre los gobiernos a nivel mundial, ya que en el ámbito de Internet las fronteras se hacen muy difíciles de definir y mucho más complicadas de controlar.
Igualmente sería oportuno aprovechar la coyuntura para intentar soslayar el riesgo de asimetría o desigual alcance que el proceso de globalización está teniendo en los distintos países y latitudes, proceso que, de no corregirse llevaría a acentuar aún más las ya alarmantes diferencias entre países ricos y pobres.

Paradójicamente, y aunque en estos momentos parece que nadie tiene claro todavía el camino a seguir, se está pidiendo a los Gobiernos que regulen los mercados con normativa convencional internacional, acuerdos efectivos y mayores mecanismos de control, en una época en la que exigimos cada día mayores libertades y autonomía a todos los

[2] Cfr. F. VINCENT CHULIÀ, Introducción al Derecho Mercantil, cit., p. 716

niveles.
Es de desear que esta situación no degenere en una merma los Derechos y libertades logrados a lo largo de la Historia de la Humanidad, y que se han ido plasmando en documentos como la Declaración Universal de Derechos del Hombre, ... , o, en fechas más recientes, Ley de Protección de datos de carácter personal.

No obstante, considero que debemos ser optimistas y apostar decididamente por el perfeccionamiento, tanto técnico como legislativo, del entorno electrónico de Internet, puesto que, sin duda, ofrece muchas más ventajas que inconvenientes.

***

En cuanto a la estructura de este trabajo, he de reconocer que me ha resultado un poco complicado limitar la avalancha de información e innovaciones de todo tipo que descubro cada día, y que, casi siempre, me parecen muy interesantes.
Me resulta fascinante que, por ejemplo, los carteros de la India, vayan por las casas repartiendo el correo y faciliten a los vecinos (muchos de ellos analfabetos) la posibilidad de emitir correspondencia electrónicamente escribiendo en una tablilla sus mensajes, que son a su vez recibidos de forma inmediata en administración de correos de la ciudad de destino, donde se los hacen llegar al destinatario; o la posibilidad de recibir o impartir clases particulares a distancia, a través de la Red, con una comunicación "virtualmente" presencial, directa e inmediata; los diagnósticos médicos a distancia; el control de fronteras europeas gracias al pasaporte digital, el voto electrónico y tantas otras.

Con todo, da un poco de miedo estar tan controlado.
Me permito en este punto comentar una pequeña anécdota personal, que creo viene al caso e ilustra un poco cuánto están cambiando

nuestros hábitos "gracias" a las nuevas tecnologías:

A principios de este año acudí a las oficinas del polideportivo al que voy habitualmente para renovar la suscripción anual. Mientras esperaba a que me atendieran pude ver carteles en todas las paredes ofreciendo la TARJETA ONA[3] ¡INFÓRMESE!. Y, yo, muy obediente, me informé. En resumen, se trata de una nueva tarjeta (como una de crédito con su "chip"), que se puede solicitar -de momento es opcional y gratuita- al Gobierno Vasco y que sustituye a la tarjeta sanitaria, a mi tarjeta del polideportivo, con ella puedo acceder a todas las bibliotecas de Euskadi, incorpora firma electrónica certificada, ... Después de recibirla se han ido incorporando nuevas opciones de uso, como por ejemplo, tramitaciones en la Diputación Foral de Guipúzcoa (la "madre" Hacienda, entre otras cosas), consulta de puntos del carnet de conducir, de la vida laboral, de datos catastrales, ... Con cada una de las incorporaciones de uso en mi tarjeta ONA, me han ido retirando las tarjetas antiguas y actualizando mis datos personales en cada una de sus bases de datos. Lo cual es muy práctico, supongo, porque la cartera me abulta mucho menos, pero me hace pensar que una gran parte de mi vida va quedando registrada en ese pequeño chip, y que debe ser muy fácil saber cuándo me han recetado medicamentos, cuándo estaba “haciendo unos largos” en la piscina, o los libros que he tomado prestados de la biblioteca.

En estos aspectos deberá demostrar su efectividad la aplicación de la Ley de protección de datos de carácter personal.

Volviendo al esquema de este trabajo, he optado por analizar las fases habituales de las relaciones comerciales en el entorno electrónico, comenzando por definir dicho entorno (Internet), para luego analizar las peculiaridades del proceso desde que una empresa anuncia sus

[3] Web oficial del Gobierno Vasco: www.euskadi.net/ona

productos hasta que finaliza la relación comercial.
En cualquier caso, y visto el ritmo vertiginoso de las innovaciones en este ámbito del comercio electrónico, asumo que esta información quedará obsoleta en muy poco tiempo.

Respecto a las fuentes de información utilizadas, la mayor parte de los datos los he obtenido a través de las webs oficiales de la Comunidad Europea o de los Ministerios españoles correspondientes, de la Diputación Foral de Guipúzcoa o del Gobierno Vasco; de la Asociación Española de Comercio Electrónico, y otras muchas que detallo en el apartado de "Bibliografía". También me han resultado de gran ayuda la "Guía del Comercio Electrónico de 2008", de la Editorial Anaya, "Formación y Perfección del Contrato en Internet" de Ángela Guisado Moreno, o "Teletrabajo y comercio electrónico" de Biblioteca de Derecho de los Negocios, entre otros.

2. INTERNET: CONCEPTO Y ASPECTOS BÁSICOS

Sin pretender realizar un análisis exhaustivo de lo que es Internet, incluyo algunas anotaciones previas que ayuden a definir el concepto de Comercio Electrónico.

Resulta difícil establecer una única definición de Internet puesto que posee numerosas dimensiones:[4]

a) Internet es una red informática que utiliza las líneas telefónicas,

[4] Rodrigo González, Oscar: "Guía práctica del Comercio electrónico", Editorial Anaya, 2008.

microondas, satélites, etc., y es capaz de conectar entre sí miles de ordenadores de todo el mundo.

Posee una jerarquía de tres niveles formados por redes de eje central (*backbones*), redes de nivel intermedio y redes aisladas (*stub Networks).* Es una red informática global que conecta redes locales alrededor del mundo empleando un mismo lenguaje o protocolo.

Un protocolo es una descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. De hecho, un aspecto clave de la expansión de Internet lo constituye la capacidad para compartir información y el acceso libre y abierto a los documentos básicos, especialmente a las especificaciones de los protocolos. El protocolo generalmente aceptado es el TCP/IP (*Transmission Control Protocol/Internet Protocol).*

b) Es un conjunto de recursos y herramientas a los que se tiene acceso.

Es una amplia fuente de información que cambia y se expande constantemente, y a través de ella se puede enviar y recibir instantáneamente, a través de todo el mundo, cualquier tipo de información, imagen, o sonido.

El sistema permite que la red continúe operativa aunque algún equipo falle, ya que los paquetes de datos pueden tomar otro camino para llegar a su destino. Así, Internet es una red "democrática" en la que todos los equipos tienen la misma importancia, lo que permite que no posea dueño sino sólo una serie de normas técnicas y de buen uso que se espera sigan todos los usuarios.

c) Es una comunidad de personas (físicas y jurídicas) que se sirven de ella para realizar diversas tareas.

Desde su creación en los años 60, ha crecido enormemente y en la actualidad es utilizado por empresas, consumidores individuales

o instituciones gubernamentales, comerciales o educativas. Su utilización sigue creciendo rápidamente debido a la reducción de los costes, los constantes avances tecnológicos y la creciente necesidad de información y comunicaciones.

2.1. La Red de redes. El sistema de nombres de dominio [5]

Un dominio es el conjunto de caracteres que identifican un sitio de Internet accesible por un usuario. El Sistema de Nombres de Dominio permite dirigir la información a un nombre de dominio, cuyo servidor se encarga de traducir la correspondiente dirección de IP de cada equipo, siendo IP la representación numérica de la localización de un ordenador dentro de una red que utiliza el Protocolo de Internet (IP).

Se distinguen tres niveles:

1. Dominio de nivel más alto o TLD. En un nombre de dominio, la parte del nombre que aparece la última a la derecha, por ejemplo xxx.es (sería "es"). Dentro de este nivel los hay de dos tipos:

a) genéricos, internacionales o TLD, que son los dominios básicos. A su vez pueden ser abiertos (.com, .net, .info, .name, ...) o restringidos, ideados estos últimos para el uso exclusivo de comunidades o grupos (.edu, .gov, .museum ...).

b) geográficos o territoriales o ISO-3166 TLD. Son utilizados por organizaciones que desean establecerse en Internet o que quieren proteger la identidad de su marca o nombre

[5] Rodrigo González, Oscar: "Guía práctica del Comercio electrónico", Editorial Anaya, 2008.

comercial en un país o territorio concreto (.es, .fr, .uk, .eu, ...).

2. Dominio de segundo nivel o *Second Level Domain***.** Es la parte del nombre de dominio que aparece inmediatamente a la izquierda del *Top Level Domain: uned.es " uned".*

3. Dominio de tercer nivel o *Third Level Domain***,** corresponde al siguiente nivel jerárquico después de los dominios de segundo nivel. Es la porción de nombre del dominio que aparece dos segmentos a la izquierda del Top Level Domain: licenciaturas.uned.es "licenciaturas"

2.2. **Problemática** [6]

Un hecho que está provocando un gran número de litigios, es el mercado ilícito en relación con los nombres de dominio, no sólo los relativos a la actividad especulativa de los *ciberokupas*, sino al uso indebido de marca, a pretensiones concurrentes, coacciones a través del contenido, venta de dominios caducados, dilución de marca culposa, etc.

El sistema de nombres de dominio se emplea en Internet para identificar unívocamente a los equipos conectados a la red a través de nombres, en lugar de números que son más difíciles de memorizar, distribuidos en muchos servidores por toda la red a través de una gran base de datos

[6] Rafael Illescas y Otros, "Derecho del Comercio electrónico", La Ley, Biblioteca de los negocios, 2001

jerárquica.

Los dominios genéricos están controlados y regulados por el ICANN (*Internet Domain Name Process)*. En España el dominio es ".es" y está regulado por la Orden de 21 de marzo de 2000, que da una razonable protección para los propietarios de marcas y denominaciones sociales.

El dominio genérico ".com" está saturándose ya que es internacional y admite una única asignación por nombre (empresa), aunque seguramente hay cientos en todo el mundo que tienen la misma denominación o acrónimo. Así, los dominios empiezan a verse como marcas, lo que ha propiciado el nacimiento de los piratas, ladrones de dominios, *cibersquatters* o ciberokupas, personas que registran nombres correspondientes a personas famosas o marcas notorias o que puedan serlo, con objeto de especular con ellas y en algunos casos se producen con extorsión, coacción, competencia desleal, dilución o denigración de la marca, haciendo muchas veces chantaje con contenidos pornográficos. Una variante del ciberokupa es el typosquatter, que consiste en registrar variantes de dominios existentes a los cuales el internauta puede acceder por equivocación al escribir erróneamente el dominio original. Así este *cibersquatting* provoca procedimientos ilícitos y comisión de delitos.

2.3. **Soluciones**

Algunas instituciones internacionales como la OMPI[7] han intentando solventar los conflictos que plantea la utilización de marcas en Internet, ya no sólo desde el punto de vista de los conflictos de marcas-nombres de dominio, sino desde el plano amplio de las marcas en Internet.

[7] OMPI: Organización Mundial para la Propiedad Intelectual

En la Conferencia Internacional de la OMPI de 1999, se abordaron ya algunos de estos problemas proponiéndose, entre otras:

- La protección de las marcas en Internet en virtud de la legislación pertinente de cada Estado miembro, previendo también la necesaria coexistencia en Internet de los derechos de marcas previstos en las legislaciones de varios Estados, rompiendo así la territorialidad (básica en Internet).
- Fijaban un criterio de vinculación de un acto de utilización de marca en Internet con el Estado miembro en el que se haya producido el efecto comercial. A este respecto ofrecieron varios factores, no tasados, para su determinación:
    - La atención a clientes del territorio en cuestión
    - El establecimiento de relaciones motivadas por el comercio con personas del país en cuestión
    - Visitas efectivas al sitio web para el que se utiliza el signo o en el que éste es utilizado por personas procedentes de dicho Estado
    - Utilización de un dominio de nivel superior que corresponda a un código de país de la Norma ISO 3166
    - La indicación de precios en una moneda nacional determinada
- Recogía el descargo de responsabilidad como vía para evitar la infracción, incluyendo en el sitio web una referencia a que el signo no se utiliza en relación con un Estado miembro determinado y que los productos o servicios ofrecidos no están disponibles allí.
- Con respecto a los nombres de dominio, se han elaborado una serie de recomendaciones:
    - Se elaboró un catálogo de *Best Practices* a seguir por los Registros de Internet.
    - Se propuso un procedimiento de resolución de disputas para que fuera adoptado por ICANN.

- También se propuso un sistema de exclusión de las marcas notorias y renombradas, en virtud del cual los titulares de las mismas podrían obtener la exclusión en los nuevos gTLDs para evitar el registro de nombres de dominio idénticos en un amplio campo geográfico y para diferentes clases de productos o servicios.

Otras instituciones junto a la OMPI han abordado esta problemática. El IAHC (*International Ad Hoc Committee*), creado para solventar los problemas de administración de Internet y registro de nombres de dominio, adoptó en el *Memorandum of Understanding on the generic top-level domain name space of the Internet Domain Name System* de 1997 algunos acuerdos, entre los cuales:

- Introducir nuevos gTLDs (.firm, .store, .web, .arts, .rec, .info, .nom, ...)
- Crear instituciones para la administración de los mismos
- Creación de procedimientos de resolución de conflictos relativos a los nombres de dominio

La Administración de los Estados Unidos no aceptó dichas propuestas y elaboró un informe (*Green Paper)* en el que detectaba, entre otros: la inexistencia de competencia en el registro de nombres de dominio, la ineficacia de las medidas de prevención y solución de conflictos entre nombres de dominio y marcas. Elaboraba, así mismo, una propuesta de reformas.

Posteriormente al *Green Paper* se redactó el *White Paper* recogiendo los comentarios al primero así como la respuesta del Gobierno estadounidense. Aparentemente, en el mismo se quería disminuir el nivel de presencia norteamericana en la gestión y gobierno de Internet, sobre todo por el desacuerdo de la Unión Europea, contraria con la primacía de EEUU en este contexto.

La Comisión de la Unión Europea realizó investigaciones al Gobierno de EEUU y a la empresa NSI por prácticas contrarias a la libre competencia. En noviembre de 1996, emitió un *Green Paper on a Numbering Policy for Telecommunications Services in Europe*[8] en el que criticaba la administración de Internet a través de una entidad privada de los EEUU, y abogaba por la introducción de dominios territoriales como ".eu".

En enero de 2000 la Comisión Europea elaboró un documento sobre *La creación del Dominio de Nivel Superior de Internet .eu,* cuya finalidad era crear un nuevo TLD para evitar su uso por particulares, empresas y organizaciones de la UE, y garantizar así un adecuado respeto de la legislación y de las políticas europeas.

En España, la Ley de Marcas en su artículo 31.2 establece dos vías por las que el titular de una marca nacional puede atacar un nombre de dominio idéntico o similar; establece el derecho del titular de la marca a prohibir la utilización de la misma para "ofrecer productos, comercializarlos o almacenarlos con este fin o prestar servicios con el signo"; también confiere al titular la posibilidad de prohibir la utilización del signo "en los documentos de negocios y la publicidad".[9]

Por su parte, los servicios de la OEPM (Oficina Española de Patentes y Marcas) se dirigen fundamentalmente a la consecución de:

- El reconocimiento y mantenimiento de la protección registral de las diversas manifestaciones de la propiedad industrial
- La difusión de la información tecnológica contenida en éstas.[10]

Se plantean otro tipo de litigios en el comercio electrónico, que son

[8] http://europa.eu.int/rn/record/green/gp9611/index.htm
[9] Isabel Ramos, Doctora en Derecho y Profesora de Derecho Mercantil, Universidad Carlos III de Madrid
[10] José López Calvo, Director de la OEPM Oficina Española de Patentes y Marcas

abordados más adelante en este trabajo.

3. COMERCIO ELECTRÓNICO

3.1. Definición

El desarrollo de las nuevas tecnologías, el avance de las telecomunicaciones en general y de Internet en particular, así como de los medios de transporte, nos acerca a un vasto mercado potencial, inimaginable en el comercio tradicional. Internet salva el obstáculo de las distancias, tanto físicas como temporales, anula las diferencias horarias, los tiempos entre la emisión y la recepción de un mensaje. Una página *web* se convierte en un escaparate en el que presentar cualquier producto, servicio o información en cualquier punto del planeta de manera casi instantánea. Esta nueva modalidad de comercio emplea para sus transacciones las redes de telecomunicación en sustitución del intercambio físico directo, sustituyendo el mundo físico por el mundo virtual.

Si se entiende el comercio electrónico como Intercambio Electrónico de Datos (EDI), éste surgió en los años 60 del siglo XX en EEUU con la idea de mejorar la calidad bien de los datos que se intercambiaban los proveedores de los sectores del ferrocarril o del automóvil, o bien de aquellos datos que se utilizaban en sus propias compañías. Una década más tarde, la Transferencia Electrónica de Fondos (EFT) favoreció el desarrollo y expansión de las telecomunicaciones para asuntos comerciales, en especial en la transferencia de giros y pagos; y más adelante la SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) para el intercambio de datos bancarios, así como el Sistema Nacional de Compensación electrónica y el Servicio Español de pagos interbancarios. No obstante, la implantación del EDI, en empresas medianas y pequeñas no fue tan extendida como se esperaba debido a los altos costes que se requerían para su

implantación[11], además de necesitar una tecnología de la información mayor de la que algunas empresas pequeñas tenían.

A pesar de ello, la perspectiva para el comercio electrónico cambia radicalmente con la explosión del fenómeno Internet de los últimos años.

Internet ha modificado profundamente la comunicación a nivel mundial, creado nuevas modalidades de ocupación y de valor económico, obligando a diferenciar entre Comercio Electrónico "tradicional" y comercio electrónico basado en Internet. Es, sin duda, la red comercial más grande que existe en el mundo.

En este contexto, se podría definir el Comercio Electrónico como el uso de redes (Internet) para realizar la totalidad de actividades involucradas en la gestión de negocios: ofrecer y demandar productos y servicios, buscar socios y tecnologías, hacer negociaciones con su contraparte, seleccionar el transporte y los seguros que más convengan, realizar los trámites bancarios, pagar, cobrar, comunicarse con los vendedores de su empresa, recoger los pedidos; es decir todas aquellas operaciones que requiere el comercio

Hacer comercio electrónico no significa solamente comprar cosas a través de Internet, sino la posibilidad de establecer una línea de comercio estable y realizar a través de medios electrónicos toda una conducta mercantil que incluye ofertas, pedidos, negociaciones, en general todo lo que es usual en el comportamiento de la vida mercantil, incluyendo los problemas legales que conllevan las transacciones de negocios en el entorno ajeno a lo electrónico. El comercio electrónico se sitúa así en un escenario abierto a todos y hace posible un sistema de información empresarial de extensión global en el que ninguna empresa

[11] ¿Qué es comercio electrónico? http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html

que ofrece bienes o servicios en la red tenga que dirigirse a un mercado definido según criterios geográficos.

Así mismo, los gobiernos de cada país modifican también su forma de funcionamiento al realizar sus compras y licitaciones utilizando la red e incluso muchos servicios a empresas y particulares. Liquidación de impuestos, trámites de pagos y cobros se hacen ya directamente por el sistema de Comercio Electrónico.

La trascendencia de este cambio de perspectiva ha hecho que se vea en el comercio electrónico una verdadera revolución, y es indiscutible que está sufriendo un crecimiento de gran magnitud que, ni siquiera la actual crisis económica mundial parece que lo vaya a frenar.

Los potenciales de crecimiento son impresionantes.
La *Spanish eCommerce and Interactive Marketing Association* acaba de publicar el informe "e-commerce Market Spain 2009" en el que ofrece los siguientes datos:

Potencial de Internet en lengua española:

- El español es la tercera lengua más utilizada en Internet (detrás del inglés y del chino)
- Hay 113 millones de usuarios hispano-parlantes: 9% mundial
- Desde el año 2000 ha crecido un 360%

¿Presencia o ausencia?

- Internet se ha convertido en un modelo basado en los motores de búsqueda. En España Google tiene un 98% de participación en el mercado.
- Los negocios con presencia *no online* se están convirtiendo en invisibles debido a que no es posible buscarlos.
- Sin embargo, sólo el 12.2% de las empresas españolas tiene una página web.
- Sólo el 9.8% de las Empresas españolas con más de 10 empleados y el 2.2% de la Empresas con menos de 10 de empleados vende

en Internet.

Por ello, concluye con la afirmación de que: *"La presencia online es un primer paso inevitable para acceder al Mercado".*

Internet en España: índice de penetración:

- España se encuentra en el puesto número 15 del ranking mundial en penetración en Internet con casi un 51% del total de la población. Este porcentaje está por debajo de la media de la Unión Europea (60%).
- Más del 75% de los usuarios de Internet se conectan desde sus casas.
- La mayor parte del tiempo utilizado se reparte en búsquedas y en el uso del correo electrónico.
- Las redes sociales son las actividades que más rápidamente están creciendo en la actividad online.

E-commerce en España:

- El mercado español tiene, en su territorio, 20 millones de potenciales compradores online.
- En 2008 los ingresos obtenidos en el modelo B2C (Business to Consumer) se estiman en 6.400 millones de Euros, un incremento del 42% sobre 2007 (más de 4.500 millones de Euros).
- El 49.6% de los usuarios de Internet han comprador algo online en 2008. Cerca de 10 millones de personas compraron online en 2008.
- La media anual de gasto en 2008 fue de 625 € por comprador (595 € en 2007)

E-commerce en Hispanoamérica. Mercados emergentes:

- América Latina es un área geográfica con mucho potencial.
- América Latina tiene el 8% de los usuarios del planeta. Sin embargo, cuenta sólo con el 3% de los compradores de Internet (únicamente el 15% compra en Internet).
- Solamente hay un mercado significativo en Brasil, México y Argentina. La mayoría de las ventas en América Latina están

hechas en tiendas online situadas en USA.

3.2. ANALISIS

Puntos Fuertes	**Puntos Débiles**
- Competitividad del canal *online* - Largo recorrido del nicho del modelo de negocio	- Baja penetración de Internet entre usuarios y empresas - Baja confianza del consumidor
Oportunidades	**Amenazas**
- Mercado español potencial de 450 millones - Múltiples sectores en los que integrarse y crecer	- Estrictas leyes de protección de datos personales - Recesión económica y políticas fiscales y de impuestos

Fuente: www.aecem.org (César Tello). Original del documento en inglés, traducción propia.

Por otra parte, y abundando en la relevancia del Comercio Electrónico en la actividad económica española, incluyo algunos datos aportados por la Comisión del Mercado de las Comunicaciones en el INFORME SOBRE EL COMERCIO ELECTRÓNICO EN ESPAÑA A TRAVÉS DE ENTIDADES DE MEDIOS DE PAGO (IV Trimestre 2008), que ha publicado recientemente:

• En el cuarto trimestre de 2008, el comercio electrónico en España alcanzó un volumen de negocio de 1.248,7 millones de euros, un 22,2% más que en el mismo trimestre de 2007; con un total de 17,2 millones de operaciones.

• El volumen de negocio acumulado en el año 2008 del comercio electrónico en España, logró la cifra record de 5,2 millones de euros, registrando un crecimiento anual del 39%.

• El montante económico generado en el cuarto trimestre se distribuyó principalmente entre las siguientes diez ramas de actividad: transporte aéreo (10,1%), marketing directo (9,7%), agencias de viaje y operadores turísticos (9,2%), juegos de azar y apuestas (7,1%), transporte terrestre de viajeros (6,5%), espectáculos artísticos, deportivos y recreativos (5,9%), servicios legales, contabilidad y gestión (4,3%), educación (4,1%), electrodomésticos, radio, televisión y sonido (3,2%), y por último, ordenadores y programas informáticos (3,1%).

• En el cuarto trimestre de 2008, el volumen de negocio de las transacciones con origen en España y dirigidas hacia el exterior fue de 581,8 millones de euros, representando el 46,6% del importe total, con 8,2 millones de operaciones. La mayor parte del importe de dichas compras se dirigió a la Unión Europea con 508,2 millones de euros (87,3%) y en menor medida a Estados Unidos con 42,1 millones (7,2%) y al área C.E.M.E.A. con 16,2 millones (3,1%).

• El importe de las transacciones realizadas desde el exterior y dirigidas a sitios web españoles fue de 146,9 millones de euros, lo que supuso un 11,8% del volumen de negocio total, con 1,9 millones de operaciones. Las transacciones procedentes de la Unión Europea representaron la mayor parte del importe del volumen de negocio (68,0%), con 99,8 millones de euros, seguidas de las procedentes de Estados Unidos (14,9%), con 21,8 millones de euros, situándose Asia - Pacífico en tercer lugar con 9,4 millones de euros (6,4%).

• Estas cifras situaron el saldo neto de volumen de negocio con el exterior en una cifra negativa de 434,9 millones de euros.

• La cifra de negocio del comercio electrónico generado en España y dirigido a puntos de venta virtuales dentro del país fue de 520,1 millones de euros, el 41,6% del importe total, con 7,1 millones de operaciones.

3.3. NECESIDAD DE REGULAR JURÍDICAMENTE EL COMERCIO

Los actos de comercio, cualquiera que sea su alcance y contenido, requieren de, como mínimo, una regulación jurídica, ya que solamente a través de la observación de los preceptos jurídicos, estos actos pueden tener certeza, confiabilidad, reiteración y permanencia entre las partes y entre las naciones. Es por ello que los diferentes gobiernos se han preocupado por dar a los actos de comercio normas legales necesarias para que, por una parte, el comercio exterior de un Estado determinado se transforme en factor de progreso y desarrollo de sus propios intereses y, por la otra, para que queden garantizados los derechos y las obligaciones de las partes que intervienen en la celebración de estos actos, los cuales se llevan a cabo a través de un acuerdo de voluntades regulando por dichas normas jurídicas.

El desarrollo del Comercio Electrónico en España se ha visto favorecido por algunos factores que conviene destacar:

a) La Unión Europea ha seguido una política activa favoreciendo la Sociedad de la información.

   Ya en el Libro Blanco de Delors en 1993[12] se manifestaba que: "El principal cometido de la UE es mantenerse en el filo de la sociedad global interconectada y hacer lo necesario para que los ciudadanos europeos puedan recoger sus beneficios". Se hace una reflexión profunda, de carácter político, que va a permitir la interpretación económica y social de Europa dentro de la sociedad informacional, basando el crecimiento, la competitividad, el empleo y un nuevo modelo de desarrollo económico, en los siguientes aspectos:

[12] *Libro Blanco sobre Crecimiento, competitividad, empleo, retos y pistas para entrar en el s. XXI.* Com(93)700 Final

a. Desarrollo de las Tecnologías de la Información y la Comunicación de Europa.

b. Liberalización de las telecomunicaciones europeas

c. Sensibilización en el ámbito de la información dentro de las distintas naciones europeas.

d. Apoyo a la pequeña y mediana empresa (PYME)

e. Mayor protagonismo político europeo en el entorno mundial.

En el Informe Bangeman[13] se materializaban empresarialmente las ideas sociales de Delors respecto a Europa, intentando aprovechar al máximo los puntos fuertes de la UE. En dicho estudio de alto nivel, se desarrollan las líneas de la interconexión e interoperatividad tecnológica, la aparición de una masa crítica, la protección de los derechos de Propiedad Intelectual, y el fortalecimiento de las redes y acelerar la introducción de nuevas aplicaciones telemáticas, todo ello con el objetivo de controlar los riesgos y optimizar los beneficios de la Sociedad de la Información en nuestro continente, el cual posee un gran potencia en el sector industrial de los contenidos.[14]

b) 1998 fue un año de continuidad en la liberalización de los mercados de las telecomunicaciones, con el consiguiente incremento de consumidores y negocios en Internet y en los accesos *on line* a diversos servicios.

---

[13] *Europa y la Sociedad global de la información. Recomendaciones al Consejo Europeo.* Bruselas: Oficina de Publicaciones Oficiales de las Comunidades. 1984. (Informe Bangeman)

[14] Caridad Sebastián, Mercedes, "TELETRABAJO Y COMERCIO ELECTRÓNICO EN LA SOCIEDAD DE LA INFORMACIÓN",. Edit. Centro de Estudios Ramón Areces. Universidad Carlos III

c) El aterrizaje de nuevos medios digitales, como la televisión y los servicios web-TV ofreciendo la posibilidad de compras on-line.
d) La creación de la moneda única europea
e) El descenso en los costes de la tecnología.

Los legisladores europeos han intentado propiciar un marco de confianza en el Comercio Electrónico dictando Directivas, Reglamentos y Recomendaciones que ordenan distintos aspectos del mismo y, en particular, incrementando en lo posible la protección de un tipo específico de contratante, el consumidor o usuario, al que pretenden facilitar su circulación en el tráfico.

Entre ellos el Reglamento (CE) n° 460/2004, de 10 de marzo de 2004 por el que el Parlamento Europeo y el Consejo han creado la Agencia Europea de Seguridad de las Redes y de la Información para que actúe "como punto de referencia e inspire confianza gracias a su independencia, a la calidad del asesoramiento que preste y de la información que divulgue, a la transparencia de sus procedimientos y métodos de funcionamiento y a su diligencia a la hora de desempeñar las funciones que se le asignen, respondería a esas necesidades", ... "apoyándose en los esfuerzos realizados a nivel nacional y comunitario y desempeñando sus funciones cooperando con los Estados miembros y estar abierta a contactos con la industria y otros agentes interesados".
Son conscientes de que "Las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social "y de que la "seguridad de las redes de comunicación y de los sistemas de información, ... es un asunto que preocupa cada vez más a la sociedad" así como de "la posibilidad de que surjan problemas en sistemas de información claves, debidos a la complejidad de los sistemas, a accidentes, errores o ataques, que puedan repercutir en las infraestructuras físicas que prestan servicios esenciales para el bienestar de los ciudadanos de la Unión Europea". "El

número de fallos de seguridad es creciente y ha causado ya importantes perjuicios económicos, minando la confianza de los usuarios y perjudicado el desarrollo del comercio electrónico", por lo que en el Considerando 14 del Reglamento 460/2004 se busca asegurar la confianza mediante la información, educación y formación en materia de seguridad de las redes y de la información, de particulares, empresas y administraciones públicas.

Como consecuencia, el cometido fundamental de la Agencia es el de "contribuir al establecimiento de un elevado nivel de seguridad de las redes y de la información en la Comunidad, así como desarrollar una cultura de la seguridad de las redes y de la información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público en la Unión Europea, contribuyendo con ello al buen funcionamiento del mercado interior".

Otros aspectos que también han recibido una atención especial por parte de los legisladores, son los problemas de seguridad informática y de confidencialidad de documentos, la protección de los datos personales o el de los pagos a través de la Red.
A este respecto, comercio electrónico y sus tecnologías asociadas, empleadas con fines ilícitos o en circunstancias no regladas o criminógenas, adquieren una especial y potencial litigiosidad que afecta a todas las jurisdicciones: penal, civil, mercantil, fiscal, laboral, administrativa, etc.

Dentro de la jurisdicción penal, la acción u omisión específica, antijurídica y culpable, determina una serie de tipos delictivos en el comercio electrónico, como:

- La piratería informática
- Los virus
- Infracciones referidas a los datos de carácter personal y

patrimonial.

El delito informático contempla las TIC como medio o como fin en sí mismo.

- En el primer caso, su función será instrumental, sin que en algunos casos sea necesaria la tipificación de delitos o faltas que puedan aplicarse por analogía.

  Referido a los datos de carácter personal y patrimonial: las cookies (pequeños ficheros de datos que se generan a través de las instrucciones que los servidores web envían a los programas navegadores, y que se guardan en un directorio específico del ordenador del usuario) pueden recabar datos sin nuestro consentimiento; algunos servidores pueden vender las direcciones de sus clientes, los correos pueden contener virus, la obra intelectual puede ser violada, los accesos anónimos e ilegales a sistemas informáticos pueden distorsionar la autoría, la identidad declarada puede no ser real, pagos fraudulentos con dinero electrónico, copia, distribución y venta ilegal de software, etc.

- En el segundo supuesto, se trata de puro delito informático que tiene por objeto, por ejemplo, causar daños en el sistema informático (hacker), por medio de un virus informático introducido por correo electrónico.

También existe la problemática de los conflictos de marcas-nombres de dominio, a la que me he referido más arriba en el apartado de INTERNET-PROBLEMÁTICA. (Otos litigios que plantea el comercio electrónico).[15]

[15] Carlos Barriuso Ruiz, Abogado especializado en comercio electrónico

3.4. **Legislación**

En el siguiente cuadro se presenta una síntesis de la legislación actual vinculada al comercio electrónico:

ÁMBITO DE APLICACIÓN	NORMA
Firma electrónica	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 Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información
Ley / Jurisdicción	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) 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 LSSICE: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio

	Electrónico
Dinero electrónico	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
Contratación	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
Bases de datos	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
Intimidad	DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
Derechos de autor	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

Una serie de normas abrieron el camino de lo que sería conocido como marco jurídico del comercio electrónico.

En el ámbito comunitario, en la *Directiva 98/34/CE* del Parlamento Europeo y el Consejo, de 28 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. Modificada por la *Directiva 98/84/CE* del Parlamento Europeo y del Consejo de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso, aparece una definición de comercio electrónico que ha sido utilizada de manera constante en normas posteriores : "*cualquier servicio prestado normalmente a título oneroso, a distancia, mediante un equipo electrónico, para el tratamiento (incluida la compresión digital) y el almacenamiento de datos, y a petición individual de un receptor de servicio*".

En su Anexo V, se recoge una lista indicativa de servicios que no están incluidos en la definición anterior, de la que se puede deducir los que se consideran excluidos:

- Los servicios no realizados a distancia. Esto es, servicios realizados en presencia física tanto del proveedor como del receptor de los mismos, incluso si implican el uso de aparatos electrónicos.
- Los servicios no realizados por medios electrónicos, es decir servicios con un contenido material aunque hayan sido realizados con ayuda de aparatos electrónicos (por ejemplo, sacar dinero de un cajero automático o servicios que requieren de una entrega *off line (*sin utilizar Internet).
- Los servicios no realizados mediante un procedimiento electrónico o un sistema de inventario, como por ejemplo: servicios de telefonía vocal, telefax, télex, servicios realizados por teléfono o fax, consulta telefónica a un médico o a un abogado, marketing directo realizado por teléfono...

- Los servicios de transmisión de datos sin petición individual para una recepción simultánea por un número ilimitado de receptores individuales.

A la relación anterior hay que añadir, sin consideración de lista cerrada,

- las cuestiones fiscales y el IVA,
- los juegos de azar,
- la radiodifusión televisiva y la radiofónica,
- el uso del correo electrónico por parte de personas físicas que actúan fuera de su profesión, negocio o actividad profesional, incluso cuando los usan para celebrar contratos entre sí,
- servicios de control legal de la contabilidad de una empresa y asesoramiento médico

cuestiones que la *Directiva sobre el comercio electrónico* excluye de su campo de aplicación, por ser, estas dos últimas, actividades que requieren el reconocimiento físico.

Por el contrario, sí se incluyen servicios, aunque no sean remunerados por sus destinatarios, como aquellos que consisten en ofrecer formación en línea o comunicaciones comerciales, o los que ofrecen instrumentos de búsqueda, acceso y recopilación de datos.
Los servicios de la sociedad de la información cubren también servicios consistentes en transmitir información a través de una red de comunicación, o albergar información facilitada por el destinatario del servicio.

Así pues, la Directiva no llega a ofrecer propiamente una definición de comercio electrónico, ni a delimitarlo por razón de su objeto o sujetos. No obstante queda perfilado a través de dos vías: encuadrándolo como un "servicio de la sociedad de la información" y a través del implícito reconocimiento de dos modalidades de comercio electrónico: el que se realiza entre empresarios y/o profesionales y el que tiene lugar

entre éstos y los consumidores.[16]

El término "servicio de la sociedad de la información" no se refiere exclusivamente al fenómeno del comercio electrónico, sino que persigue un objetivo más amplio: garantizar la libre circulación de los servicios de la sociedad de la información en el ámbito del Mercado interior de los Estados miembros.

La Directiva sobre el comercio electrónico (*Directiva 2000/31 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), ha sido transpuesta, de manera prácticamente literal, a nuestro ordenamiento jurídico mediante la Ley 34/2002, de 11 de julio, *de Servicios de la Sociedad de la información y de Comercio electrónico (*en adelante: LSSICE*)*.

El objeto de esta Directiva es la del fomento del Comercio Electrónico, uno de los instrumentos elegidos para la efectiva realización del mercado interior europeo (artículo 2 del Tratado de la Comunidad Europea).
Se opta por una regulación de mínimos que deje a los Estados miembros la posibilidad de introducir variantes dentro del marco propuesto, ya que se pretende que el rápido desarrollo de las nuevas tecnologías no deje obsoleto en poco tiempo un marco regulador exhaustivo.

La *Directiva 97/7* del parlamento Europeo y el Consejo de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de

[16] Guisado Moreno, Ángela: "Formación y perfección del contrato en Internet", Marcial Pons.

contratos a distancia (antecedente de la Directiva del Comercio electrónico) pretendió garantizar un nivel mínimo de protección al consumidor, protegiendo a los compradores de bienes o servicios contra la solicitud de pago de mercancías no encargadas y contra los métodos de venta agresivos, entre otros aspectos. Aunque no se dirige específicamente al comercio realizado por medios electrónicos, sí adelanta algunas de las medidas que luego fueron reforzadas, como:

a. Se dispensa al consumidor de toda contraprestación en caso de suministro no solicitado, sin que la falta de respuesta pueda considerarse como consentimiento.
b. Se impone el requisito de información previa, con confirmación escrita o en soporte duradero, a la celebración de todo contrato a distancia sobre la identidad del proveedor, características esenciales del bien o del servicio, su precio, incluidos todos los impuestos y gastos de entrega en su caso, modalidades de pago, entrega o ejecución, coste de la 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 o del precio, y, cuando sea procedente, la duración mínima del contrato, cuando se trate de contratos de suministro de productos o servicios destinados a su ejecución permanente o repetida. Esta exigencia de información previa y de confirmación va a ser recogida y ampliada en la Directiva 2000/31 y se explica fácilmente si tenemos en cuenta que, por tratarse de una adquisición a distancia, el comprador no ha tenido la oportunidad de comprobar las características del producto, ni ha observado las instalaciones del vendedor de modo que le merezca confianza, ni tiene otro modo de verificar que el vendedor acepta su petición de compra.
c. Igualmente, y considerando que el consumidor no tiene la posibilidad real de ver el producto o de conocer las características del servicio antes de la celebración del contrato,

establece un derecho de rescisión. Gracias a éste, el consumidor dispone de un plazo mínimo de siete días laborables para rescindir el contrato sin penalización alguna y sin indicación de los motivos.

d. En caso de que el precio haya sido total o parcialmente cubierto mediante un crédito concedido por el proveedor o por un tercero previo acuerdo celebrado entre el tercero y el proveedor, el contrato de crédito quedará resuelto sin penalización en caso de que el consumidor ejerza su derecho de resolución.
e. Salvo pacto en contrario, el proveedor deberá ejecutar el pedido en un plazo máximo de treinta días a partir del día siguiente a aquel en que el consumidor le haya comunicado su pedido.
f. Así mismo, los Estados velarán porque existan medidas apropiadas para que el consumidor pueda solicitar la anulación de un pago en caso de utilización fraudulenta de su tarjeta de pago y para que en este caso se abonen en cuenta al consumidor las sumas abonadas en concepto de pago o se le restituyan. Las medidas que el Estado puede adoptar van desde la obligatoriedad para los establecimientos de verificar la identidad del comprador como titular de la tarjeta, ya en el mismo establecimiento de compra, ya, en nuestro caso en una página Web de la empresa, protegida mediante un dispositivo seguro. Este punto está especialmente sometido a los avances de la técnica y a las medidas técnicas de Seguridad del comercio electrónico.
g. Los Estados podrán adoptar o mantener disposiciones aun más estrictas, a fin de garantizar una mayor protección al consumidor, pero nunca menor.

Posteriormente el Consejo publicó la *Resolución del Consejo de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información*, por la que invitaba a la Comisión a que examinara la legislación vigente en la Comunidad y a que adoptara las medidas de iniciativa legislativa necesarias, teniendo en cuenta las

nuevas circunstancias en que los avances de las nuevas tecnologías habían colocado a la sociedad, en el campo de la protección de los consumidores.

En el mismo sentido de protección al consumidor, la Unión Europea había dictado ya en 1993 la *Directiva 93/13 del Consejo, sobre Cláusulas Abusivas en los Contratos Celebrados con Consumidores*, que supuso una novedad normativa para la protección del consumidor, y cuya trasposición en España se hizo a través de la *Ley 7/1998, de 13 de abril, "sobre Condiciones generales de la Contratación" (LCGC).* El objeto principal de éstas hacía referencia a las condiciones generales de los contratos, es decir, las cláusulas impuestas por el prestador de servicios a sus clientes y que estos tienen que aceptar para poder acceder a los servicios, ya que, normalmente, se trata de una empresa poderosa frente a la que el usuario no tiene posibilidad de negociación:

- la LCGC sanciona con la 'nulidad' las cláusulas generales no ajustadas a la ley,
- Determina la 'ineficacia por no-incorporación' de las cláusulas que no cumplan los requisitos exigidos para que puedan entenderse incorporadas al contrato
- Las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez.
- Cuando exista contradicción entre las condiciones generales y las condiciones particulares específicamente previstas para ese contrato, prevalecerán éstas sobre aquéllas, salvo que las condiciones generales resulten más beneficiosas para el adherente que las condiciones particulares
- Las dudas en la interpretación de las condiciones generales oscuras se resolverán a favor del adherente.
- No quedarán incorporadas al contrato las siguientes condiciones generales:

- o las que el adherente no haya tenido oportunidad real de conocer de manera completa al tiempo de la celebración del contrato o cuando no hayan sido firmadas, cuando sea necesario, y
- o las que sean ilegibles, ambiguas, oscuras o incomprensibles, salvo que, en cuanto a estas últimas, hubieren sido expresamente aceptadas por escrito por el adherente y se ajusten a su normativa específica.

Otras normas fundamentales en este campo como son:

- la *Directiva 1999/93/CE del Parlamento Europeo y el Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica*, y que fue a su vez transpuesta en el Derecho español mediante la *Ley 59/2003, de 19 de diciembre, de firma electrónica*, o
- la *Directiva 2002/65/CE del Parlamento Europeo y el Consejo de 23 de Septiembre de 2002 relativa a la comercialización a distancia de servicios financieros destinados a los consumidores),*

se analizarán separadamente en los epígrafes de Firma electrónica y Medios de pago.

Hay que destacar también el *Reglamento 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004*, en vigor desde el 29 de diciembre de 2005*, sobre la cooperación entre autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores* que pretende la cooperación entre autoridades públicas encargadas de la aplicación de la legislación con el fin de detectar, investigar y hacer cesar o prohibir las infracciones intracomunitarias a la legislación protectora de los intereses de los consumidores. Pretende fomentar el comercio electrónico transfronterizo, así como su eficacia, al facilitar la solución transfronteriza de litigios relativos al comercio electrónico.

3.5. Modalidades de comercio electrónico

El comercio electrónico implica la realización de la actividad comercial de intercambio asistida por las telecomunicaciones y herramientas basadas en ellas.

Esto supone un nuevo enfoque a la hora de entender la relación de intercambio entre comprador y vendedor. Consecuencia de esta definición, muchas tecnologías pueden ser usadas como apoyo del comercio electrónico, siendo mucho más que un fenómeno basado en Internet. No surge como consecuencia de la Red sino que abarca un amplio rango de tecnologías de comunicaciones, incluyendo: [17]

- EDI: Intercambio electrónico de datos
- EFT: Transferencia electrónica de fondos
- Tarjetas de crédito débito
- Soportes multimedia
- Fax
- Móviles
- Aplicaciones relacionadas con las redes de comunicación:
    - Correo electrónico
    - BBS: Tablones electrónicos de anuncios
    - Videoconferencia, etc.

En este contexto pueden interactuar organizaciones y clientes: el número de participantes es ilimitado y no tienen porqué ser conocidos. Las redes están abiertas y el acceso no está protegido, lo cual hace necesario el uso de medidas de seguridad y autentificación. El

[17] Rodrigo González, Oscar: "Guía práctica del Comercio electrónico", Editorial Anaya, 2008.

comercio electrónico se transforma en un fenómeno que afecta en igual medida a empresas, consumidores y administraciones públicas.

Se acostumbra a hacer una clasificación de las distintas modalidades o categorías de Comercio Electrónico en función del tipo de relación que se establece entre las distintas partes que pueden integrar el intercambio comercial.

La tabla que sigue recoge y contrapone las características de estos dos tipos de comercio electrónico:

COMERCIO ELECTRÓNICO TRADICIONAL	**COMERCIO ELECTRÓNICO BASADO EN INTERNET**
Sólo entre empresas	Empresas-consumidores Empresas-empresas Empresas-administraciones públicas Usuarios-usuarios
Círculos cerrados, a menudo específicos de un sector	Mercado mundial abierto
Número limitado de empresas participantes	Número ilimitado de participantes
Redes cerradas propias	Redes abiertas, no protegidas
Participantes conocidos y dignos de confianza	Participantes conocidos y desconocidos
La seguridad forma parte del diseño de la red	Son necesarias la seguridad y la autentificación
EL MERCADO ES UN CÍRCULO	**LA RED ES EL MERCADO**

Entre las diversas modalidades en las que puede realizarse el comercio electrónico encontramos las transacciones:

a. **B2B** Business to business: Supone la realización de intercambios comerciales entre proveedores y clientes intermediarios (no finales). En un modelo de producción Pull se hace necesario la continuidad del flujo de los aprovisionamientos para que la cadena de producción no quede estancada, así surge la Extranet en la cual una empresa está permanentemente en contacto con sus empresas proveedoras a través de terminales informáticos.

b. **B2C** Business to customer: Permite que los proveedores de productos y servicios orienten sus funciones hacia el usuario final y obtengan información al detalle acerca de los potenciales consumidores: quién accede, qué busca, cuánto tiempo utiliza, etc. Además con la utilización inteligente de estos datos, se está en disposición de ofrecer a los usuarios los paquetes exactos de bienes y servicios de cara a lograr un impacto efectivo.

c. **C2C** Consumer to Consumer**:** Los consumidores actúan como vendedores y compradores a través de una plataforma de intercamio. Las subastas son el modelo más extendido dentro de esta categoría, siendo "ebay" el ejemplo más destacado

d. **C2B** Consumer to Business: Un consumidor o grupo de ellos utiliza la Red de alguna forma para conseguir mejores condiciones en la oferta presentada por una empresa. El modelo más destacado de esta categoría es el de agrupación de compradores.

e. **Administraciones Públicas**

Internet está empezando a ser utilizado por las Administraciones públicas que, de esta forma, pueden actuar como agentes reguladores y promotores del comercio electrónico y como usuarias del mismo, por ejemplo, en los procedimientos de contratación pública o bien de compras.

Ejemplos de esta actividad:

- Servicios de la Administración a las empresas, y el cobro de impuestos

- Proveedores de bienes y servicios a las Administraciones. A este respecto hay que indicar la obligatoriedad de facturación electrónica por parte de los proveedores de la Administración a partir de septiembre de 2009.
- Difusión de información pública al ciudadano
- Pago de impuestos a través de la Red.

Resulta significativo que en el año 2007 la Hacienda Estatal española recibiera más de siete millones y medio de declaraciones a través de la Web, la mayoría de las cuales correspondían al IRPF. Ello supuso un aumento de casi el 70 por ciento.

En nuestro entorno cercano, también en Francia, en el año 2008 se superaron los 7 millones de declaraciones telemáticas de la Renta.

4. SUJETOS INTERVINIENTES EN LAS OPERACIONES DE COMERCIO ELECTRONICO

En los entornos electrónicos intervienen multitud de operadores económicos, aunque no todos ellos lo hacen a título de parte contratante.

4.1. Actores públicos y privados en la economía política del e-Comercio

Algunos gobiernos y organizaciones internacionales gubernamentales han sido actores políticos de primer orden en el comercio electrónico, adoptando políticas muy activas para la promoción del comercio electrónico en Internet y para el control de los riesgos asociados al acceso, a las redes y a la información.

Estados Unidos ha tenido y tiene una importancia decisiva en la medida

en que sin sus políticas gubernamentales no existiría ni el Internet que conocemos hoy en día ni el comercio electrónico que alberga. Junto a Estados Unidos, los países miembros de la Unión Europea han adoptado desde principios de los años noventa políticas nacionales y comunitarias también decisivas para la expansión de los mercados electrónicos y para el control de los riesgos presentes en ellos.

En la misma línea de promoción del comercio electrónico han participado activamente algunas organizaciones gubernamentales internacionales, entre las que cabe destacar:

1. Naciones Unidas:
    a. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo CNUCD
    b. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI
    c. Unión Internacional de Telecomunicaciones UIT
    d. Organización Mundial de la Propiedad Intelectual OMPI
2. Organización Mundial del Comercio OMC
3. Organización para la cooperación y el Desarrollo Económico OCDE

Por otra parte, la Comisión Europea ha aprobado la *Decisión 2005/752, de 24 de octubre, por la que se establece un grupo de expertos en comercio electrónico*. Este grupo de expertos estará compuesto por los puntos de contacto de cada Estado miembro definidos en la LSSICE, un miembro de cada Estado miembro, y por representantes de la Comisión que se reunirán habitualmente en los locales de la Comisión según las modalidades y el calendario que ésta establezca. La misión de este grupo de expertos es la de consulta voluntaria de la Comisión sobre cuestiones relativas a la Directiva del comercio electrónico incluyendo, entre otros, los ámbitos siguientes: la cooperación administrativa en el marco del procedimiento previsto para restringir la libertad de

prestación de servicios respecto de un determinado servicio de la sociedad de la información; la información sobre códigos de conducta elaborados a escala comunitaria; la jurisprudencia nacional, especialmente en materia de normas sobre responsabilidad, entre otros.

En el sector privado, diversos tipos de actores han influido en los mercados electrónicos y de muy diversas formas han contribuido a controlar los riesgos del comercio electrónico. Todos los actores privados que directa o indirectamente han tenido influencia destacable en la evolución de los mercados electrónicos pueden ser agrupados en tres grandes categorías: organismos técnicos, grupos activistas y empresas de la economía de la información.

Uno de los organismos técnicos más importantes en la gestión de Internet es la *Internet Corporation for Assigned Names and Numbers* (ICANN), que desde su creación en 1998 a instancia del gobierno estadounidense se ha convertido en una especie de "gobierno de Internet" gracias a sus actividades de gestión del sistema de nombres y números.

Otros organismos técnicos, completamente privados, también son en buena medida responsables de que Internet continúe siendo un medio de comunicación con una arquitectura abierta y de libre acceso, como la *Internet Society* y los organismos vinculados a ella: *Internet Architecture Board, Internet Engineering Task Force, Internet Engineering Steering Group, Internet Research Task Force e Internet Research Steering Group*. Todos ellos han velado por la preservación de los principios originarios de Internet y por el mantenimiento de estándares técnicos acordes con dichos principios, al igual que ha hecho el *World Wide Web Consortiun* en relación a la WWW.

4.2. Empresas de la Economía de la Información

En el comercio electrónico en Internet pueden distinguirse tres niveles de

actividad en los que se sitúan todas las empresas que operan en los mercados electrónicos.[18]

El primer nivel es el "físico", el nivel de las infraestructuras básicas que posibilitan la transmisión de la información a través de las redes de telecomunicaciones y entre los ordenadores interconectados. En él se ubican los operadores de telecomunicaciones, las empresas que mantienen y expanden las redes de telecomunicaciones.

1. El segundo nivel es el "lógico", el nivel del código informático que hace posible que los ordenadores puedan procesar e intercambiar información mediante protocolos y programas compatibles. En él se sitúan las empresas que fabrican equipos y componentes informáticos, las cuales operan en ocasiones también en el nivel del código informático.
2. El tercer nivel "lógico" o del código informático, donde se sitúa toda la información que es intercambiada mediante archivos, páginas web, etc., gracias al software del segundo nivel y al hardware y redes del primer nivel. Se encuentran las empresas de software, que cada vez ofrecen más productos y servicios del nivel de los contenidos

Estos tres niveles actúan de manera integrada haciendo que el sistema de comunicaciones funciones adecuadamente.

3. En cuarto lugar están todas las empresas de comercio electrónico propiamente dicho, entre las cuales se encuentran también empresas de hardware y de software.
4. A caballo entre el nivel del código informático y el nivel de los contenidos, se encuentran todas las empresas que ofrecen servicios estrechamente vinculados al comercio electrónico:

[18] Vid. LESSING, Lawernce (2001) The future of ideas, op. Cit. p. 23

provisión de acceso, sistemas de pago, certificación digital, protección informática, protección de la privacidad, selección de contenidos, alojamiento de páginas web y geo-ubicación, que además son, a menudo, ofrecidos por empresas de hardware y software.

Por tanto, operadores de telecomunicaciones, fabricantes de equipos y componentes informáticos, empresas de programas informáticos, empresas de comercio electrónico y servicios vinculados constituyen los sectores económicos en los que se encuentran los principales actores privados con poder y autoridad en el comercio electrónico.

5. EMPRESAS DE e-COMERCIO Y SERVICIOS COMERCIALES EN INTERNET

Un conjunto de empresas sustancialmente diferentes a las presentadas anteriormente es el formado por aquellas que realizan operaciones de comercio electrónico y aquellas dedicadas a ofrecer servicios para la realización de transacciones comerciales en Internet. Aunque en la mayoría de los casos son empresas con actividades al margen de los mercados electrónicos, algunas compañías concentran sus actividades en ellos o se dedican exclusivamente.

Las oportunidades de beneficio que ofrece el comercio electrónico están en el origen de la creación de empresas en línea y han llevado a muchas empresas tradicionales a vender y comprar sus productos en Internet. En los análisis microeconómicos suele distinguirse entre las empresas “puras” de comercio electrónico (creadas exclusivamente para hacer negocios en la red), y aquellas otras empresas tradicionales que han pasado parte de sus actividades a Internet. Esta distinción no resulta determinante para explicar por qué una empresa triunfa o fracasa en este entorno.

Estos sujetos (empresarios o profesionales) interactúan en el ámbito del B2B (*Business to business*), mientras que en el ámbito del B2C (*Business to consumers*) la relación se establece entre el empresario o profesional como prestador de servicios y el consumidor. Esta diferenciación de sujetos intervinientes está sujeta a distinta normativa, ya que la participación de consumidores está especialmente protegida en la legislación como parte considerada más débil en la relación contractual (aspecto que ya ha sido analizado más arriba).

En cuanto a las obligaciones de estos actores, me referiré a ellas en el apartado referente a la "Formalización de los contratos".

En resumen, la dinámica de la Red es asumida por cuatro actores:

1. Operadores: su función es proporcionar la infraestructura de telecomunicaciones necesaria para que funcione Internet.
2. Proveedores de conexiones: Enfocados, por un lado, hacia los usuarios de la Red, permitiendo el acceso a las múltiples posibilidades que ofrece Internet, desde aspectos meramente informativos a los más puramente comerciales. Por otro lado actúan en el ámbito empresarial ofreciendo a las empresas una vía para estar presentes en la Red; su oferta incluye la confección de las páginas Web, su implantación en el servidor y el acceso a Internet.
3. Proveedores de contenidos: son aquéllos que ofrecen la información y soportan la actividad económica en la Red. Constituyen la oferta específica dentro de Internet y los pioneros de un nuevo mercado. En este grupo se encuentran las instituciones oficiales, universidades, empresas de todo tipo e incluso particulares que ofrecen sus servicios *online*.

4. Usuarios: configuran el último escalón, la cúspide y sentido de la Red. Hacia ellos se dirigen las informaciones, ventas, transacciones, etc.

5.1. Régimen de responsabilidad de los prestadores de servicios [19]

Este aspecto está regulado por la Directiva 2000/31/CE 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), y por la **LSSICE**: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, que es una trasposición prácticamente literal de la Directiva.

La Directiva, en su artículo 2.b) define al prestador de servicios como: "cualquier persona física o jurídica que suministre un servicio de la sociedad de la información". Y en el apartado c) al prestador de servicios establecido: "prestador que ejerce de manera efectiva una actividad económica a través de una instalación estable y por un período de tiempo indeterminado. ..."

Establece también que los "Estados miembros no podrán restringir la libertad de prestación de servicios de la sociedad de la información de otro Estado miembro, salvo por razón de orden público, salud pública, seguridad púbica y protección de los consumidores (incluidos los inversores)

[19] "Dº de la contratación electrónica de R. Illescas Ortiz pp. 135; "Contratación y Comercio electrónico" 195-137: La responsabilidad civil de los intermediarios en Internet y otras redes, J Plaza Penades; "Derecho sobre internet" S. Cabanillas y R. Juliá, Libro electrónico, pp 8 ss "Los litigios que plantea el comercio electrónico: aspecto penal" en Dº del comercio electrónico pp 451-476.

La Directiva declara la limitación de la responsabilidad de los prestadores de servicios de intermediación, por el peligro que supondría el considerar que todos y cada uno de los titulares de los nodos de Internet que hubieran posibilitado que unos contenidos lleguen hasta el usuario final, fueran cooperadores en la conducta de comercio ilícito del que originó ese contenido. Ello determinaría un riesgo para la pervivencia del sistema de prestación de servicios por vía electrónica.

Así pues, los intermediarios que realicen actividades de mera transmisión, almacenamiento o alojamiento de datos no van a ser responsables, en principio, de los contenidos que manejen por cuenta de otros, salvo que alteren, falsifiquen o negocien ilícitamente con ellos, o bien no impidan su transmisión almacenamiento o alojamiento pese a conocer la ilicitud de dichos datos. Por tanto, de acuerdo con la LSSICE, quedan exonerados de responder de los contenidos que almacenan, puesto que legalmente no se les puede exigir que conozcan los contenidos, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos. No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión. Se precisa, así mismo, que las actuaciones de transmisión y provisión de acceso a que se refiere el apartado anterior incluyan el almacenamiento automático, provisional y transitorio de los datos, siempre que éste sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el "tiempo razonablemente necesario" para ello, concepto jurídico indeterminado, ya que no establece el tiempo considerado "razonablemente necesario".

No obstante, están obligados a:

1. Colaborar con los órganos públicos para la ejecución de las resoluciones que no puedan cumplirse sin su ayuda.

A este respecto, el artículo 11 dice: "*Cuando un órgano competente por razón de la materia hubiera ordenado (...) que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de los prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, podrá ordenar a dichos prestadores que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran. En todos los casos en que la ley atribuya competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo*".

La obligación de colaboración se convertiría en plenamente operativa con la existencia previa de una orden de cesación emanada de la autoridad competente (en su caso judicial) de la actividad de un tercero. Sin embargo, en la práctica, dicha obligación determina que el prestador de servicios de intermediación debe actuar como colaborador de la Administración y censurar contenidos o acceso cuando sea apercibido a ello, fijándose severas multas en el supuesto de falta de colaboración.

La LSSICE dedica su título VII al régimen sancionador administrativo, aplicable al prestador de servicios de la sociedad de la información. Divide las infracciones en muy graves, graves y leves, y para cada tipo recoge sus correspondientes sanciones administrativas, que consisten en multas que van desde menos de 30.000 € para las infracciones leves, hasta los 600.000 € máximos para las infracciones muy graves. Esta potestad sancionadora se ejercerá de conformidad con lo establecido al respecto en la *Ley*

30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.

Se consideran infracciones muy graves:

- el incumplimiento de órdenes dictadas, relativas a la restricción a la libre prestación de servicios; o
- el incumplimiento a la obligación de suspender la transmisión o el alojamiento e datos, en virtud del deber general de colaboración del artículo 11.

Son infracciones graves:

- el incumplimiento significativo de la obligación de ofrecer información general por el prestador; o
- el envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o más de tres en el plazo de un año sin cumplir los requisitos establecidos para el envío de comunicaciones electrónicas de la Ley; o
- el incumplimiento habitual de la obligación de confirmar la recepción de una aceptación.

Y son infracciones leves:

- la falta de comunicación al Registro público en que estén inscritos, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios;
- el no facilitar la información respecto a los trámites de contratación.

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses.

2. Retener los datos de tráfico relativos a las comunicaciones electrónicas, de acuerdo con lo que establezca el Reglamento de desarrollo de la Ley.

Para este supuesto, la Ley impone indirectamente al proveedor la obligación de retirar la información que haya almacenado o de hacer imposible el acceso a ella cuando tenga "conocimiento efectivo" de que un tribunal u órgano administrativo competente así lo ha ordenado. Haría falta, por tanto, que existiera resolución de cese de actividad previa para que surja la responsabilidad del proveedor intermediarlo.

Este "conocimiento efectivo" no viene definido por la Ley, y la situación es especialmente problemática en los buscadores que almacenan en su caché una copia de todas las páginas de Internet indexadas, copia que es llevada a cabo por programas robots y sin verificación de contenidos. Si la página de Internet de origen se modifica, o se retira por mandato judicial, el caché puede encontrarse en situación de ilegalidad sin que exista por parte del intermediario, ninguna intencionalidad. Este problema se habría evitado si se hubiera incluido en la Ley la necesidad de notificación formal de este tipo de resoluciones a los prestadores de servicios de memoria temporal.

Por otra parte, la LSSIC dedica la Sección segunda del Capítulo II al régimen de responsabilidad y prevé para los prestadores de servicios la sujeción a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico (Art. 1089 CC: "*Las obligaciones nacen de la ley, de los contratos y cuasi contratos y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia*".)

En los delitos y faltas que se cometan utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente.

Los autores, inductores, cooperadores en la ejecución a los que se refiere el artículo 28 de la LSSICE responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden:

1. Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo.
2. Los directores de la publicación o programa en que se difunda.
3. Los directores de la empresa editora, emisora o difusora.
4. Los directores de la empresa grabadora, reproductora o impresora.

"*Cuando por cualquier motivo distinto de la extinción de la responsabilidad penal, incluso la declaración de rebeldía o la residencia fuera de España, no pueda perseguirse a ninguna de las personas comprendidas en alguno de los números del apartado anterior, se dirigirá el procedimiento contra las mencionadas en el número inmediatamente posterior*" (*Art. 16 Alojamiento de datos (hosting vs. housing).*

El artículo 16 impone idéntica obligación de retirada o impedimento de acceso a los contenidos a los prestadores que desarrollan la función de alojar o albergar de forma estable datos ajenos, con la única particularidad de que, en este caso, la obligación de retirar o de imposibilitar el acceso a los contenidos surge para el prestador por el solo hecho de adquirir conocimiento de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, configurándose la eventual noticia relativa a la existencia de resolución de cese emanada de órgano competente como una más, entre otras posibles, de las vías por las que puede llegar a adquirirse el conocimiento de la ilicitud.

La definición incluye cualquier página Web, u otro servicio que permita que usuarios distintos del administrador incorporen contenidos.

Existe un mayor rigor en la regulación de la responsabilidad de este tipo de prestador dado que el grado de actividad y de conocimiento del

prestador respecto de los datos alojados se supone mayor en este último caso.

El Art. 17 propone la misma solución para el prestador que facilita enlaces a contenidos o a instrumentos de búsqueda. En principio, estos prestadores no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que no tengan conocimiento efectivo de la ilicitud de la actividad o de la información a la que remiten y, que si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace.

Tampoco será necesario que exista resolución de órgano competente previa que declare la ilicitud para que nazca la obligación indirecta de este prestador de cesación aunque, si existe ésta, surge una presunción *iuris tantum* de que ya existe conocimiento efectivo del prestador.

5.2. **Prestadores de servicios de certificación** [20]

La identidad en la Red está basada en la existencia de las terceras partes de confianza, que son las entidades que verifican y dan fe de la identidad de los internautas. Los Servicios de certificación son entidades cuyo fin es verificar la identidad y otros datos relevantes de una persona para que ésta pueda identificarse en la Red.

Existen diferentes entidades de certificación que emiten certificados de seguridad para personas, para empresas, para colectivos, para colegios profesionales, para universidades o para entes públicos.

Los certificados emitidos por cada prestador suelen estar vinculados a determinados colectivos de usuarios. Así, por ejemplo, un DNI electrónico emitido por la Policía será inicialmente aceptado para

[20] Ignacio Alamillo Domingo "Derecho del Comercio electrónico", La Ley, Biblioteca de los negocios, año

realizar trámites con la administración pública, mientras que un certificado emitido por un Colegio profesional será aceptado como instrumento electrónico que identifique al colegiado respecto a su actividad profesional, o un certificado de las cámara de comercio (Camerfirma) será aceptado por las empresas adheridas en sus transacciones comerciales.

Estas entidades, son la parte fiable que acredita la ligazón entre una determinada clave y el usuario propietario de la misma y actúan como una especie de notario electrónico que garantiza la veracidad de la información puesta en la red. En definitiva, son los órganos encargados de otorgar confianza en la infraestructura de las claves públicas, ya que resulta absolutamente necesario confiar en una tercera parte de toda solvencia que garantice la identificación de una persona física o jurídica a través de una clave pública.

La Ley 59/2003 de Firma electrónica establece en su art. 2.2 el concepto legal de prestador de servicios de certificación: " *la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica*", y extiende su aplicación a "*los Prestadores de Servicios de Certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España*".

La Directiva europea, por el contrario, contiene una concepción amplia de prestador, como se desprende del Considerando 9º de la misma, cuando establece que la "*firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con ella o que la utilicen. La definición de dichos productos y servicios no debe limitarse a la expedición y gestión de certificados, sino incluir también cualesquiera*

otros servicios o productos que utilicen firma electrónica o se sirvan de ella, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relativos a la firma electrónica". Definiendo en el artículo 2.11 de la Directiva al proveedor de servicios de certificación como: "la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica".

Los servicios de certificación podrán ser prestados tanto por instituciones públicas como privadas, sin que para ello deba solicitarse una licencia previa. El art. 4.1 del R.D. Ley establece, en consonancia con la Directiva europea, la necesidad de que la prestación de servicios de certificación se realice "*en régimen de libre mercado, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea*"

No obstante, conforme a los artículos 17 a 21 de la Ley 59/2003, los servicios de certificación deberán cumplir con los siguientes requisitos y obligaciones:

5.2.1. Obligaciones generales

Los Prestadores de Servicios de Certificación que deseen emitir cualquier clase de certificado, deberán cumplir las siguientes obligaciones de carácter general:

- comprobar la identidad y demás datos personales del solicitante
- facilitar al signatario el dispositivo de creación y verificación de firma
- no almacenar ni copiar los datos de creación de firma del solicitante
- antes de la emisión del certificado, deberán informar al solicitante sobre el precio, condiciones de uso y limitaciones del certificado

- mantener un registro público de los certificados emitidos
- en caso de cese de su actividad, deberán comunicarlo este hecho con la debida antelación (mínimo dos meses) a los titulares de los certificados
- estar inscritos en el Registro de Prestadores de Servicios de Certificación

5.2.2. Obligaciones específicas

Además de las citadas obligaciones generales, los Prestadores que emitan certificados reconocidos deberán cumplir las siguientes obligaciones específicas:

- indicar la fecha y hora de la expedición y/o revocación del certificado
- demostrar fehacientemente la fiabilidad de sus servicios
- garantizar rapidez y seguridad en la prestación de sus servicios
- contar con empleados cualificados para los servicios ofertados
- utilizar sistemas y productos fiables que garanticen la seguridad técnica de la certificación
- contar con medidas para prevenir la falsificación de certificados
- utilizar sistemas fiables y seguros de almacenamiento
- disponer de recursos económicos suficientes, que sirvan de garantía frente a una eventual responsabilidad por daños y perjuicios causados negligentemente -conservar durante un período de tiempo (generalmente 15 años) la información relativa al certificado emitido, para el caso de que dicha información pueda ser utilizada como prueba en algún procedimiento judicial o administrativo.

El conjunto de obligaciones citadas (generales y específicas) tiene como objetivo proporcionar seguridad y confianza en la prestación de los servicios de certificación y servir de garantía de calidad del servicio.

También el artículo 12, referido a las obligaciones impuestas a los prestadores que expiden certificados reconocidos, impone, entre otras, las siguientes obligaciones:

- Garantizar su rapidez y seguridad
- Asegurar la extinción o suspensión de la eficacia de los certificados de forma segura e inmediata
- Garantizar la confidencialidad durante el proceso de generación de los certificados.
- Garantizar la seguridad técnica y fiabilidad de los sistemas y productos.

En este mismo sentido, el art. 6 de la Ley 14/1999 crea los "sistemas voluntarios de acreditación de los Prestadores de Servicios de Certificación", que no son más que procedimientos totalmente voluntarios y compatibles con la libre constitución de una entidad como prestador de servicios de certificación, si bien está sujeta a una tasa establecida en el art. 23.*c* de la Ley.

Existe también un Registro público de prestadores en el Ministerio de Justicia, en el que deberán solicitar su inscripción con carácter previo al inicio de la actividad todos los establecidos en España (art. 7.1 de la Ley), cuya función es meramente declarativa (no constitutiva).

En cuanto a los derechos y facultades de los Prestadores de Servicios de Certificación, son los siguientes:

1. <u>Derecho a homologar, revisar y auditar</u>

   Los prestadores suelen reservarse el derecho a homologar a las personas con las que colaboran, bien como parte del proceso de admisión de colaboradores y clientes, bien como un proceso de revisión de los procedimientos, políticas y prácticas de los mismos, ya que, en última instancia el prestador asume la responsabilidad

frente al suscriptor y frente a terceras personas que han confiado en el certificado o en las firmas electrónicas del suscriptor.

En el mismo sentido, suele reservarse el prestado el derecho de auditar la instalación de las tecnologías que sirven de soporte a la emisión y gestión de los certificados.

2. Derecho de remisión de certificados

Que se reserva el prestador en función del resultado del procedimiento de validación de la información contenida en la solicitud, y de la aprobación de la misma.

El factor decisivo para admitir este derecho, es que el prestador responde casi ilimitadamente por los daños causados por el certificado.

3. Facultad de revocación de certificados

El uso de esta facultad viene determinado a por la concurrencia de uno de los motivos contenidos en las "Prácticas de Certificación" y resto de documentación contractual.

La Declaración de Prácticas de Certificación es un documento elaborado por una Autoridad de Certificación que recoge o regula la prestación de los servicios de certificación por parte de dicha Autoridad de Certificación en su condición de Prestador de Servicios de Certificación,[21] vinculado a una aplicación o servicio determinado.

Entre las causas generales de revocación se encuentran:

- El robo, pérdida, modificación, divulgación no autorizada, u otro compromiso de la clave privada del sujeto del certificado.

[21] IZENPE, S.A. www.izenpe.com

- Que alguna de las partes haya incumplido alguna de sus obligaciones
- Cuando, por causa fortuita, la información de otra persona se ve amenazada o comprometida.

4. Facultad de suspensión de certificados

   Prevista en el art. 9 de la Ley, "podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores".

5.3. Responsabilidad de los prestadores de servicios de certificación de firma electrónica [22]

Conforme al artículo 23 de la Ley 59/2003, como principio de carácter general, los Prestadores responden civilmente por los daños y perjuicios que pudieran causar a sus usuarios o a terceros cuando actúen con negligencia en el cumplimiento de sus obligaciones. Se trata de una la responsabilidad subjetiva contractual y extracontractual. También el artículo 1.2 de la misma Ley dice que "Las disposiciones contenidas en esta Ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten".

Además, una vez revocado el certificado los Prestadores seguirán estando sujetos a responsabilidad en cierta medida, si bien, ni la normativa comunitaria ni la doctrina han fijado un criterio claro para esclarecer el alcance de esta responsabilidad. Por un lado, se considera

[22] María Claudia Cambi y José Carlos Erdozain, "Derecho del Comercio electrónico", La Ley, Biblioteca de los negocios, 2001

que los Prestadores deben estar sujetos a una responsabilidad limitada, respondiendo únicamente de los daños y perjuicios que causaran por el incumplimiento negligente de la obligación de publicar la revocación del certificado o de la obligación de inscribirlo en el registro de certificados del Prestadores, con lo cual, el titular acabaría asumiendo todos los riesgos derivados de un posible robo o extravío de la clave. Por otro lado, se intenta extender su responsabilidad para que respondan también por las posibles utilizaciones ilegítimas de la clave de firma.

5.3.1. Límites de la responsabilidad

Entre los límites a la responsabilidad de los Prestadores que admite la doctrina se encuentran los siguientes:

-Límites de uso:

Podrán limitar su responsabilidad emitiendo el certificado únicamente para un uso determinado (ciertos ámbitos, transacciones, operaciones, etc.). Con esta limitación, el Prestador no será responsable cuando el certificado se utilice más allá de la finalidad para la cual fue expedido. Esta limitación debe establecerse de forma expresa, clara e inequívoca en el propio certificado, facilitando con ello que los terceros conozcan la limitación existente.

-Limites de cuantía:

Estos límites se dirigen a proteger a los Prestadores, limitando su responsabilidad a un importe máximo relacionado con el valor de las transacciones realizadas utilizando el certificado. En este sentido, los Prestadores tienen dos opciones:

1. Establecer que el certificado sólo sea utilizado en transacciones que no excedan de una determinada cuantía.

Inconveniente: El certificado puede ser utilizado en una gran cantidad de operaciones de distinto tipo, siempre que no se superaran los límites cuantitativos establecidos, por lo cual, la responsabilidad del Prestador se incrementa.

2. Establecer que el certificado sólo pueda utilizarse hasta una determinada cantidad máxima con independencia de las transacciones que se realicen. Por ejemplo, un certificado válido hasta que se cubra la cantidad total de 24 millones de euros.
   Inconveniente: Si bien los derechos de los Prestadores se encuentran más protegidos, ésta limitación perjudica los intereses de los usuarios de los certificados, pues éstos deberán estar controlando en todo momento el valor total de las operaciones realizadas con el certificado.

6. LA FIRMA ELECTRÓNICA [23]

Como ha quedado expuesto más arriba, en esta nueva sociedad llena de redes telemáticas abiertas y al alcance de cualquiera que tenga una conexión a Internet, todavía existe mucha desconfianza respecto a la seguridad de las comunicaciones y más aún a la certeza jurídica de las transacciones comerciales.
Por ello ya han empezado a cobrar gran importancia términos como seguridad y autentificación, que se han hecho imprescindibles para que los usuarios se "atrevan", por ejemplo, a dar sus datos a comercios online o a hacer la Declaración de la Renta a través de Internet. A partir de este panorama tecnológico surge la necesidad de contar con un

[23] PAGINA WEB DEL MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA

mecanismo por el cual se pueda demostrar que quien escribe es quien dice ser, que el contenido de su mensaje es auténtico y con la validez legal de la firma manuscrita.

Evidentemente la seguridad total no existe, ni en comercio tradicional ni en el entorno electrónico. No obstante, la utilización de las nuevas tecnologías en las transacciones comerciales y los inconvenientes que se planteaban desde el punto de vista jurídico, han llevado a los legisladores a la creación de sistemas seguros que garanticen la autenticidad, la integridad y la confidencialidad de los datos que se transmiten a través de la red, requisitos éstos imprescindibles para garantizar su plena eficacia jurídica.

La evolución tecnológica y la dimensión mundial de Internet hicieron necesario buscar un sistema electrónico alternativo que sirviera para sustituir a la firma manuscrita y que a la vez cumpliera sus mismas funciones, es decir, que asegurara la identidad de las partes contratantes, y las vinculara en cuanto a las declaraciones de voluntad que realizaran.

La fórmula se ha encontrado en la "firma electrónica" y en los proveedores de "servicios de certificación". [24]

La firma electrónica consiste en un instrumento generado por documento electrónico relacionado con la herramienta de firma en poder del usuario, y que es capaz de permitir la comprobación de la procedencia y de la integridad de los mensajes intercambiados, ofreciendo bases para evitar su repudio. Con ello se alcanza el vínculo contractual o la autenticidad de un documento, al igual que si se tratara de una firma manuscrita.

[24] INTECO Instituto Nacional de Tecnologías de la Comunicación

Los documentos electrónicos ofrecen así una mayor fiabilidad y precisión que los tradicionales, ya que se emplean técnicas especiales para la protección del contenido. Entre ellas cabe destacar la criptografía, de la que me ocupo seguidamente, y, junto a ella, la posibilidad de emplear códigos de acceso secretos o técnicas basadas en la biometría, es decir, en sistemas de identificación de los operadores a través de rasgos físicos o biológicos.

6.1. Funcionamiento

6.1.1. La criptografía [25]

La Criptografía es la ciencia que se ocupa del cifrado seguro de mensajes. Está estrechamente relacionada con las Matemáticas y, en particular, con los números primos.

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el sistema criptográfico es simétrico o de clave secreta. Por tanto, el sistema simétrico o de clave secreta es aquél en el cual se da un proceso matemático complejo que convierte información de texto plano en algo aparentemente ininteligible de texto cifrado, sobre la base de una clave secreta de paso o *password*.

La criptografía simétrica, de clave sencilla o de clave secreta, es la más simple y antigua (fue utilizada hasta los años 70). En este sistema, la clave secreta, para cifrar y para descifrar, es idéntica.

Existen graves problemas o desventajas en los métodos simétricos. Uno de ellos es la "distribución de las claves", de modo que si se tiene una clave y se cifra un documento o un mensaje y otra persona tiene que descifrarlo, la otra persona tiene que tener la misma clave utilizada para el cifrado, sin la cual no lo va a poder descifrar. Esto conlleva el

[25] GRUPO DE TRABAJO DE COMUNICACIÓN Y DIVULGACIÓN COMISIÓN TÉCNICA DE APOYO A LA IMPLANTACIÓN DEL DNI ELECTRÓNICO

inconveniente de que la clave teóricamente secreta, al ser distribuida al menos a una persona más, ya no es secreta. A lo que hay que añadir que, normalmente, se utilizan claves distintas en función de lo que se quiere proteger, lo que supone que se deben mantener y recordar una gran cantidad de claves.

La firma electrónica se instrumenta mediante un sistema de "criptografía asimétrica", basado en el uso de dos claves.

Al realizar una firma electrónica, el sistema informático del titular introduce un algoritmo sobre el documento a firmar, obteniendo un extracto de longitud determinada y específico para este documento de modo que si se produjera una mínima modificación posterior, se generaría un extracto totalmente diferente y por ello, no se correspondería con el original que firmó el titular. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits, se somete seguidamente a un cifrado mediante la clave secreta del titular.

Los algoritmos más utilizados de clave pública son: los de Gelman, el DSA y el RSA. La gran ventaja de este sistema es que uno posee una sola clave privada y no tiene que distribuírsela a nadie, con lo cual se reducen en gran parte los problemas de falta de confidencialidad.

Con él se obtiene un extracto final cifrado con la clave privada del autor, que se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes

Una vez re
y para ello
la clave p
Certificación), descifrará el extracto cifrado del autor y a continuación calculará el extracto *hash* que le correspondería al texto del mensaje y, si el resultado coincide con el extracto anteriormente descifrado, se

considera válida; en caso contrario significaría que el documento ha sufrido una modificación posterior y por tanto no es válido.

En resumen, existen dos esquemas clásicos de encriptación:

1. La simétrica, que obliga a al emisor y receptor del mensaje a utilizar la misma clave para encriptar y desencriptar el mismo (como por ejemplo el criptosistema DES (*Data Encription Standard,* desarrollado por IBM), y
2. La encriptación asimétrica o criptográfica de claves públicas que está basada en el concepto de pares de claves, de forma que cada uno de los elementos del par (una clave) puede encriptar información que sólo el otro componente del par (la otra clave) puede desencriptar.

   El par de claves se asocia con un solo interlocutor, así un componente del par (la clave privada) solamente es conocida por su propietario mientras que la otra parte del par (la clave pública) se publica ampliamente para que todo el mundo pueda verla (en este caso destaca el famoso cripto-sistema RSA cuyas iniciales son las de sus creadores: Rivest, Shamir y Adelman). Esta clave pública es dada por un tercero que es el conocido como "*autoridad de certificación".*

El sistema se compone de cuatro etapas:

1. A cada usuario se le asigna una clave pública.
2. Igualmente, cada usuario posee una clave privada que sólo él conoce, y que puede cambiar cuantas veces desee.
3. Se crea un directorio de claves públicas accesibles al público general.
4. El usuario de la red envía sus mensajes con la clave pública del destinatario encriptada con su clave privada. El destinatario sólo

podrá abrir el mensaje con la clave pública junto con su clave privada.

Es un método generalmente aceptado por los usuarios, ya que garantiza adecuadamente la seguridad y la confidencialidad del mensaje transmitido.

En la firma el titular utiliza el código personal que sólo él conoce (criptografía asimétrica) y esto es lo que impide que después se pueda negar su autoría (no revocación o no repudio). De este modo el titular de la firma queda vinculado por el documento emitido e igualmente la validez de la firma podrá ser invocada por cualquier persona que disponga de la clave pública del titular.

Para la firma electrónica se necesita un dispositivo de firma electrónica que sea capaz de capturar o registrar la firma escrita y todos sus aspectos, tales como tiempo (sello del tiempo), presión y trazado. También necesitará un programa capaz de codificar la firma electrónica de modo seguro y asimétrico en un documento electrónico con poder probatorio.

6.1.2. Fecha y hora de certificación (*time stamping*)

La naturaleza irreversible del tiempo es un elemento clave en las relaciones entre los procesos, ya que los lazos de interdependencia entre los hechos están en función del orden en que se realiza cada uno de ellos y suelen ser manifestación de las relaciones causales que los unen.

En el entorno digital, en el que la mayor parte de la información se encuentra en soporte magnético o digital, es importante que la información pueda ser identificada con un medio capaz de certificar que un documento existía, que fue creado o que fue actualizado, en un instante de tiempo histórico determinado. Por ello, cualquier proceso

que le de valor al documento digital, debe disponer de un mecanismo que ponga de manifiesto la secuencia temporal de modo indudable.

El llamado "sello de tiempo" (*time stamping*), es la respuesta a estas necesidades, ya que éste es el que prueba que, en un determinado instante histórico de tiempo, todos los agentes involucrados disponían de un determinado documento, lo que daría confianza a todas las partes involucradas.

El sistema persigue congelar el estado de cualquier objeto digital en un instante histórico de tiempo, probando que el documento, tal y como se conoce, ya existía y no ha sido modificado, hasta el momento.

Garantizada la identidad digital de la entidad que extiende el sello digital de tiempo, el cliente asegurará que tal documento existía en la fecha y horas establecidas en el sello y, puesto que está firmado por una autoridad depositaria de toda su confianza, no se cuestionarán la integridad de los datos.

El "sello de tiempo" emitido corresponde de manera única e irrevocable al documento que existía en ese instante histórico de tiempo, de manera que es imposible asociar ese sello de tiempo a cualquier otro documento. Así se evita que el servicio genere un sello con una fecha y hora determinada, y que posteriormente su propietario pueda utilizarlo indebidamente en un documento distinto a aquél para el que el "sello" se creó originariamente.

Se deben sellar los datos en sí, independientemente de su contenido, de modo que sea imposible modificar ni un solo bit del documento sin que ese cambio sea detectado e invalide el valor del sello. De producirse la manipulación de la información, el sistema proporcionaría valores distintos a los que el usuario espera recibir, de modo que en el proceso de verificación del sello, sería detectado y se procedería a la anulación de su valor, garantizando la integridad y autenticidad de los sellos emitidos. De tal modo se acreditaría quién es el autor de los mismos y que no ha existido ninguna manipulación de los datos.

Esto se logra a través de la certificación del certificador habilitado, el que tiene que responder en caso de que se le impute cualquier problema o cuestión acerca de la validez del sello. Para que esto ocurra será necesario acordar previamente lo referido a cómo establecer, legal y técnicamente, la hora oficial en la implementación de la firma digital.

Con la mejora de los elementos científicos y las necesidades y requerimientos de la ciencia, la industria, y el comercio, resultó crítico realizar una más precisa medición y guarda del tiempo. Es destacable la labor desarrollada por el Bureau International des Poids et Mesures, así como la de la multiplicidad de institutos, cada uno ajustado a la necesidad de su sector, que le dan solución efectiva, ya que cada uno desarrolla los servicios que sus usuarios requieren, de la manera más adecuada para ellos.

Es interesante en este sentido tener en cuenta con qué países se van a realizar operaciones de Comercio Exterior, para adoptar vínculos a institutos que ya se hallen reconocidos en estos países, facilitándose así la interconexión entre redes y reduciendo al mínimo la cantidad de saltos de interconexión, evitándose, dentro de lo posible, los lapsus de tiempo.

No obstante, debe tenerse en cuenta que no es posible tener una lectura de la hora "exacta" y "única" en todos los lugares del mundo, por lo que para resolver el hecho de la simultaneidad, en un caso de derecho de prelación, o el tiempo de vencimiento de un certificado digital, deberá decidirse, previamente, el problema de las horas.

La exactitud se resuelve adoptando un estándar de tolerancia aceptado por la generalidad, como lo sería el tomar un microsegundo de diferencia respecto del UTC -la hora de París- y todo lo que ocurriese dentro de ese lapso de un microsegundo, lo consideraremos simultáneo. Ese lapso es un "átomo" de tiempo, la mínima división de la escala.

El objetivo sería lograr una solución

- internacionalmente aceptable,
- que reconozca uniformemente un tiempo dado,
- que contemple la realidad de países que cuentan con medios propios para realizar mediciones muy cercanas a las del BIPM, y
- y la realidad de países como el nuestro, que no cuentan con ningún medio propio, pero pueden recibir estos datos de otros.

La legislación debe contemplar que, en muy poco tiempo, lo adelantos tecnológicos quedan rápidamente superados, por lo que el objeto debe ser mantener una lectura del tiempo, no basada en una tecnología determinada.

En esta línea de defender los intereses del usuario, la Ley de Firma Digital incorpora una novedad, que aparece recogida entre los requisitos exigibles a los prestadores de servicios de certificación. La novedad consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante. Y es que, en algunas ocasiones, la fecha que figura en un documento puede llegar a ser tan importante como que éste vaya firmado, sobre todo a efectos probatorios en un juicio.

6.2. Marco jurídico

La regulación jurídica de la firma electrónica se ha llevado a cabo en nuestro entorno mediante 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 y su trasposición en España mediante la Ley 59/2003, de 19 de diciembre.

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo de la Unión Europea, creó un marco jurídico para la firma electrónica y para determinados servicios de certificación, con el fin de garantizar un adecuado funcionamiento del mercado comunitario y además formuló

la necesidad de buscar acuerdos transfronterizos para garantizar la interoperabilidad a nivel mundial.

Esta Directiva pretende mantener un marco jurídico coherente en toda la Comunidad, consciente de que ese marco claro aumentará la confianza en las nuevas tecnologías. Igualmente contribuye al uso y al reconocimiento legal de la firma electrónica. Es importante alcanzar el equilibrio entre las necesidades de los consumidores, de las empresas y de la propia Administración y además de todo ello, para contribuir a la aceptación general de los métodos de autenticación electrónica, debe garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales de los estados miembros.

Para incrementar la confianza de los usuarios en sus comunicaciones y en el comercio electrónico, los proveedores de servicios de certificación deberán observar las normativas sobre protección de datos y el respeto de la intimidad.

Esta Directiva entiende por firma electrónica: “los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación..." (Artículo 2.1).

Igualmente distingue la "firma electrónica" de la denominada "firma electrónica avanzada", un especie de firma electrónica "cualificada", y la define como "...la firma electrónica que cumple con los siguientes requisitos:

a) estar vinculada al firmante de manera única;
b) permitir la identificación del firmante;
c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; y
d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable." (artículo 2.2).

En España la Directiva ha sido traspuesta a nuestro Ordenamiento a través de la Ley 59/2003, que define la firma electrónica en su artículo 3.1:

"La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante."

Asimismo la Ley distingue entre "firma electrónica avanzada" y "firma electrónica reconocida":

- (Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

- (Art. 3.3) Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

- (Art. 3.4) La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- En caso de ser desconocida la firma electrónica, corresponde a quien la invoca acreditar su validez.

El modo de funcionamiento de la firma electrónica basado en clave pública es el siguiente:

- Cada parte tiene un par de claves, una se usa para cifrar y la otra para descifrar.

- Cada parte mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública).

- El emisor obtiene un resumen del mensaje a firmar con una función llamada “hash” (resumen).

  El resumen es una operación que se realiza sobre un conjunto de datos, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la función “hash”.

- El emisor cifra el resumen del mensaje con la clave privada. Ésta es la firma electrónica que se añade al mensaje original.

El receptor, al recibir el mensaje, obtiene de nuevo su resumen mediante la función “hash”. Además descifra la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó. Si ambos coinciden la firma es válida por lo que cumple los criterios ya vistos de autenticidad e integridad además del de no repudio ya que el emisor no puede negar haber enviado el mensaje que lleva su firma.

Por otra parte, la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), considera a la firma electrónica como el "equivalente funcional" de la firma manuscrita, siempre que cumpla con los requisitos previstos en su art. 7º:

"Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de

datos; y

b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente".

Otras normas a tener en cuenta sobre este tema son las siguientes:

Leyes Orgánicas

- **Ley orgánica 6/1985**, de 1 de Julio, del poder judicial. Artículo Doscientos treinta.
- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Leyes

- **Ley 11/2007**, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos
- **Ley 24/2001**, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden social. **Título V**. de la acción administrativa. **Capítulo XI**. Acción administrativa en materia de seguridad jurídica preventiva. **Sección VIII**. Incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva.
- **Ley 24/2001**, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. **Título IV**. Normas de gestión y organización administrativa. **Capítulo III**. Procedimientos. **Artículo 68.** Modificaciones de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común para impulsar la administración electrónica.
- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Reales Decretos-Ley

- **Real Decreto Ley 14/1999**, de 17 de septiembre, por el cual se regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

Reales Decretos

- **Real Decreto 263/1996**, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.
- **Real Decreto 994/1999,** de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- **Real Decreto 1114/1999**, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.
- **Real Decreto de 1289/1999,** de 23 de julio, de creación de la Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías en España.
- **Real Decreto 111/2000,** de 28 de enero, por el que se modifican determinados artículos del Reglamento General de Recaudación, aprobado por Real Decreto 1648/1990, de 20 de diciembre, en materia de ingresos correspondientes a declaraciones prestadas por vía telemática.
- **Real Decreto 1317/2001**, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas.

- **Real Decreto 1029/2002**, de 4 de octubre, por el que se establece la composición y el régimen de funcionamiento del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.
- **Real Decreto 209/2003**, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- **Real Decreto 292/2004**, de 20 de febrero de 2004, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimientos de concesión.
- **Real Decreto 421/2004**, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

Órdenes Ministeriales

- **Orden de 13 de abril de 1999** por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre la Renta de las Personas Físicas.
- **Orden de 26 de julio de 1999** por la que se regulan las bases de datos y ficheros automatizados de carácter personal existentes en la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.
- **Orden del 21 de diciembre de 1999** por la que se fijan los umbrales estadísticos de asimilación definidos en el artículo 28 del reglamento (CEE) 3330/91 del consejo y se autoriza la presentación de declaraciones Intrastat por vía telemática
- **Orden de 20 de enero de 1999** por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de las declaraciones-liquidaciones mensuales de grandes empresas.

- **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.
- **Orden de 28 de febrero de 2000** por la que se establecen las condiciones generales y el procedimiento para la renovación y revocación del certificado de usuario X 509 V3 expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda al amparo de la normativa tributaría.
- **Orden de 26 de septiembre de 2000** por la que se establece el sistema para la presentación telemática por internet de los documentos de circulación utilizados en la gestión de los impuestos especiales.
- **Orden de 21 de diciembre de 2000** por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por internet de las declaraciones correspondientes a los modelos 117, 123, 124,126, 128,216, 131, 310, 311, 193, 198, 296 y 345.
- **Orden de 11 de Diciembre de 2001** por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM.
- **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.
- **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.
- **Orden HAC/1181/2003, de 12 de mayo**, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios

electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria

- **Orden PRE/1551/2003, de 10 de junio**, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

6.3. Certificados de seguridad electrónicos [26]

Si bien he hecho referencia más arriba, en el apartado de "Sujetos intervinientes en las operaciones de comercio electrónico" a los Prestadores de Servicios de Certificación y a su responsabilidad en los servicios de certificación de firma electrónica, añadiré algunos apuntes más sobre los Certificados de Seguridad electrónicos.
Son éstos dispositivos que posibilitan el almacenamiento de diversos datos relativos al propietario de los mismos (datos personales, claves, etc.) y que permiten identificarlo en la red, garantizando tanto la emisión de los datos como su recepción, la integridad de la información transmitida, la confidencialidad y el no repudio de la transacción.

El objeto es generar confianza en el usuario haciendo que el entorno de Internet resulte seguro. Para ello se ha creado el concepto de "identidad digital", es decir, un identificador digital único dentro de la red que permite a su poseedor ser identificado como tal dentro de la misma.

[26] Camerfirma: www.camerfirma.com
EDATALIA: www.edatalia.com

En el marco jurídico comunitario, los certificados de seguridad han sido expresamente definidos como: "...la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta..." (Artículo 2.9 de la Directiva 1999/93/CE).

El artículo 6 de la Ley 59/2003 de Firma Electrónica, lo define como "un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa".

Los "certificados reconocidos" deben ser emitidos por las *autoridades de certificación*, o *proveedores de servicios de certificación*. Éstos certificados ofrecen las mayores garantías ya que reúnen una serie de requisitos que aumentan su seguridad.

El artículo 11 de la referida Ley establece los siguientes requisitos mínimos:

a. La indicación de que se expiden como tales.
b. El código identificativo único del certificado.
c. La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
e. La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
f. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g. El comienzo y el fin del período de validez del certificado.
h. Los límites de uso del certificado, si se establecen.
i. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

6.4. Utilidades del Certificado de seguridad electrónico [27]

El certificado de seguridad electrónico puede ser utilizado para muchas aplicaciones, entre otras:

6.4.1. Firma digital. El certificado de seguridad se utiliza para firmar todo tipo de documentos digitales, desde simples e-mails hasta los más complejos contratos mercantiles. Esto implica garantía de no repudio, de conocimiento inequívoco de quien es el emisor del

[27] Diputación Foral de Guipúzcoa: www.gipuzkoa.net. Campaña de firma electrónica
HISPADATA SOLUTIONS: www.hispadata.com
REVISTA DE DERECHO INFORMÁTICO: FIRMA ELECTRONICA I. El panorama actual (Agosto de 2008)

documento y de la integridad del documento, es decir, que el documento firmado es el original y que nadie ha modificado su contenido después de su firma. También es usado para firmar ciertas operaciones, como por ejemplo, formalizar una orden de transferencia bancaria o una declaración fiscal.

6.4.2. **Seguridad en la comunicación**. El certificado sirve para codificar una comunicación entre dos personas, haciendo que toda la información transmitida sea confidencial. Un ejemplo de ello lo tenemos en la mayoría de páginas web donde se nos pide el número de una tarjeta de crédito para efectuar un pago. Están utilizando certificados digitales, y con ello garantizan que sólo el comercio podrá acceder a la información del número de la tarjeta de crédito.

6.4.3. **Seguridad entre las partes:** Ante la duda de que el receptor sea realmente quien dice ser y por lo tanto el emisor puede tener confianza para enviar una información, la autoridad de certificación cumple con la importante función de certificar quien es el auténtico receptor. Un caso específico es el de los servidores web; ante la duda de si la página web que estamos consultando pertenece realmente a la empresa que creemos, la consulta del certificado digital que pueda tener esta web nos va a certificar que realmente esta web pertenece a la empresa en cuestión.

6.4.4. **Identificación ante un acceso restringido**. Hasta ahora en el momento de entrar en un espacio digital restringido se utilizaba el par *login* + *password*, sistema con un nivel de seguridad muy bajo. Todo indica que el siguiente sistema de identificación será el certificado digital. En el momento de entrar en Intranets, accesos a una red local, a un servidor determinado, o incluso a

aplicaciones específicas, la tecnología utilizada será la del certificado de seguridad electrónico.

Por ejemplo, uno de los obstáculos con que se ha encontrado la Administración para su completo desarrollo en la red y para la puesta a disposición de los ciudadanos a través de Internet de un conjunto de servicios y trámites, era la necesidad de garantizar la identidad del administrado. En distintos servicios, es básico el poder garantizar esta, puesto que la información que ha de dar la administración para un completo desarrollo de este trámite es confidencial. En este ámbito está resultando decisiva la implantación del uso del certificado digital, máxime dada la necesidad del no-repudio por parte de la administración y del administrado en el desarrollo de sus relaciones.

6.4.5. Firma de software. Esto permite a la entidad que va a utilizar el *software* garantizar que éste es el original, conocer quien lo ha creado, y muy importante, que con posterioridad a su firma, nadie lo ha modificado. Esto garantiza que dicho *software* no contiene virus, y si los contiene, es el propio creador del *software* quien los ha incorporado, pudiendo ir en contra de éste con una prueba firmada.

6.5. Clases de certificados [28]

[28] Diputación Foral de Guipúzcoa: www.gipuzkoa.net. Campaña de firma electrónica
CERES: http://www.ceres.fnmt.es
HISPADATA SOLUTIONS: www.hispadata.com
REVISTA DE DERECHO INFORMÁTICO: FIRMA ELECTRONICA I. El panorama actual (Agosto de 2008)

6.5.1. Certificados de Servidor

El Certificado de Servidor aporta a una página *web* la característica de seguridad y confianza necesaria para poder entablar cualquier tipo de relación con los potenciales usuarios. Los Certificados de Servidor permiten incorporar el protocolo SSL (*Secure Socket Layer*) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos transmitidos.

6.5.2. Certificados para WAP

Los Certificados WAP permiten a las *web* comerciales la realización de transacciones seguras con los consumidores móviles. Los nuevos portales basados en transacciones móviles seguras expandirán el comercio electrónico entre los usuarios móviles y los WEB SITES dedicados al comercio. Los Certificados WAP permiten mantener conexiones seguras basadas en encriptación y autenticación con dispositivos de telefonía móvil.

6.5.3. Certificados Personales

Otorgan seguridad a los correos electrónicos basados en un standard S/MIME. Se podrán firmar o cifrar los mensajes de correo para asegurarse de que sólo el receptor designado sea el lector de nuestro mensaje.

6.5.4. CA's Corporativas

Es la solución óptima para las empresas que quieran disponer de un sistema de generación de cualquier tipo de Certificado para sus usuarios (trabajadores, proveedores, clientes, etc.) y servidores. Una CA Corporativa puede generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código e incluso para IPSec-VPN. En función del tipo de funcionalidad que se le quiera dar a la CA se deberá escogerse un diferente tipo de CA Corporativa.

6.5.5. Certificados para firmar Código

El Certificado para la Firma de Código, permitirá a un Administrador, Desarrollador o Empresa de Software firmar su Software (ActiveX, Applets Java, Plug-ins, etc.) y Macros, y distribuirlo de una forma segura entre sus clientes.

6.5.6. Certificados para IPSec-VPN

Los Certificados para VPN son los elementos necesarios para que la empresa aproveche las cualidades y ventajas de la utilización de las VPNs de un modo plenamente seguro. Las VPNs surgen como consecuencia de la creciente demanda de Seguridad en las comunicaciones ya sea entre Router-Router o Cliente-Servidor. La apertura de las redes corporativas a empleados remotos (con gran importancia en el caso del Teletrabajo, sucursales, *business, partners* o clientes.

6.6. Ventajas

Mediante la utilización de los certificados electrónicos, tanto las transacciones electrónicas como cualquier otra clase de transmisión de información a través de Internet, estará más protegida, originándose de esta forma una mayor confianza y seguridad en los usuarios en relación con los contenidos de los mensajes enviados y recibidos.

Su mayor ventaja es la certeza que produce sobre la identificación de la persona que envía un determinado mensaje, ya que autentifica fehacientemente la identidad del emisor.

6.7. Validez de los certificados de seguridad

6.7.1. Vigencia

Los certificados de seguridad son válidos por un período de tiempo determinado, indicado en el propio certificado: fecha y hora del comienzo y la extinción de su validez. La validez de los certificados no debe ser demasiado extensa, pues, en este caso, las claves protegidas se encuentran expuestas a mayores riesgos de ser copiadas, apropiadas o utilizadas ilegítimamente por terceros.

Algunos países, limitan la duración máxima de los certificados entre tres y cinco años. Una firma electrónica sólo será válida si se expidió dentro del período de validez del certificado de seguridad correspondiente. En caso de que la firma electrónica haya sido expedida fuera de este período, las transacciones celebradas utilizando dicha firma carecen de seguridad jurídica.

Es España, la Ley 59/2003 detalla, como causa de extinción del a vigencia de un certificado, las siguientes:

a. Expiración del período de validez que figura en el certificado.
b. Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
c. Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
d. Resolución judicial o administrativa que lo ordene.
e. Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las

condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f. Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
g. Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
h. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

6.7.2. Revocación

Por regla general, los certificados serán revocados una vez que cumplan el período temporal de validez por el cual fueron creados. Sin embargo, también cabe la posibilidad de que el certificado sea objeto de una revocación anticipada, generalmente cuando la clave privada

ha sido puesta en peligro (perdida o extraviada), por lo que puede ser utilizada por personas no autorizadas o para fines ilegítimos.

Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a. Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
b. Resolución judicial o administrativa que lo ordene.
c. La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c y g del artículo 8.1.
d. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación. Los certificados perderán su validez desde el momento mismo en que concurra alguna de las causas de revocación, si bien, en algunos casos, se requiere que dicha revocación sea debidamente publicada por el proveedor de servicios.

7. D.N.I. ELECTRÓNICO[29]

Fundamentado en las ventajas que proporciona la "firma electrónica", tal y como se han expuesto más arriba en este trabajo, el D.N.I.

[29] www.dnielectronico.es
www.dni.org.es
www.dnielectronico.eu
www.inteco.es/Seguridad/DNIElectronico/

electrónico aporta al D.N.I. tradicional "... nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece." [30]

El desarrollo de la Sociedad de la Información tiene como objetivo "fomentar el uso de la tecnología en todos los ámbitos sociales, incrementar la competitividad y el crecimiento económico", así como "mejorar la calidad de vida de los ciudadanos y evitar el riesgo de brecha digital, promoviendo la igualdad social y regional".[31]
Para ello precisa de la generalización de la confianza de los ciudadanos en las transacciones electrónicas.[32] El DNI-e responde a esa necesidad otorgando identidad personal a los ciudadanos facilitándoles el que puedan realizar múltiples gestiones de forma segura a través de medios telemáticos y asegurando la identidad de los participantes en la comunicación.

Ello es posible dado que Documento Nacional de Identidad goza de plena aceptación en la sociedad española, ya que, con una antigüedad de más de 50 años, está presente en la mayoría de las relaciones de los ciudadanos entre sí y en las relaciones comerciales y administrativas. Es el único documento de uso generalizado en todos los ámbitos a nivel nacional y es un referente obligado para la expedición de otros documentos, como el pasaporte, el permiso de conducir, el número de la seguridad social, etc. Es más, no obtener el DNI, cuando se está obligado a ello, está considerado como una falta sancionada con hasta 300€, según lo establecido en el artículo 26 de la Ley 1/92 de

[30] Preámbulo del RD 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
[31] www.red.es
[32] PAGINA WEB DEL MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA

Protección de Seguridad Ciudadana. Esta misma Ley indica que las personas mayores de 14 años están obligadas a obtenerlo y exhibirlo siempre y cuando un agente de la autoridad se lo requiera.

Además su número figura como dato en el 97% de las bases de datos de entidades de organismos públicos y privados, y, como afirma el artículo 2 del RD 1553/2005 de 23 de diciembre por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, "...tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo".
Esta característica del DNI tradicional se mantiene en el DNI electrónico. A ella hay que añadir el valor de la firma electrónica, la cual, realizada a través del Documento Nacional de Identidad tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel." *Art. 1.5.* RD 1553/2005.

7.1. Proceso de implantación

En abril de 2006, el entonces Ministro del Interior D. José Antonio Alonso, presentaba el proyecto de implantación del DNI electrónico afirmando que el DNI-electrónico era un documento más seguro que el tradicional y que tendría efectos positivos para las empresas y las administraciones, puesto que la incorporación de la identidad digital y de la firma electrónica en los procesos de negocio y en las empresas, en particular las PYME, permitirían afrontar con garantías de éxito la modernización de las mismas y mejorar su competitividad.[33]

También Doña Soledad López, Subsecretaria de Interior en el año 2006, explicó en el Senado las características del DNI electrónico, afirmando

[33] Dirección General de la Policía. El Periódico, 5 de Abril de 2006

que éste aportaría "a todos los ciudadanos más seguridad de forma compatible con nuestra privacidad" así como que "la implantación del DNI electrónico situar(í)a a España en la vanguardia de los Servicios de Administración Electrónica"

El proceso se había iniciado a partir del Acuerdo del Consejo de Ministros de 23 de diciembre de 2004 por el que se creó un Comité de Coordinación y una Comisión Técnica con el objeto de crear los mecanismos de implantación del DNI-e en nuestro país. La dotación presupuestaria efectiva para asegurar la financiación del proyecto en el período 2005-2009, a través del Presupuesto del Ministerio del Interior ascendió a 63.010.150 millones de euros. Adicionalmente, el Ministerio del Interior y el de Industria, Turismo y Comercio firmaron un Acuerdo de Colaboración el 7 de julio de 2005 por un importe de 11.642.000 millones de euros para los años 2005-2006. El contrato de adjudicación, que incluía la fabricación de los materiales y los dispositivos para su elaboración y emisión, fue adjudicado a la Unión Temporal de Empresas formada por Telefónica, Indra y Software AG.

El coste total aproximado de la implantación del DNI electrónico en el periodo 2.005 - 2.008 ha sido de 313,85 millones de euros, de los que el Proyecto Técnico ha supuesto 220 millones de euros. El coste principal del proyecto son las tarjetas criptográficas, soporte del DNI-electrónico que representan, en dicho periodo de tiempo, las dos terceras partes del coste total. [34]

Dichas tarjetas soporte han sido "la estrella del proyecto", y su diseño y fabricación se encomendaron a la Fábrica Nacional de Moneda y Timbre, quien incluyó un soporte físico de policarbonato de alta

[34] Web del Ministerio del Interior. Gobierno de España

seguridad,[35] altamente resistente y fiable. La tarjeta criptográfica incorpora numerosas medidas de seguridad con tintas ópticamente variables o visibles con rayos ultravioletas, micro-escrituras, fondos de seguridad y relieves. Además, la grabación de los datos se realiza por láser destructivo que quema la superficie de la tarjeta. Otros detalles técnicos se enumeran más abajo.

Por otra parte, en los trabajos de preparación de DNI-e el Ministerio del Interior ha contado con el asesoramiento de dos autoridades en materia de protección de datos personales y la seguridad: el director de la Agencia Española de Protección de Datos y el director del Centro Criptológico Nacional (Autoridad Nacional de Seguridad), para asegurar que se estaban empleando las tecnologías y procedimientos adecuados para que el DNI electrónico dispusiera de la máxima seguridad posible.

Una vez finalizado el proceso de diseño, las Autoridades españolas han preparado una estrategia de implantación del documento (abril del 2006) por el que se proponen expedir unos seis millones de DNI electrónicos por año, intentado hacer llegar el nuevo DNI a todos los ciudadanos de una manera más rápida y cómoda, en una sola comparecencia del interesado y evitando que sea necesario aportar la documentación que se pueda remitir telemáticamente desde el órgano administrativo en que se encuentre a la Dirección General de la Policía. El DNI electrónico se ha estado desplegando desde el año 2006 a un ritmo que a finales de 2008 supuso dos millones de unidades expedidas.[36]

---

[35] CONSUMER EROSKI www.consumer.es: Por IGNACIO FOSSATI PARA CONSUMER.ES Febrero 2004

[36] Abalia Interactiva: http://www.interactiva.com.

Se ha creado también una Oficina Técnica del DNI-e, con el objetivo de facilitar a las empresas las especificaciones técnicas necesarias y ayudar a los servicios informáticos a desarrollar los diferentes servicios basados en el DNI-e. El personal de la Oficina técnica lo componen los especialistas de la Dirección General de la Policía y está ubicada en el Centro de Proceso de Datos de El Escorial (Madrid).

Todo ello está suponiendo un gran desarrollo de distintos servicios de atención presencial y a distancia que utilicen documentos electrónicos y que se firmen electrónicamente con el nuevo DNI-e. Muchas entidades financieras ya están desplegando servicios de banca electrónica por Internet que permiten hacer uso del DNI-e para la identificación del usuario, aminorando los riesgos de ataques informáticos como los denominados "phishing" y "pharming".[35]

7.2. Elementos técnicos y de seguridad [37]

El DNI electrónico es prácticamente idéntico al anterior pero incorpora un circuito integrado o microchip, que constituye la principal novedad visible por el usuario. El propósito de la tarjeta soporte es contener los datos de filiación del ciudadano, los datos biométricos (modelo dactilar, foto y firma manuscrita) y los dos pares de claves RSA con sus respectivos certificados (autenticación y firma).

Encargado de guardar de forma segura información y procesarla de forma interna almacena la siguiente información en formato digital:

- Certificados X509v3 de ciudadano (autenticación y firma) y claves privadas asociadas, que se generarán e insertarán durante el proceso de expedición del DNI electrónico:

[37] www.dni.es

1. Certificado de autenticación

- Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.
- El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios no tendrán garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

2. Certificado de firma electrónica reconocida

Este certificado es el que se utiliza para la firma de documentos garantizando la integridad del Documento y el No repudio de origen.

Es un certificado X509v3 estándar, que tiene activo en el Key Usage el bit de ContentCommitment (No Repudio) y que está asociado a un par de claves pública y privada, generadas en el interior del CHIP del DNI.

Es este Certificado expedido como certificado reconocido y creado en un Dispositivo Seguro de Creación de Firma, el que convierte la firma electrónica avanzada en firma electrónica reconocida, permitiendo su equiparación legal con la Firma Manuscrita (Ley 59/2003 y Directiva 1999/93/CE).

El hecho de que haya dos certificados persigue que el ciudadano pueda distinguir entre las actividades de autenticación y firma electrónica cuando se produzcan, al margen de la similitud de los procesos criptográficos implicados en ambas.

- Claves para su utilización. Antes de empezar a usar el DNI electrónico es preciso conocer el PIN o número secreto asociado, y que debe ser proporcionado junto con el documento en el momento de la expedición.
- La huella dactilar.
- Imagen digitalizada de la fotografía.
- Firma manuscrita en formato digital.
- Datos de la filiación del ciudadano, correspondientes con el contenido personalizado en la tarjeta.

DATOS de GESTIÓN:

- Traza de fabricación.
- Número de serie del soporte.

- Certificado de Componente. Su propósito es la autenticación de la tarjeta del DNI electrónico mediante el protocolo de autenticación mutua definido en CWA 14890.

- Permite el establecimiento de un canal cifrado y autenticado entre la tarjeta y los Drivers.
- Este certificado no estará accesible directamente por los interfaces estándar (PKCS11 o CSP).
-

Tarjeta física del DNI electrónico.

- La tarjeta física del DNI electrónico sigue el estándar ISO-7816-1.
- Chip ST19WL34.
- Sistema operativo DNIe v1.1.
- Capacidad de 32K.
- Está fabricada en policarbonato, que es un material que permite su uso continuado y frecuente sin sufrir deterioro, durante el tiempo de vigencia del DNI, es decir, 10 años.
- La personalización de la tarjeta se realiza mediante la grabación en el cuerpo de la tarjeta con láser de los datos de filiación, fotografía y firma manuscrita. Este sistema de personalización garantiza la imposibilidad de manipulación de estos datos.

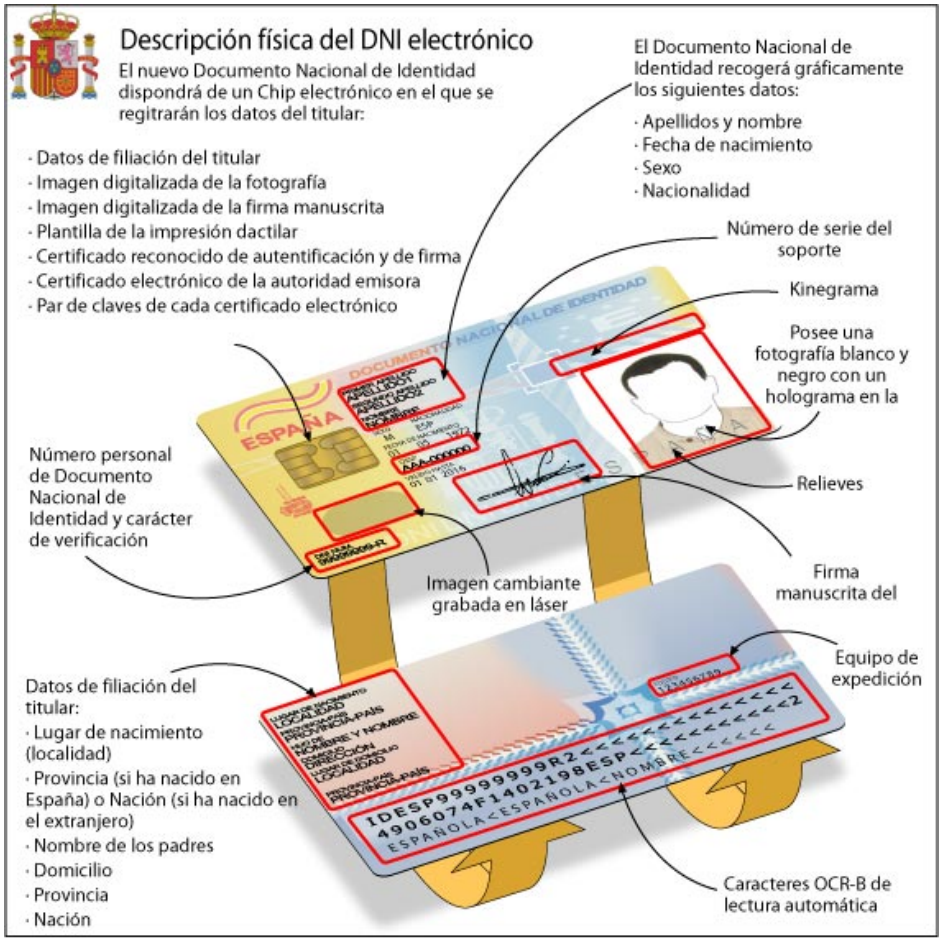
Aspecto fundamental en su desarrollo, el DNI-e incorpora numerosos elementos de seguridad:

- Medidas de seguridad físicas como tintas especiales, relieves o fondos de seguridad.

- Medidas de seguridad digitales como *encriptación* de datos del chip, acceso mediante clave secreta que nunca abandonan el chip y la certificación de la Dirección General de la Policía.

Cuenta con las más modernas medidas de seguridad ante la manipulación y falsificación del documento, muchas de ellas fácilmente identificables por cualquier persona sin ningún procedimiento especial. El conjunto de todas las medidas hace del DNI electrónico un documento altamente seguro, tanto desde el punto de vista físico, como electrónico.

En el DNI electrónico se han desarrollado tres niveles de seguridad. En un primer nivel, holograma, letras táctiles, imágenes láser cambiantes...; en un segundo nivel, imágenes codificadas, microtextos, kinegramas...; y, por último, medidas criptográficas y biométricas.



Orígen: Página web del Ministerio del Interior

PRIMER NIVEL

- Perceptibles a simple vista
- Hologramas / Kinegramas
- Tinta OVI
- Imagen láser cambiante (CLI)
- Letras táctiles
- Estructuras superficiales en relieve

SEGUNDO NIVEL

- Perceptibles mediante equipos mecánicos y electrónicos
- Tintas reactivas UV
- Microtexto
- Fondo de Seguridad (Guilloches)

- Imágenes codificadas

TERCER NIVEL

- Perceptibles en laboratorio
- Medidas criptográficas y biométricas integradas en el chip.

En el anverso de la tarjeta se encuentran los siguientes elementos:

- En el cuerpo central de la tarjeta:
    - Primer apellido
    - Segundo apellido
    - Nombre
    - Sexo
    - Nacionalidad
    - Fecha de nacimiento
    - Número de serie del soporte físico de la tarjeta (IDESP)
    - Fecha de fin de validez
    - Fecha de validez del documento
- En la esquina inferior izquierda:
    - Número del Documento Nacional de Identidad del Ciudadano
- En el espacio destinado a la impresión de imagen láser cambiante (CLI):
    - La fecha de expedición en formato DDMMAA
    - La primera consonante del primer apellido + primera consonante del segundo apellido + primera consonante del nombre (del primer nombre en caso de ser compuesto)

El reverso de la tarjeta contiene los siguientes elementos:

- En la parte superior:
    - Lugar de nacimiento
    - Provincia-País
    - Nombre de los padres
    - Domicilio
    - Lugar de domicilio
    - Provincia-país del domicilio
    - Número de la oficina de expedición del DNI-e
- Información impresa OCR-B para lectura mecanizada sobre la identidad del ciudadano según normativa OACI para documentos de viaje.

El DNI electrónico no contiene ninguna otra información relativa a datos personales ni de cualquier otro tipo (sanitarios, fiscales, tráfico, etc.) distintos a los que aparecen impresos en la superficie de la tarjeta.

Expedición y vigencia

El nuevo DNI se entrega prácticamente en el mismo momento de su petición y no es necesario acudir dos veces a la Oficina de Expedición, sino que la solicitud y la obtención del documento se hace en una única comparecencia, en cualquiera de las Oficinas de de la policía de cada demarcación existentes en España.

Los documentos vírgenes viajan en unas cajas fuertes equipadas con un mecanismo que, en caso de manipulación, libera un ácido que inutiliza las tarjetas almacenadas en su interior.

Su validez no varía con respecto al DNI actual, manteniéndose los mismos periodos actuales (Artículo 6. Validez, RD 1553/2005, de 23 de diciembre), es decir:

a) Cinco años, cuando el titular no haya cumplido los treinta al momento de la expedición o renovación

b) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.
c) Permanente cuando el titular haya cumplido los setenta años.

Por el contrario, la validez de los certificados contenidos en el chip de la tarjeta tendrá un período de vigencia de treinta meses. (Artículo 12, RD 1553/2005, de 23 de diciembre)

7.3. Dispositivos de lectura

Para la utilización del DNI electrónico es necesario contar con determinados elementos hardware y software que permitan el acceso al chip de la tarjeta. Así mismo se requiere que el usuario recuerde la clave que se le asignó cuando lo obtuvo y que puede cambiar en sistemas automatizados instalados en las dependencias policiales en las que se expide el DNI. Para ello solo es necesario identificarse con la huella dactilar. Dicha clave es alfanumérica, acepta símbolos y diferencia las mayúsculas de las minúsculas.

En primer lugar, se necesita conexión a Internet y un lector compatible. Algunos equipos disponen ya de una ranura para el DNI electrónico de serie. De no ser así, las dos formas más sencillas de tener esta funcionalidad pasan por:

- un teclado con lector de DNI electrónico o
- una unidad para tal efecto pero externa, como las representadas a continuación.

7.3.1. Elementos hardware

• Un Ordenador personal (Intel -a partir de Pentium III- o tecnología similar).

• Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.

Un lector que compatible con el DNI electrónico, precisa de, al menos:

• Cumplir el estándar ISO 7816 (1, 2 y 3).
• Soportar tarjetas asíncronas basadas en protocolos T=0 (y T=1).
• Soportar velocidades de comunicación mínimas de 9.600 bps.

• Soportar los estándares:

– API PC/SC (Personal Computer/Smart Card)
– CSP (Cryptographic Service Provider, Microsoft)
- API PKCS#11

7.3.2. Elementos software

Este *lector externo* se conecta al ordenador por el puerto USB que, una vez detectado por el equipo, instalará los controladores adecuados (si el ordenador no lo hace por defecto se debe hacer uso del CD que viene con el lector de tarjetas). A continuación es necesario descargar el software que proporciona la Dirección General de la Policía en el área de "descargas" del portal del DNI electrónico e instalar un programa adecuado en función del sistema operativo utilizado.

Finalmente hay que insertar el DNI en la ranura y poder comenzar a usarlo. A continuación hay que instalar y aceptar los certificados digitales necesarios según la gestión que se vaya a realizar con el DNI electrónico.

• Sistemas operativos

El DNI electrónico puede operar en diversos entornos:

- Microsoft Windows ("Microsoft Windows (2000, XP y Vista)")
- Linux
- Unix
- Mac

• Navegadores

El DNI electrónico es compatible con los siguientes navegadores:

- Microsoft Internet Explorer (versión 6.0 o superior)
- Mozilla Firefox (versión 1.5 ó superior)
- Netscape (versión 4.78 o superior)

• Controladores / Módulos criptográficos

Para poder interaccionar adecuadamente con las tarjetas criptográficas en general y con el DNI electrónico en particular, el equipo ha de tener instalados elementos de software denominados módulos criptográficos.

- En un entorno Microsoft Windows, el equipo debe tener instalado un servicio que se denomina "Cryptographic Service Provider" (CSP).
- En los entornos UNIX / Linux o MAC podemos utilizar el DNI electrónico a

7.4. Nuevas aplicaciones con el DNI-e

El nuevo DNI aporta seguridad, rapidez, comodidad y la inmediata realización de trámites administrativos y comerciales a través de medios telemáticos. INTECO

El uso más conocido para el DNI electrónico tiene que ver con las diferentes Administraciones Públicas**,** las cuales permiten realizar trámites a distancia, sin tener que acudir a las oficinas de la Administración, sin tener que guardar colas y en cualquier momento (24 horas al día, 7 días a la semana). Además, facilita hacer trámites sin tener que aportar una documentación que ya exista en otra Unidad de la Administración, lo que conllevará la práctica eliminación del papel en la tramitación y pérdidas de tiempo innecesarias. (REAL DECRETO 1553/2005, Disposición adicional cuarta. *Remisión de información por vía telemática: "1. La documentación requerida para la expedición del Documento Nacional de Identidad en el artículo 5.1 de este Real Decreto no será exigible cuando sea posible remitir ésta desde los órganos competentes por medios telemáticos a la Dirección General de la Policía, de conformidad con lo que se establezca mediante Convenio.")*

Las posibilidades de utilización son muy amplias. En principio el uso del DNI electrónico es válida para todo tipo de tramitación telemática: desde solicitar una beca a presentar la declaración de la Renta y otros impuestos o acceder a los datos de la Seguridad Social, así como el acceso a información personal en bases de datos públicas, pedir un certificado de empadronamiento, dar de alta en el registro de nacimientos o reclamar el derecho a la pensión, solicitar la ayuda al desempleo, así como la realización de transacciones con empresas, etc.[38]

[38] INTECO Instituto Nacional de Tecnologías de la Comunicación

- El Art. 16.2 de la Ley 59/2003 de Firma Electrónica establece que: ”La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados”
- La Administración General del Estado será uno de los principales proveedores de servicios que se podrán utilizar con el DNI electrónico, de esta forma su utilización supone una ventaja en los trámites con la Administración Pública, en la que ya no sería necesario la presencia física para garantizar la identidad.

No obstante, además de realizar trámites completos con las Administraciones Públicas, es importante la implicación activa del sector privado en el desarrollo de nuevos servicios que exploten las potencialidades del DNI-e y den valor a los procesos de negocio. El objetivo es potenciar la contratación electrónica gracias al acceso a recursos on-line de forma más segura.[39]

El DNI-e permite a los usuarios tener una identidad en Internet, por lo que es función de las empresas desarrollar diferentes servicios basados en la identificación y firma electrónica, de forma que dinamicen la relación comercial con sus clientes. Estos servicios ya están siendo ofrecidos con la máxima seguridad. El sector financiero, por ejemplo, puede jugar un papel protagonista en la generación de modelos de negocio rentables en torno al DNIe.

Actualmente son habituales las transacciones y acceso a la banca online, o las compras firmadas a través de Internet, que pueden realizarse de forma segura con la identificación digital que proporciona el DNI-e.

---

[39] www.red.es

Pero no sólo el sector financiero es apropiado para funcionar en este entorno. Todos los sectores económicos son susceptibles de beneficiarse de las garantías de seguridad y fiabilidad que ofrece la firma electrónica a través del DNI-e. Por ejemplo el "Sector Agencias de Viajes" está ofreciendo cada vez en mayor medida la contratación telemática, utilizando el certificado de firma del DNI-e, de paquetes vacacionales, viajes o estancias "on-line", incluidos los servicios que hasta la fecha requerían la firma formal de documentos. [40]

Un elemento a destacar puesto que será cada vez más habitual para usar el DNI electrónico, es la TDT (Televisión Digital Terrestre)**.** Ya existen en la actualidad equipos TDT que nos permiten acceder a servicios de la Administración y usar el DNI como firma digital.

7.5. Marco Legal

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.
- REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
- *El artículo 1.4 del RD 1553/2005, dice:*
  "Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos

[40] www.dnielectronico.es

previstos en la Ley 59/2003, de 19 de Diciembre, de firma electrónica."

- Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

8. CONTRATO POR MEDIOS ELECTRONICOS [41]

Las relaciones comerciales incluyen cualquier transacción o intercambio de información comercial, actividades diversas como la publicidad, la oferta, la atención al cliente o la formalización de contratos de compra-venta de bienes y servicios, así como las actividades previas y posteriores a los mismos.

Los contratos son actos jurídicos celebrados por dos o más partes y que tienen por objeto modificar, regular o extinguir una relación jurídica patrimonial. El Código Civil define el contrato de compra y venta como aquél por el que "uno de los contratantes se obliga a entregar una cosa determinada y el otro a pagar por ella un precio cierto, en dinero o signo que lo represente".

El Contrato Electrónico ha sido definido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico del 18 de enero del 2001, como "todo contrato celebrado sin la presencia física simultánea de las partes, prestando éstas su consentimiento en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, conectados por medio de cable, radio, medios ópticos o cualquier otro medio electromagnético".

De esta definición es de destacar el hecho de que tanto el contenido de la oferta y de la aceptación contractual vienen configurados en

[41] Guisado Moreno, Ángela: "Formación y perfección del contrato en Internet", Marcial Pons, año http://www.ventanalegal.com/revista

www.injef.com/derecho/derecho-de-las-tic/414.html

http://vlex.com/tags/formacion-contrato-electronico-685763

servicio.estudios@eVeritas.com

programas informáticos y que circulan a través de líneas de telecomunicación (medios electromagnéticos).

Internet proporciona un nuevo ámbito de comercialización en el que, en buena medida, se realizan los mismos contratos que hasta ahora en los medios tradicionales. Por ello resulta de interés determinar la posibilidad de aplicar el marco jurídico existente o si, por el contrario, se requiere de nuevas figuras jurídicas para regularlo.

Así mismo, la existencia de riesgos e imperfecciones consustanciales a todo mercado, se presentan igualmente en el mercado abierto de Internet. La amplia problemática específica de este entorno deriva fundamentalmente del desenvolvimiento virtual del tráfico y de la desmaterialización del contrato y sus soportes documentales, al prescindirse de los documentos y firmas convencionales; dificultades para determinar el momento y el lugar de perfección del contrato, así como la jurisdicción competente en caso de litigio y la ley aplicable al tráfico transfronterizo, especialmente cuando las partes actúan de forma desterritorializada (a través de equipos móviles sin cables); la distribución de riesgos y responsabilidades entre los sujetos intervinientes; problemas derivados de la actuación anónima de las partes, de la suplantación de identidades, equipos y sistemas electrónicos; fallos técnicos de los propios equipos y sistemas.

8.1. Formación del contrato

8.1.1. Condiciones generales de la contratación electrónica

En el ámbito de la Teoría General del Contrato, el acuerdo contractual atraviesa tres etapas: [42]

[42] servicio.estudios@eVeritas.com

1. Generación: está referida a los llamados tratos o negociaciones preliminares y al proceso interno de la formación del contrato

2. Perfección: responde al nacimiento mismo del acuerdo al quedar perfeccionado por el concurso de la oferta y la aceptación

3. Consumación[2]: a la realización y efectividad de las prestaciones derivadas del contrato, siempre sobre la base de las expectativas de cumplimiento que tienen las partes al momento de celebrar el contrato.

Ahora bien, si se parte del hecho frecuente de que la contratación electrónica es una contratación sometida a formatos previos, en los que las condiciones de la contratación se incluyen en la oferta de forma unilateral por una de las partes sin que la otra tenga opción de negociación sino únicamente de adhesión, caso de querer contratar el bien o servicio, la fase de la "generación" pierde relevancia.

Esta práctica es habitual en Internet, donde la oferta aparece en la página *web*, de la empresa oferente, la cual hace una mera mención de la existencia de tales condiciones generales, remitiendo al potencial cliente a otra página (normalmente mediante un enlace) donde aquéllas se encuentran para que éste pueda conocerlas.

La cuestión que se plantea es si la declaración electrónica que contiene la oferta o propuesta de contratación debe incorporar de modo directo tanto las condiciones particulares como las generales, o si legalmente cabría la posibilidad de que estas últimas quedasen incorporadas al contrato por simple referencia o remisión. Se trata de una cuestión de gran relevancia por su frecuencia y consecuencias prácticas.

El art. 5.4 de la Ley de Condiciones Generales de Contratación de 1998,

[2] CASTAN T., José. *Derecho Civil Español, Común y Foral*, tomo III. 10ª. ed., Madrid, 1967

establece que "*en todos 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 de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde contarán todos los términos de la misma*". Igualmente en el RD 1906/1999 de desarrollo reglamentario de dicha ley, se definen los requisitos con los que las condiciones generales se entienden incorporadas al contrato:

1. Informar al adherente sobre todas y cada una de las cláusulas del contrato.
2. La información ha de efectuarse con una antelación mínima de tres días naturales anteriores a la celebración del contrato.
3. Remitir al adherente, por cualquier medio adecuado a la técnica de comunicación a distancia utilizada, el texto completo de las condiciones generales.

Tales exigencias pueden resultar complicadas de cumplir en el ámbito de Internet, por lo que se considera satisfactoriamente cumplido el requisito:

1. Mediante la exposición permanente de las cláusulas del contrato en la web de la empresa oferente.
2. Con la exigencia de que condiciones estén disponibles para que el consumidor pueda almacenarlas y reproducirlas (art. 10.3. de la Directiva de Comercio electrónico). En el mismo sentido se expresa el art. 27.1 de la LSSICE.

8.1.2. Tiempo de la perfección del contrato

El contrato puede ser celebrado entre personas presentes y no presentes, dependiendo del medio adoptado para emitir las manifestaciones de voluntad. La utilización de medios electrónicos, en particular Internet, permite la posibilidad de celebrar contratos entre presentes y no presentes en la red, dependiendo de la tecnología utilizada[17]. Esto es así, puesto que el intercambio electrónico de datos[18] puede funcionar de forma instantánea o interactiva, o de manera que exista cierto margen de tiempo importante (desde minutos a horas).

Si se utilizan conexiones por medio de *redes punto a punto*[19], el sistema de intercambio electrónico de datos puede funcionar de manera instantánea o interactiva. En este caso, el momento de perfeccionamiento del contrato se regirá por las mismas reglas que para la contratación entre presentes.

Si, por el contrario, se utilizan conexiones por medio de *redes de valor añadido*[20] , en la cual los mensajes quedan guardados en la red de valor añadido en los buzones de cada usuario, el sistema de intercambio electrónico de datos, puede funcionar de forma no instantánea, en cuyo caso la contratación se considerará como una contratación entre personas no presentes y se aplicarán las reglas de la contratación por correspondencia.

En cuanto al momento de la perfección del contrato, es decir, cuando las manifestaciones de voluntad de las partes contratantes coinciden (oferta y aceptación), permite conocer a partir de qué momento el contrato existe, así como determinar cuál es la ley aplicable:

---

[17] Vid. BARCELÓ JULIÀ, R. *Comercio Electrónico*

[18] Sistema EDI (Electronic Data Interchange)

[19] La conexión por medio de una red punto a punto une las aplicaciones del ordenador emisor con las del ordenador receptor de forma directa.

[20] La red de valor añadido (red gestionada) permite que los usuarios se envíen mensajes, igual que si tuvieran una red punto a punto a través del sistema de intermediación de mensajes. Este sistema opera así: el centro de compensación al recibir un mensaje lo deposita en el buzón del sujeto que aparece como destinatario, donde el mensaje permanece hasta que el destinatario decida acceder al mismo.

- a la capacidad de las partes contratantes,
- en el supuesto de modificaciones legislativas ocurridas durante la formación del contrato, determinar los plazos de prescripción, el límite de la retroactividad en el caso de contratos sometidos a condición, la transferencia de los riesgos de la cosa objeto del contrato, los precios del mercado o la rescisión de los contratos hechos en fraude de los acreedores[3] , etc. (Aspecto este bastante improbable en el ámbito de la Contratación Electrónica, caracterizada por la velocidad en la ejecución[4]).

El artículo 1262 del Código Civil afirma: "El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que ha de constituir contrato".

Este primer supuesto del artículo recoge el momento de la formación del consentimiento como elemento esencial para la formación del contrato, según el cual han de concurrir oferta y aceptación sobre la cosa y la causa del contrato.

8.1.3. Teoría de la emisión, declaración o manifestación.

Según esta teoría el contrato se considera perfecto desde el instante en que el aceptante emite su declaración de voluntad.

- El artículo 54 del CCo establece "los contratos que se celebren por correspondencia quedan perfeccionados desde que se conteste aceptando la propuesta o las condiciones con que ésta fuere modificada" En este caso el legislador atiende a la Teoría de la

[3] DÍEZ PICAZO, L., *Fundamentos de Derecho Civil Patrimonial*. Madrid, 1993, 4ª ed.
[4] BARCELÓ JULIÀ, R. *Comercio Electrónico entre empresarios. La formación y prueba del Contrato Electrónico (EDI)*. Tirant lo blanch, Valencia, 2000.

Emisión (declaración), al señalar "...que se conteste aceptando la oferta o las condiciones..."[11]

8.1.4. Teoría de la expedición, comunicación, remisión o desapropiación

El contrato nace desde el momento en que el aceptante expide su aceptación, pues se considera que al dejar de situarse tal declaración en la esfera de acción del aceptante y trasladarse a la esfera del oferente, el aceptante ya ha hecho todo lo que estaba en sus manos para dar nacimiento al contrato. Teoría recogida por el Código de Comercio.

8.1.5 Teoría de la recepción

El nacimiento del contrato se produce cuando la aceptación llega al ámbito o esfera del oferente, sin que sea necesario su conocimiento.

Como el Código de Comercio nada dice al respecto, por remisión del artículo 50 del Cco. al Código Civil se aplicará el mismo lugar establecido en el artículo 1262.2 CC, es decir, el lugar en que se hizo la oferta. No obstante, algunos autores[12] consideran que esto es contrario al espíritu del Código de Comercio y que por ende debe considerarse el lugar de la formación del contrato el mismo lugar en que se emite la aceptación.

---

[11] Este criterio no es unánime. Algunos autores consideran que el Código de Comercio sigue la teoría de la expedición (mailbox rule), cfr. Puig Brutau, J. ob cit. p. 193, y STS de 21 de febrero de 1994 (RJ 1994, 1102).

[12] SÁNCHEZ CALERO. *Instituciones de Derecho Mercantil*. Madrid, 15ª ed., 1999, p. 444; Menéndez Mato

El Modelo Europeo de Acuerdo de EDI[24] , establece en su artículo 3.3 la teoría de la recepción, al señalar: "Un contrato celebrado mediante el EDI se considerará celebrado en el lugar y momento en que el mensaje de EDI que contenga la aceptación de una oferta llegue al sistema informático del oferente"[25] .

Este modelo ofrece a las partes la posibilidad de pactar la obligación de enviar un acuse de recibo. Si se ha pactado y se ha acusado el recibo, la perfección del contrato se produce con la simple recepción de la aceptación y el recibo tendrá una finalidad probatoria.

El Modelo de acuerdo de intercambio de la American Bar Association. La sección 2.3 del Modelo señala: "Si el apéndice al acuerdo de intercambio especifica que ante el envío de un tipo de documento, el receptor debe enviar un documento de aceptación, este documento no dará lugar a ninguna obligación a menos que la parte trasmisora del mismo haya recibido el mencionado documento de aceptación".

Debe entenderse que la correcta recepción se produce cuando los mensajes sean accesibles en el ordenador de la parte receptora designado para la recepción de los mensajes.

Este modelo fija la obligación de enviar un acuse de recibo, lo cual constituye una prueba de la existencia del contrato, pero no modifica el momento de perfección del mismo.

8.1.6. Teoría de la cognición, conocimiento o información

En este sistema el contrato nace cuando el oferente tiene efectivo conocimiento de la aceptación. Se fundamenta en el principio de que toda declaración de voluntad es eficaz desde el momento que llega a su destinatario.

---

[24] Vid. DOCE No. L 338/98 de 28 de diciembre de 1994.
[25] La teoría d la recepción permite evitar en gran medida el riesgo de que las distintas legislaciones -de países miembros- entren en conflicto en relación con el uso del EDI.

Ahora bien, el artículo 1262 en su segundo párrafo señala "La aceptación hecha por carta no obliga al que hizo la oferta sino desde que llegó a su conocimiento. El contrato en tal caso se presume celebrado en el lugar en que se hizo la oferta". La frase "sino desde que llegó a su conocimiento" hace referencia a la Teoría de la Cognición (conocimiento), es decir, no basta para el perfeccionamiento del contrato que la aceptación haya llegado al domicilio (teoría de la recepción) sino que además se requiere que el oferente se haya enterado del contenido de la comunicación en la cual consta la aceptación, salvo que el aceptante pruebe que el oferente no la conoció por falta de diligencia.

Por tanto, entre personas distantes, el momento de perfección del contrato será el de conocimiento de la aceptación por parte del oferente; y el lugar de perfeccionamiento del contrato, el lugar en que se hizo la oferta.

No obstante, este criterio ha sido matizado por el Tribunal Supremo en diversas sentencias[10] , interpretando que el artículo 1262.2 del CC recoge la "Teoría de la Recepción" atenuada con una presunción de conocimiento, esto es, que se presume que el oferente tiene conocimiento de la aceptación cuando la correspondencia entra dentro de su círculo o ámbito de intereses.

De esta forma, se observa que en materia mercantil se justifica la aplicación de la Teoría de la Emisión (declaración) por las exigencias de rapidez del tráfico comercial; en materia civil, la aplicación de la Teoría de la Recepción y el Conocimiento favorecen la seguridad jurídica.

Estos sistemas pueden a su vez estar combinados[9] y dar lugar a nuevas teorías, como las siguientes:

8.1.7. Teoría de la cognición presunta.

[10] Cfr. STS del 7 de noviembre de 1976, del 12 de julio de 1979 y del 22 de diciembre de 1992.
[9] Idem p. 246.

Considera que el contrato celebrado por correo o telegrama se concluye en el momento y en el lugar en que el oferente tenga conocimiento de la aceptación, se entiende que existe este conocimiento cuando llega la aceptación a la dirección del oferente, salvo que el oferente demuestre, que sin su culpa, le fue imposible tener acceso a ella.

8.1.8. Teoría mixta entre expedición y cognición

Según este sistema, el contrato en relación con el oferente se perfecciona en el momento de la expedición de la aceptación (*mailbox rule*), pero en relación con el aceptante el contrato está concluido cuando su aceptación sea conocida por el oferente (teoría de la cognición).

La Oferta y la Aceptación

8.2 La oferta

La oferta es una declaración de voluntad a través de la cual se propone la celebración de un contrato, el cual debe contener todos los elementos esenciales, tales como el precio de los productos o servicios, el plazo de duración de la oferta y los demás requisitos propios del mismo.

En relación con Internet, no toda oferta comercial de un proveedor hecha en este entorno electrónico va a constituir en rigor una declaración de voluntad contractual. Para que realmente estemos ante una oferta vinculante, se requiere que ésta contenga determinados datos que se consideran fundamentales El Convenio de Viena establece que debe ser una oferta "suficientemente precisa", exteriorizarse de algún modo y reflejar la indubitada voluntad del oferente de vincularse contractualmente.

En Internet la oferta ofrece algunas peculiaridades puesto no suele ir dirigida a destinatarios determinados. La doctrina mayoritaria considera que, si la oferta expuesta en la página web no contiene el dispositivo técnico de aceptación, o la misma es incompleta, no se trata de una oferta. Se puede distinguir así entre *webs* activas y pasivas, siendo pasivas las que se limitan a exhibir y publicitar sus productos/servicios, mientras que las activas promueven la comercialización de los mismos.
Esta actuación diferenciada provoca consecuencias jurídicas distintas en uno y otro caso:

- En el caso de las *webs* pasivas, los anuncios por sí solo no vinculan al oferente, lo cual no impedirá que el cliente potencial pueda efectuar el correspondiente pedido, dando lugar a la efectiva celebración del contrato.
- En las *webs* activas su oferta tendrá carácter vinculante para el oferente, lo que le obliga a contratar en las condiciones ofrecidas en tanto no las revoque o modifique.

Se trata normalmente de una proposición unilateral que una de las partes dirige a la otra para celebrar con ella un contrato. No se trata de un acto preparatorio sino de una declaración contractual, a través de la cual el contrato puede entenderse cerrado con la sola aceptación de la otra parte, sin necesidad de una posterior declaración del que hizo la oferta[5]. La oferta debe ser completa, es decir, ha de contener todos los requisitos esenciales al contrato, para que pueda quedar perfeccionado con la sola aceptación del destinatario y ha de dar a conocer al destinatario la firme voluntad de obligarse del oferente. Si la proposición se ha emitido con la reserva del oferente (acompañada por ejemplo de cláusulas "salvo confirmación") entonces no se tratará de una verdadera oferta. Esta proposición (oferta) va dirigida a la otra parte

[5] PUIG BRUTAU, J. *Fundamentos de Derecho Civil. Doctrina General del Contrato*. Tomo II. Vol. 1. 3ª ed. ed. Bosch, Barcelona, 1988

con quien se pretende celebrar el contrato[6], quien deberá emitir la aceptación.

La LSSICE define la comunicación comercial como "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", concepto equivalente al de publicidad comercial, de ahí que se imponga la obligación de identificarlas como tales con la palabra "publicidad" al objeto de distinguirlas de las comunicaciones meramente informativas.
La misma ley, en su art. 21, prohíbe la práctica del *spamming*, o envío de publicidad no solicitada o autorizada previamente por el destinatario, medida que coloca a los oferentes españoles en situación de desventaja en relación con otros prestadores de servicios, en especial del ámbito comunitario.[43]

Con respecto a las comunicaciones comerciales y las ofertas publicitarias, el art. 8.1 de la LGDCU DE 1984 establece que el contenido de las ofertas o promociones publicitarias "serán exigibles por los consumidores aun cuando no figuren expresamente en el contrato celebrado o en el documento o justificante recibido", (concepto de "integración publicitaria del contrato").

Por su parte, el art. 27 de la LSSICE (trasposición del art. 10 de la Directiva

[6] El artículo 14 de la Convención de Viena señala: " 1) La propuesta de celebrar un contrato dirigida a una o varias personas determinadas constituirá oferta si es suficientemente precisa e indica la intención del oferente de quedar obligado en caso de aceptación. Una propuesta es suficientemente precisa si indica las mercaderías y, expresa o tácitamente, señala la cantidad y el precio o prevé un medio para determinarlos..."
[43] Guisado Moreno, Ángela: "Formación y perfección del contrato en Internet", Marcial Pons, año

de Comercio electrónico) establece unos requisitos obligatorios para el prestador del servicio antes de realizarse el contrato: los trámites que deben seguirse para celebrar el contrato, si el prestador va a archivar el documento electrónico en que se materialice el contrato y si éste va a ser accesible, los medos técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, la lengua o lenguas en que podrá formalizarse el contrato, etc.

A su vez, la Ley de Comercio Minorista (art. 40) establece la obligación que tiene el vendedor de suministrar al consumidor de manera clara y veraz y utilizando cualquier técnica adecuada al medio de comunicación a distancia utilizado, datos como: identificación del vendedor, características esenciales del producto, precio impuestos incluidos, gastos y forma de entrega y transportes, plazo de validez de la oferta, etc.

8.3 La aceptación [44]

La aceptación de una oferta es la manifestación de consentimiento del destinatario con los términos en que ha sido formulada aquélla y de la manera propuesta o autorizada por el oferente. Es decir, se exige la coincidencia total entre la oferta y la aceptación. Este requisito propio de la aceptación se denomina “regla del espejo”.

No obstante, pueden existir distintas fórmulas de aceptación, las cuales se detallan a continuación:

8.3.1. Aceptación que modifica la oferta.

Si el receptor de la oferta desea cambiar los términos en que se le ha presentado, la aceptación así emitida sólo tendrá el valor de una nueva

[44] servicio.estudios@eVeritas.com

oferta (contraoferta). El art. 54 del Código de Comercio señala en relación con los Contratos celebrados por correspondencia, que la perfección del contrato tiene lugar "desde que se conteste *aceptando la propuesta o las condiciones con que ésta fuera modificada*". Significa que la verdadera aceptación es aquella que no requiere a su vez ser aceptada por el oferente.

8.3.2. Invitación a ofrecer.

Sucede cuando la parte que toma la iniciativa en la negociación contractual no formula una verdadera oferta sino que invita a otros a que la formulen. Por ejemplo, las manifestaciones hechas en los catálogos, los bienes de consumo expuestos en un supermercado, no son verdaderas ofertas sino que constituyen una invitación a contratar. (Argumento en contrario sostiene la Ley de Ordenación del Comercio Minorista, en su artículo 9.1). Esta "invitación a ofrecer" es especialmente importante en la Contratación Electrónica, puesto que la red se presenta como un atractivo lugar para fijar publicidad, bien a través de catálogos en tiendas o a través de *links* que llevan a otras páginas que ofrecen bienes de consumo.

8.3.3. Revocabilidad de la Oferta.

Para que el contrato se considere perfeccionado la aceptación debe manifestarse a quien ha formulado la oferta y no tiene que alterar los términos en que ha sido formulada. Asimismo, es necesario que la aceptación tenga lugar antes de que la oferta caduque o sea revocada. En el primer caso, la oferta estaría sometida a un término; en el segundo caso, es una facultad del oferente revocar la oferta hasta tanto el contrato no se considere perfecto.

En relación con la revocabilidad de la Oferta, cabe distinguir dos supuestos:

1. El oferente pueda revocar la oferta antes de la aceptación, y aun después de ella antes de su recepción: Este supuesto determina la perfección del contrato, puesto que las teorías que explican la perfección del Contrato se basan en los sistemas de la expedición o de la recepción de la aceptación.

2. El oferente esté obligado, independientemente de que el destinatario haya aceptado, a no revocar la oferta durante un cierto plazo: se refiere a la revocabilidad del elemento intrínseco a ella, independiente de la existencia o no de aceptación.

Para este último supuesto, dos son los sistemas:

a) Los que establecen que el oferente no podrá revocar la oferta hasta que el destinatario la haya rechazado o haya dejado transcurrir sin aceptarla el tiempo suficiente para considerar razonable la revocación, como el Código Civil Alemán (δ δ 145-149); y

b) Los que consideran que la oferta es revocable mientras el contrato no se haya perfeccionado (Sistema del Derecho Francés y de todos los Códigos de tradición Latina). En el Código Civil Italiano, este sistema tiene un matiz, puesto que si el aceptante ha emprendido de buena fe la ejecución del contrato antes de haber tenido conocimiento de la revocación, el proponente ha de indemnizarle los gastos y las pérdidas sufridas por la iniciada ejecución (art. 1328). En el Derecho Francés este principio también se mitiga, pues se considera que el plazo debe darse por admitido cuando resulte impuesto por los usos, como sucede en materia comercial.

En cualquiera de los dos sistemas, siempre que el oferente se obligue a mantener la oferta por un tiempo determinado, la revocación carece de efecto durante ese plazo.

Ni el Código Civil ni el Código de Comercio español contienen una disposición expresa sobre la revocabilidad o no de la oferta. La jurisprudencia ha sostenido que "es doctrina científica comúnmente admitida que la oferta puede ser revocada mientras el contrato no se haya perfeccionado"[7]

No obstante lo anterior, el criterio universalmente aceptado es el de la recepción de la aceptación: Convenio de Viena de 1980 art. 18.2; Principios UNIDROIT art. 2.6 ó art. 2205 de los Principios del Derecho Europeo de los contratos de 1999-2000. Así mismo, la Ley 41/1999 sobre sistema de pagos y de liquidación de valores art. 11 adopta el criterio de la recepción. También la LSSICE art. 28 obliga al oferente a confirmar la recepción de la aceptación. [45]

8.4. Lugar de perfeccionamiento del contrato

Teniendo en cuenta que la contratación electrónica se realiza entre personas no presentes, tiene especial relevancia determinar el lugar de perfeccionamiento del contrato, lo cual permitirá determinar los tribunales competentes y el derecho aplicable.

Entre personas presentes físicamente, el momento de nacimiento de la relación contractual viene determinado por el momento del intercambio de las manifestaciones "oferta y aceptación", coincidentes en tiempo y espacio.

Aunque el CC y CCo establecen que "el contrato... se presume celebrado en el lugar en que se hizo la oferta", la LSSICE prevé para los contratos celebrados vía electrónica con consumidores, que se

[7] Vid. STS de 29 de octubre de 1956.
[45] Guisado Moreno, Ángela: "Formación y perfección del contrato en Internet", Marcial Pons

presumirán celebrados en el lugar en que éste tenga su residencia habitual; para los celebrado entre profesionales y salvo pacto contrario, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

8.5. Las partes en la contratación mercantil electrónica

8.5.1. Capacidad

En lo que respecta a la capacidad de las partes contratantes, al igual que en la contratación tradicional, serán de aplicación las reglas establecidas en el Código Civil art. 1263 y ss., relativas a la capacidad para contratar y los efectos que la concurrencia de error, violencia, intimidación o dolo tienen sobre los respectivos contratos. Si bien con las peculiaridades que los entornos virtuales propician.

A través de la firma electrónica reconocida se resuelven ciertas dudas sobre la capacidad de las partes, en la medida en que el prestador de servicio de certificación pueda tener acceso al dato de la capacidad de obrar del futuro signatario, si bien el firmante es libre de facilitar los datos relativos a su capacidad, salvo en el caso de certificados reconocidos.

8.5.2. Sujetos parte

A estos efectos, conviene recordar lo ya expuesto en el apartado sobre Comercio electrónico referente a los sujetos intervinientes en el comercio electrónico y los tipos básicos de relaciones que se establecen en este entorno, donde los contratos se celebran entre personas distantes o sin la presencia simultánea de los sujetos contratantes:

a. EMPRESAS: Entre empresas o B2B (*business to business*)

b. CONSUMIDORES: Entre empresas y consumidor o B2C (*business to consumers*)

c. ADMINISTRACIÓN: Entre empresas y Administración o B2A (*business to Administrations*)

d. PRESTADORES DE SERVICIOS DE CERTIFICACION

e. LA ACTUACIÓN MEDIANTE REPRESENTACION [46]

Hay que añadir a estos sujetos a aquellos que, igual que en la contratación tradicional, actúan por cuenta y en nombre de un tercero, lo que necesariamente sucede en las sociedades mercantiles.

A estos efectos se aplican las mismas normas del Derecho de obligaciones y contratos con los ajustes exigidos por el entorno electrónico.

La Ley de Firma Electrónica admite en su art. 7 la posibilidad de que soliciten certificados electrónicos de personas jurídicas sus administradores y representantes legales o voluntarios con poder bastante a estos efectos. En estos casos quien queda obligado por la firma electrónica es la persona jurídica a quien corresponde, siempre que asuma el acto como propio o el mismo se hubiera celebrado en su interés. En caso contrario los efectos del acto recaerán sobre la persona física firmante.

Acreditada la existencia de un falso representante, le serán imputados los efectos de su propia actuación según el art. 1727.2

[46] Guisado Moreno, Ángela: "Formación y perfección del contrato en Internet", Marcial Pons

CC, sin perjuicio de la correspondiente responsabilidad del titular de la firma electrónica por negligencia en su conservación.

f. AGENTE ELECTRÓNICO

La Ley Modelo de comercio electrónico tipifica el "agente electrónico" como un sistema de información programado para operar automáticamente, si bien de su actuación se derivan consecuencias jurídicas para el sujeto titular de los correspondientes sistemas y equipos electrónicos. En este sentido no es un representante en sentido estricto, sino que actúa como un *alter ego* del titular del sistema. Obviamente hay que considerar parte contratante, a quien deben imputarse los correspondientes efectos jurídicos, al sujeto que lo programa (o por cuya cuenta se programa).

En la práctica la actuación mediante agente electrónico conduce a que se vean considerablemente mermadas las posibilidades de negociación entre las partes contratantes, al no mantener éstas un contacto directo.

g. INTERMEDIACION NOTARIAL

Aunque no existe todavía una reglamentación específica de la fe pública en la contratación electrónica, puede admitirse ésta de acuerdo con lo previsto en el art. 55 CCo, el cual admite la posibilidad de que un agente o corredor intervenga en la formación del contrato electrónico actuando como mediador entre las partes y aproximando las posiciones de éstas de cara a la perfección de dicho contrato.

No obstante, tampoco habrá representación en sentido estricto pues, en rigor, el fedatario mercantil no actúa en representación de las partes sino intermediando entre ellas.

8.6. La forma en la contratación electrónica

En primer lugar, es conveniente precisar que en el ámbito de la contratación electrónica, la calificación del contrato mercantil como contrato entre presentes o entre ausentes va a depender de aspectos puramente tecnológicos.

Si la tecnología permite la comunicación instantánea entre las partes (videoconferencia o similares) no existiendo distancia temporal entre la emisión y la recepción de los mensajes, cabría aplicar las reglas de contratación entre presentes (similar a la contratación telefónica). No es ésta, en cualquier caso, la forma habitual de comunicación aunque tal vez lo sea en un futuro cercano.

La generalidad de los contratos que hoy se celebran en Internet y en los contextos electrónicos en general han de ser considerados como contratos a distancia y de formación sucesiva, de acuerdo con la legislación actual en la materia.

Si bien en Internet no existen normas que limiten la configuración de los mensajes, ello no impediría que quienes mantienen relaciones comerciales en ese medio puedan utilizar soluciones como las del entorno EDI, donde la información que se transmite está estructurada conforme a una norma técnica que previamente ha sido convenida por las partes, tal y como establece la Ley Modelo de Comercio Electrónico de UNCITRAL art. 2.b); todo ello con el objeto de limitar el acceso a terceros, aumentando su seguridad.

No obstante, el principio de libertad de forma cuenta con una larga tradición en nuestro Derecho, por lo que los efectos jurídicos de las declaraciones de voluntad emitidas por las partes con el fin de preparar y celebrar el contrato son los mismos, independientemente de que se

efectúen por medios orales, escritos o electrónicos.

Dicha libertad de forma queda establecida en la siguiente normativa:

1. el art. 51 CCo dice: “serán válidos y producirán obligación y acción en juicio los contratos mercantiles, cualesquiera que sea la forma y el idioma en que se celebren, la clase a la que correspondan y la cantidad que tengan por objeto, con tal que conste su existencia por cualquiera de los medios que el Derecho civil tenga establecidos…”.
2. Así mismo, el art. 1278 del CC dispone que “los contratos serán obligatorios cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez”… (consentimiento, objeto y causa, art. 1261 CC).
3. La libertad de forma tiene la excepción prescrita en el art. 52 del Código de Comercio respecto de aquellos contratos que exijan algún requisito especial de forma solemne conforme al Derecho español o del Derecho del lugar en que se celebren (por ejemplo, que requieran escritura pública).
4. La LSSICE en su art. 23 equipara la forma electrónica a la forma escrita, y sólo excluye la posibilidad de celebrarse por esa vía los contratos, negocios o actos jurídicos relativos al Derecho de familia y sucesiones, añadiendo además que los contratos para los que se requiera la forma documental pública, o que requieran por ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica (art. 23.4).

Con todo, el reconocimiento legal de la validez de los contratos electrónicos no impedirá que, en la práctica se planteen numerosos

problemas en torno a la aplicación de los mismos.

8.6.1. El problema de la atribución

Partiendo de la base de que los entornos virtuales propician el anonimato, la suplantación de nombres, equipos y sistemas electrónicos e, incluso, de las firmas electrónicas, se plantea el problema de determinar la persona concreta a la que han de atribuirse los efectos jurídicos y el alcance real de una declaración de voluntad emitida por medios electrónicos, y en particular a través de Internet.

Los problemas más comunes que pueden plantearse giran en torno a:

a) la autenticidad de las declaraciones negociales electrónicas, es decir, la dificultad de saber a ciencia cierta si la declaración recibida por un determinado sujeto procede de quien aparece como su autor. Y en particular los supuestos de suplantación, consecuencia de la "apropiación" de la firma electrónica ajena de forma no consentida o ilegítima. No cabe equiparar estos casos con los de falsedad de la firma, dado que no se finge propiamente ninguna firma sino que se limita a utilizar una determinada clave asignada a otro sujeto.

En los casos de voluntad suplantada habrá de negarse la constitución de vínculo jurídico válido por faltar el elemento esencial de la voluntad contractual. No obstante, la contraparte quedaría desprotegida con esta solución ya que razonablemente y con buena fe confió en el certificado expedido por el prestador de servicios de certificación. Así pues, será el prestador de servicios de certificación quien deberá responder tanto frente al titular de la firma electrónica suplantada como frente a la contraparte receptora de la declaración electrónica. [47]

[47] J.M. EMBID IRUJO "*Eficacia de la voluntad suplantada por utilización de la firma digital". Revista de la contratación electrónica nº 14, 2003.*

b) la integridad de su contenido, es decir, la posibilidad de que el contenido de una declaración negocial electrónica resulte modificado o alterado después de suscrita ésta.

c) los relacionados con el rechazo o repudio de dichas declaraciones, es decir, si una vez realizada una declaración negocial electrónica la parte interesada niegue haberla hecho.

d) la consideración de "contratos originales" [48]

Dada la posibilidad de alteración sin dejar rastro de los archivos electrónicos, la determinación de qué debe considerarse original cobra especial trascendencia, puesto que la posibilidad de alteración es evidente en el caso de no utilización de firmas electrónicas por las partes; e incluso en el supuesto de su utilización, la evolución tecnológica puede dar lugar a que se produzcan alteraciones indetectables en contratos firmados electrónicamente.

El Acta Norteamericana de firma electrónica de fecha 1 de octubre de 2000, considera como original del contrato electrónico el ejemplar electrónico del mismo que habiendo sido archivado, refleje con exactitud la información contenida en el contrato y permanezca accesible a las personas que tienen derecho a dicho acceso en una forma susceptible de ser reproducida con exactitud para su posterior referencia, ya sea por transmisión, impresión o de otra forma.

Establece igualmente que puede negarse el cumplimiento del requisito de un contrato por escrito a un contrato electrónico si este no está en una forma susceptible de ser archivada y reproducida con exactitud para ulterior referencia por todas las partes o personas con derecho a archivar el contrato. (Sección 101 d) y e).)

La tradición jurídica española atribuye especial importancia a la intervención de terceros independientes en el contrato a la hora de

[48] www.ventanalegal.com

determinar su contenido real en el caso de discrepancias de los ejemplares que presenten las partes. Igualmente los contratos archivados por terceros independientes de las partes gozan, en derecho español, de especial trascendencia jurídica (Protocolo Notarial, Registros públicos...).

La solución propuesta por la LSSI: "Sin perjuicio de lo establecido en el art. 21 de esta Ley, en caso de discrepancia entre diversos ejemplares de un mismo contrato electrónico se considerará como el original aquél al que las partes hubieran atribuido tal carácter en el momento de su celebración, o posteriormente, y haya sido archivado por un tercero independiente de las partes manteniéndose accesible para su ulterior consulta." [49]

Los mecanismos de solución de todos estos problemas han sido aportados por:

1. La firma digital, a cuyo epígrafe en este trabajo me remito.

2. El acuse de recibo y la confirmación post contractual.

Cuando una de las partes recibe de la otra el acuse de recibo, adquiere la certeza de que la comunicación que pretendía condicha parte se ha logrado. A este respecto la LSSICE en su art. 28 impone al oferente la obligación de enviar al aceptante un acuse de recibo en el plazo de las veinticuatro horas siguientes a la aceptación o, alternativamente, una confirmación. Esto sólo es ineludible en relaciones de consumo; para las relaciones inter-empresariales se admiten pactos en contra.

No se debe confundir el acuse de recibo con el mero registro electrónico que el sistema de información puede efectuar y que

[49] www.ventanalegal.com

pueden proporcionar los proveedores de servicios intermediarios.
En cualquier caso, la omisión del acuse de recibo en los casos en que es obligatorio no impedirá la perfección del contrato.

8.7. DERECHO APLICABLE A LOS CONTRATOS ELECTRONICOS

El Derecho del comercio electrónico abarca no sólo el Derecho privado de obligaciones y contratos, sino también normas de muy variada naturaleza y procedencia, que forman un conjunto normativo heterogéneo y poco sistemático, con ausencia de normas de validez universal que den respuesta a la extensa problemática planteada.

En cuanto al carácter mercantil de los contratos electrónicos, siguiendo a la doctrina mayoritaria, cabe admitirlo cuando concurra cualquiera de las circunstancias siguientes:
a) que se trate de contratos comprendidos en el propio Código de Comercio o en leyes mercantiles especiales
b) que se trate de actos de empresa, aún cuando sean atípicos.[50] Lo relevante será la intervención en dicho contrato de, al menos, un prestador de servicios, como sujeto que actúa en la esfera de su actividad profesional o empresarial. [51]

Actualmente conviven convenios internacionales con normas nacionales y normativa comunitaria, así como el fenómeno de la autorregulación en relación con la actividad comercial en la Red y cuya

[50] J.GÓMEZ CALERO, "*El contrato mercantil: nociones generales*"

[51] M. S. FLORES DOÑA, "Impacto del comercio electrónico en el Derecho de la Contratación"

importancia es clave pues responden a la necesidad de evitar los riesgos de inseguridad jurídica y que adoptan la forma de una nueva *lex mercatoria.*[52]

Normativa

En el ámbito español, la principal norma sobre la materia es la

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), que, en su Anexo de Definiciones, letra *h*) entiende que lo es "*todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones*". En todo caso, cualquier definición deberá estar en línea con el concepto legal de contrato que ofrece nuestro Código Civil en su art. 1254: "El contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o a prestar algún servicio".

Así mismo, son aplicables:

- El Código Civil
- El Código de Comercio
- La Ley 7/1996 de Ordenación del Comercio Minorista, LOCM en su artículo 40, regula el contenido de las ofertas de venta a distancia, condiciones que deben aplicarse dentro del ámbito de la contratación electrónica. Estos requisitos son:

    a) Identidad del proveedor

    b) Características especiales del producto

    c) Precio

[52] R. ILLESCAS ORTIZ, Derecho de la Contratación electrónica. La Ley, Biblioteca de los negocios, 2001

d) Gastos de transporte

e) Forma de pago

f) Modalidades de entrega o de ejecución

g) Plazo de validez de la oferta.

- La Ley 7/1998 sobre Condiciones Generales de Contratación
- Real Decreto-Ley 14/1999 de Firma Electrónica
- La Ley de Firma Electrónica de 2003.
- El Código de Comercio de 1885 y otras leyes de naturaleza mercantil que
  resulten de aplicación.
- Ley General de Telecomunicaciones 32/2003
- Ley de la Propiedad Intelectual, en vigor desde 1996
- Reglamento de Medidas de Seguridad de los Ficheros Automatizados R.D. 994/1999
- Reglamento de Contratación Telefónica y Electrónica

De origen internacional son los dos convenios de obligada referencia, habida cuenta que la compraventa es la institución central del comercio exterior:

- Convenio de Viena de 11 de abril de 1980, sobre el Contrato de Compraventa Internacional de Mercancías, de aplicación a los contratos mercantiles de carácter internacional, cuando carezcan de una regulación específica.
  El artículo 18.2 señala: "la aceptación de la oferta surtirá efecto en el momento en que la aceptación de asentimiento llegue al oferente". Este precepto contiene un pronunciamiento a favor de la "teoría de la recepción".

De igual forma, el artículo 23 señala: “El Contrato se perfeccionará en el momento de surtir efecto la aceptación de la oferta conforme a lo dispuesto en la presente Convención”.

También son reseñables en el ámbito Comunitario las Directivas:

- Convenio de Roma de 19 de junio de 1980, sobre la Ley aplicable a las obligaciones contractuales, normativa general de los contratos mercantiles internacionales en los Estados comunitarios.

- La Directiva 2000/31/CE de 8 de junio, establece en su art. 9.1 que “*los Estados Miembros garantizarán, en concreto, que el régimen jurídico aplicable al proceso contractual no entorpezca la utilización de los contratos por vía electrónica, ni conduzca a privar de efecto y de validez jurídica a este tipo de contratos en razón de su celebración por vía electrónica*”. No obstante, también incluye en su art. 9.2 una serie de contratos que podrán excluir del ámbito de la contratación electrónica de sus respectivas legislaciones interna, como, por ejemplo, los contratos de creación o transferencia en materia inmobiliaria, excepto los arrendamientos.

  La Directiva sigue en este sentido los preceptos del Convenio de Viena de 1980 sobre el Contrato de Compraventa internacional de Mercaderías.

- Directiva 1999/93/CE de 13 de diciembre, sobre Firma Electrónica, desarrollado en este trabajo en el epígrafe del mismo nombre.

Existen otras normas procedentes de los sectores interesados en el tráfico mercantil internacional (organizaciones empresariales, cámaras

de comercio, instituciones sectoriales...), que no tienen carácter vinculante y que basan su fuerza de obligar en la autonomía de la voluntad de las partes. Proceden de instituciones como la UNCITRAL o la Cámara de Comercio Internacional y viene a formar parte de la nueva *lex mercatoria.* Entre ellas cabe destacar:

- La Ley Modelo sobre comercio electrónico de 1996 elaborada por la Convención de las Naciones Unidas para el Contrato Internacional de Mercancías.
- La Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, de 9 de diciembre de 2005
- El Modelo Europeo de Acuerdo EDI, aprobado por la Comisión Europea en 1994 con carácter de recomendación.
- Las Reglas UNCID de la CCI de 1987. Incluyen usos y costumbres. Tienen carácter de recomendación.
- Los Principios UNIDROIT de 1995, importante instrumento alternativo de unificación jurídica, elaborados por el Instituto Internacional para la Unificación del Derecho Privado.
- Los Principios del Derecho Europeo de los Contratos, muy similares a los UNIDROIT.

Para finalizar, es destacable la decisión adoptada por la Organización Mundial del Comercio y, por extensión, la Unión Europea de no crear impuestos especiales para las transacciones que se realizan a través de Internet, pero sí se aplicarán los impuestos propios de cada país, como el IVA u otros gravámenes adicionales en el punto de destino.[53]

[53] Rodrigo González, Oscar: "Guía práctica del Comercio electrónico", Editorial Anaya, 2008.

9. FACTURA ELECTRÓNICA

La facturación es una fase obligatoria dentro proceso habitual de las relaciones comerciales, una vez realizada la venta.

La importancia de este documento se ha manifestado no sólo en su regulación exhaustiva en la legislación española, sino en el interés que las Autoridades Comunitarias le han conferido al considerarla un instrumento fundamental en el proceso de formación del Mercado Único. A ello ha contribuido un informe del "Grupo de Expertos de la Factura Electrónica" de la Comunicad Europea realizado en colaboración con "Fiscalis", del que incluyo, resumidos, algunos apartados significativos (versión original en inglés, traducción propia):

9.1. Informe sobre la e-factura [54]

- El informe presenta una visión del entorno de la e-factura, en el cual las partes pueden inter-operar en un ecosistema abierto basado en la armonización de las previsiones legales y una mayor estandarización. El entorno podría ser atractivo en particular a las pequeñas y medianas empresas. Las Administraciones públicas deberán tomar medidas para ayudar a crear el entorno adecuado.

- Con objeto de explicar el porqué del cambio en las prácticas comerciales en toda Europa, es importante analizar y comunicar

(1) [54] Internacional-EC Expert Group on eInvoicing. Versión original en inglés, traducción propia.

(2)

los beneficios de la innovación. Dichos beneficios afectarán a unos 24 millones de empresas, incluyendo grandes corporaciones y pequeñas y medianas empresas, así como a todos los usuarios de Internet entre los ciudadanos de la Unión Europea.

En Europa, se ahorrarán más de 200 billones de Euros anuales gracias únicamente a los procesos electrónicos de facturación *business-to-business* (sin mencionar el enorme potencial de la facturación *business-to consumer*):

- El potencial de reducir las emisiones de CO2 por encima de los tres millones de toneladas anuales.

- Liberación de los recursos favoreciendo un incremento del trabajo productivo necesario para aumentar la productividad, necesaria y acentuada, dadas las tendencias demográficas actuales (envejecimiento de la población y reducción de la fuerza productiva).

- La Factura electrónica no es un fin en sí mismo, sino un paso hacia la digitalización de todos documentos de la cadena general de procesos, así como para promover la innovación.

- La Factura electrónica podría también apoyar la migración al SEPA (*Single Euro Payments Area*) basado en la futura automatización de pagos.

- La Factura electrónica tiene el potencial de reducir el fraude en las facturas mejorando los controles del IVA y permitiendo el uso de las técnicas de e-auditoría, las cuales necesitan promocionarse para ser adoptadas más ampliamente.

- La armonización legal aumentará las posibilidades de transferir las

técnicas entre los Estados Miembros.

- Incluso si la facturación puede parecer un proceso pequeño dentro de un contexto general, es una parte esencial de la cadena de desarrollos positivos que tienen por objeto el futuro Mercado Único.

- Muchos de los argumentos expresados pueden considerarse suficientemente poderosos en sí mismos pero tomados en su conjunto está claro que expresan que la rápida adopción y migración hacia la e-factura debería recibir la más alta prioridad posible.

  Favorable costo-beneficio y facilidad de uso

  La efectividad del costo-beneficio significa que el uso de la e-factura reduce el coste total para todos los participantes en el proceso, comparado con la factura en papel. El análisis del proceso de negocio ha mostrado que las reducciones en costo son a menudo superiores para el receptor de la factura que para el emisor.

  Sin embargo, los modelos de negocio y su implementación deberían diseñarse para proporcionar beneficios a todos los participantes.

  Las soluciones de e-factura deben ser fáciles de usar, de buscar, mantener e implementar, y deben funcionar bien integradas en los sistemas internos de los participantes; en caso contrario no serían adoptadas ampliamente por millones de empresas y de hogares.

9.2. Recomendaciones propuestas a la Comisión Europea por el Grupo de Expertos, mediante un documento fechado el 3 de julio de 2008:

- Las facturas de papel y las electrónicas deben recibir igual

tratamiento ante la ley.

- La completa armonización legal respecto de la e-factura en la "Europa de los 27" deberá ser objetivo clave del Mercado Único y fácil de utilizar en el mercado en toda Europa.
- Es importante que estas previsiones se apliquen tanto en el sector público como en el privado.
- Las previsiones del Código de Prácticas podrán incorporarse en un acuerdo bilateral pactado entre las partes comerciales.
- Cada parte comercial es responsable de la integridad de su propio sistema de control.

Tomando una perspectiva general de la relevancia legal de la factura, el Grupo de Expertos ha decidido focalizarse en particular en el archivo, contabilidad, legislación de e-commerce, prueba legal de las facturas en la resolución de conflictos y la costumbre en la Unión Europea.

En respuesta a este Informe, el Grupo de Expertos recibió el compromiso por parte de la Administración Comunitaria, de una Directiva sobre la Factura Electrónica para finales de 2008, sin que hasta la fecha (febrero de 2009) se haya dictado todavía.

9.3. Legislación vigente

- **DIRECTIVA (2006/112/EC)** relativa al sistema común del impuesto sobre el valor añadido, dedica su **Sección 5** (arts. 232-237) a la Transmisión de facturas por vía electrónica y establece que éstas deberán ser "*aceptadas por los Estados miembros a condición de que se garantice la autenticidad de su origen y la integridad de su contenido mediante uno de los siguientes métodos:*
  a) por medio de una firma electrónica avanzada .../...
  b) mediante un intercambio electrónico de datos (EDI) .../..."

Si bien admite que *"podrán transmitirse o ponerse a disposición por vía electrónica mediante otros métodos, a reserva de su aceptación por el o los Estados miembros de que se trate."*

"... los Estados miembros podrán exigir también que la firma electrónica avanzada se base en un certificado reconocido y haya sido creada mediante un dispositivo seguro de creación de firmas,"

"... los Estados miembros podrán exigir también, con arreglo a las condiciones que establezcan, la presentación adicional de un documento recapitulativo en papel."

Artículo 236

"En el caso de lotes que incluyan varias facturas transmitidas al mismo destinatario o puestas a disposición simultáneamente, por medios electrónicos, los detalles comunes a las distintas facturas podrán mencionarse una sola vez en la medida en que se tenga acceso para cada factura a la totalidad de la información".

- DIRECTIVA 2001/115/CE DEL CONSEJO de 20 de diciembre de 2001 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. La Directiva establece las menciones que son obligatorias en toda factura, e "impone a los Estados miembros la obligación de admitir la utilización de las nuevas tecnologías, tanto en la remisión de facturas como en su conservación".

- **En España**, el Real Decreto 1496/2003 del 28 de noviembre, aprueba el Reglamento, por el que se regulan las obligaciones de facturación y se modifica el Reglamento del Impuesto sobre el Valor Añadido.

- Ley 11/2007 sobre acceso electrónico de los ciudadanos a los servicios públicos
- Orden PRE 2971/2007 sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes
- Resolución 24 de octubre de 2007, sobre homologación del software para digitalización
- Orden EHA 962/2007, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas.
- 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.
- RESOLUCIÓN 2/2003, de 14 de febrero, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre determinados aspectos relacionados con la facturación telemática.
- Boletín Oficial de Vizcaya de 27 de abril de 2004 que contiene: NORMA FORAL 2/2004, de 23 de abril, de Medidas Tributarias en 2004. DECRETO FORAL 57/2004, de 6 de abril, por el que se regulan las obligaciones de facturación.
- Boletín Oficial de Navarra de 9 de junio de 2004 que contiene el DECRETO FORAL 205/2004, de 17 de mayo, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.
- Boletín Oficial de Guipúzcoa de 25 de junio de 2004 que contiene: DECRETO FORAL 61/2004, de 15 de junio por el que se regulan las obligaciones de facturación.
- REAL DECRETO 87/2005, de 31 de enero, por el que se modifican el Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre, el Reglamento de los

Impuestos Especiales, aprobado por el Real Decreto 1165/1995, de 7 de julio, y el Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1496/2003, de 28 de noviembre

- ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.
- Resolución de 24 de julio de 2003 de la Dirección General de la Agencia Estatal de Administración Tributaria por la que se establece el procedimiento a seguir para la admisión de certificados de entidades prestadoras de servicios de certificación electrónica.
- Autorización de la AEAT a CAMERFIRMA para la emisión de certificados utilizados en Facturación Electrónica
- Autorización de la AEAT a CAMERFIRMA para la emisión de certificados de uso tributario.

9.4. Características de la factura electrónica

Como ya ha quedado esbozado en el Informe del Grupo de Expertos, las nuevas tecnologías han posibilitado que la facturación tradicional en papel se pueda realizar por medios electrónicos, lo que aporta ventajas significativas, entre las que cabe destacar: [55]

- Mejora de la eficiencia, ya que disminuye la intervención manual, eliminando del proceso tareas que no generan valor.
- Ahorro de costes de impresión, papel, envío postal y

[55] EDATALIA: www.edatalia.com
http://www.efactura.org.es/

Internacional-EC Expert Group on eInvoicing. Versión original en inglés, traducción propia.

almacenamiento. El proceso de e-facturación no requiere papel con lo que se reducen los costes de consumibles (papel, tóner, faxes, fotocopias, sellos, sobres, etc.). También se eliminan los espacios físicos de almacenamiento.

- Desaparecen los costes del correo postal (sellos, sobres, etc.) o del servicio de mensajería.
- Simplificación y automatización de la gestión de envíos y recepción, aportando por tanto mayor rapidez y rentabilidad
- Eliminación de espacio físico para archivo. El archivo electrónico es más ágil y seguro.
- Disminución de tiempos de operación y envío. Los clientes dispondrán de la factura en el mismo momento que se genera. El proceso garantiza la entrega de las facturas al 100% de los destinatarios.
- Mayor seguridad jurídica aportada por la necesaria firma electrónica certificada. Mejora la disponibilidad y fiabilidad de los datos: la e-firma dota de seguridad al proceso. Se permiten accesos simultáneos y validaciones remotas.
- Se facilitan los procesos de auditoría.
- Impulso de las políticas medio-ambientales y del desarrollo sostenible: eco-Factura

La necesidad de gestionar el alto número facturas y recibos asociados a la actividad comercial de una empresa, implica asumir gastos asociados a la impresión, envío y manipulación del documento, lo que lleva aparejado un gasto aproximado de 1,2 euros por factura enviada (y recibida). [56]

9.5. El proceso tradicional de facturación en papel:

[56] http://www.interactiva.com.es/factura_electronica.htm

Impresión -> Plegado -> Ensobrado -> Sello ->		**Correo postal -> **	**Archivo**

Se convierte en:

Generación electrónica de factura	**> Firma electrónica ->**	**Envío electrónico ->**	**Archivo electrónico**

La facturación electrónica es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

De esta definición, se transmiten tres condicionantes para la realización de e-Factura:

· 1º Se necesita un formato electrónico de factura de mayor o menor complejidad (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros)

· 2º Es necesario una transmisión telemática (tiene que partir de un ordenador, y ser recogida por otro ordenador).

· 3º Este formato electrónico y transmisión telemática, deben garantizar su integridad y autenticidad a través de una firma electrónica reconocida. El artículo 3.3 de la Ley 59/2003 de 19 de diciembre define la firma electrónica reconocida como: *"la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma".*

Es decir, se tienen que dar tres condicionantes para que se dé la firma electrónica reconocida:

1º Que sea una firma electrónica avanzada es decir: "*aquella permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".* (Art 2 de la misma ley)

2º Que esté basada en un certificado reconocido, siendo certificado reconocido aquél que "*cumpla los requisitos establecidos en esta Ley en cuanto "a la comprobación de la identidad y demás circunstancias de los solicitantes"*

3º Que sea generada mediante un dispositivo seguro de creación de firma, es decir, aquel que ofrece, al menos, las siguientes garantías:

- "Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
- Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

- Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
- Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma." (Art. 24.3).

Por último y para que tenga la facturación electrónica la misma validez legal que una factura en papel, se necesita el consentimiento de ambas partes (emisor y receptor).

Adicionalmente, y como requisito de todas las facturas independientemente de cómo se transmitan, en papel o en formato electrónico, el artículo 6 del RD 1496/2003, que regula el contenido de una factura, establece que los campos obligatorios de una factura son:

- Núm. Factura
- Fecha expedición
- Razón Social emisor y receptor
- NIF emisor y "receptor"
- Domicilio emisor y receptor
- Descripción de las operaciones (base imponible)
- Tipo impositivo
- Cuota tributaria
- Fecha prestación del servicio (si distinta a expedición)

Para cumplir con la norma y que una factura electrónica tenga la misma validez legal que una emitida en papel, el documento electrónico que la representa debe contener los campos obligatorios exigibles a toda factura, estar firmado mediante una firma electrónica avanzada basado en certificado reconocido y ser transmitido de un ordenador a otro recogiendo el consentimiento de ambas partes.

El Real Decreto 1496/2003 regula las obligaciones de empresarios y profesionales de expedir y entregar factura u otros justificantes por las operaciones que realicen en el desarrollo de su actividad empresarial o profesional, así como de conservar copia o matriz de aquéllos (art. 1).
La Orden 962/2007, de 10 de abril, desarrolla determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003. Al respecto del consentimiento del destinatario, se encuentra recogido en el Artículo 2 de la citada Orden, donde dice que el consentimiento podrá formularse de forma expresa por cualquier medio, verbal o escrito.

Las obligaciones de las empresas que *emiten* facturas electrónicas son las siguientes:

- Creación de la factura

  Mediante una aplicación informática, con los contenidos obligatorios mínimos requeridos.
- Firma electrónica reconocida
- Remisión telemática
- Conservación de copia o matriz de la Factura

  Esta obligación se regula en el artículo 1 del RD 1496/2003, donde se especifica la obligación de expedir, entregar y conservar facturas.

  También han existido dudas sobre si las facturas electrónicas pueden emitirse en copia o sólo se debe guardar la matriz. Al respecto la Agencia Tributaria lo ha aclarado en el borrador antes citado (Art. 5) con la siguiente definición: "*Se entiende por Matriz de una factura (...) un conjunto de datos, tablas, base de datos o sistemas de ficheros que contienen todos los datos reflejados en las facturas junto a los programas que permitieron la generación de las facturas....*

  Se debe asegurar su legibilidad en el formato original.

- Contabilización y anotación en registros de IVA
- Conservación durante el período de prescripción
- Garantía de accesibilidad completa

  Deber de gestionar las facturas de modo que se garantice una accesibilidad completa:

  a. visualización,
  b. búsqueda selectiva,
  c. copia o
  d. descarga en línea e impresión.

  Esta es una obligación inherente a la conservación de las facturas por medios electrónicos que el legislador denomina acceso completo a datos, tratando de facilitar la auditoria e inspección de las facturas electrónicas. (Art. 9 del RD 1496/2003)
- Subcontratación a un tercero

  Todas las fases anteriores pueden ser subcontratadas a un tercero, sin perder su responsabilidad. Regulado en el artículo 5.1 del RD 1496/2003 el legislador deja claro en ese mismo párrafo que, aunque se permite la subfacturación a terceros, es el obligado tributario el responsable de cumplir todas estas obligaciones.

Las obligaciones de las empresas que *reciben* facturas electrónicas se resumen en:

- Recepción de la factura por medio electrónico
  - Verificación de los contenidos mínimos exigibles y
  - Verificación segura de la firma electrónica.

  Regulado en el artículo 21 e inherente a las obligaciones de la conservación de las facturas electrónicas se indica que: "*el destinatario se debe asegurar de la legibilidad en el formato original en el que se haya recibido, así como, en su caso, de los datos asociados y mecanismo de verificación de firma*".

A diferencia del emisor, al que se permite construir la factura desde la matriz, el destinatario debe conservar los originales firmados.

- Contabilización y anotación en registros de IVA.
- Conservación durante el período de prescripción.
- Deber de gestionar las facturas de modo que se garantice una accesibilidad completa:
    a. visualización,
    b. búsqueda selectiva,
    c. copia o
    d. descarga en línea e impresión.
- **Todas las fases anteriores puede subcontratarlas a un tercero, sin perder su responsabilidad.**

El Artículo 17 del Reglamento, establece las formas de remisión de las facturas o documentos sustitutivos:

"La obligación de remisión de las facturas o documentos sustitutivos podrá ser cumplida por cualquier medio y, en particular, por medios electrónicos, siempre que en este caso el destinatario haya dado su consentimiento de forma expresa y los medios electrónicos utilizados en la transmisión garanticen la autenticidad del origen y la integridad de su contenido.

A estos efectos, se entenderá por remisión por medios electrónicos la transmisión o puesta a disposición del destinatario por medio de equipos electrónicos de tratamiento, incluida la compresión numérica, y almacenamiento de datos, utilizando el teléfono, la radio, los medios ópticos u otros medios magnéticos".

Y el Artículo 18, la remisión electrónica de las facturas o documentos sustitutivos:

" ... a) Mediante una firma electrónica avanzada de acuerdo con lo dispuesto en el artículo 2.2 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, basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas, de acuerdo con lo dispuesto en los apartados 6 y 10 del artículo 2 de la mencionada Directiva.

b) Mediante un intercambio electrónico de datos (EDI), tal como se define en el artículo 2 de la Recomendación 1994/820/CE de la Comisión, de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos, cuando el acuerdo relativo a este intercambio prevea la utilización de procedimientos que garanticen la autenticidad del origen y la integridad de los datos.

c) Mediante los elementos propuestos a tal fin por los interesados, una vez que sean autorizados por la Agencia Estatal de Administración Tributaria. A tal efecto, deberán solicitar autorización a la Agencia Estatal de Administración Tributaria indicando los elementos que permitan garantizar la autenticidad del origen e integridad del contenido de las facturas o documentos sustitutivos remitidos.

2. En el caso de lotes que incluyan varias facturas remitidas simultáneamente por medios electrónicos al mismo destinatario, los detalles comunes a las distintas facturas podrán mencionarse una sola vez, siempre que se tenga acceso para cada factura a la totalidad de la información ...".

9.6. Homologación de software de digitalización

La Resolución de 24 de octubre de 2007, de la Agencia Estatal de Administración Tributaria, "*contempla la digitalización certificada de facturas, documentos sustitutivos y de cualesquiera otros documentos y establece que las facturas, documentos sustitutivos y otros documentos así digitalizados permitirán que el obligado tributario pueda prescindir de los originales en papel que le sirvieron de base*."

Este proceso debe garantizar "*una imagen fiel e íntegra de cada documento firmado con firma electrónica, así como la organización de la digitalización en torno a una base de datos documental con determinadas garantías, tanto para ésta como para su conservación*. La validez de la imagen digitalizada requerirá disponer de los procedimientos y controles necesarios para garantizar tanto la fidelidad del proceso, como la calidad de la imagen obtenida y de sus metadatos. El conjunto de dichos procedimientos y controles recibe la denominación de Plan de Gestión de Calidad, que deberá ser presentado junto con la solicitud de homologación del software de digitalización.

La Resolución entiende por *Plan de Gestión de Calidad*, "*el conjunto de operaciones de mantenimiento preventivo y comprobaciones rutinarias que permitan garantizar mediante su cumplimiento que, en todo momento, el estado del software de digitalización y los dispositivos asociados producen imágenes fieles e íntegras. El objetivo es velar por la correcta calidad de la imagen obtenida y de sus metadatos, independientemente del momento de tiempo en el que se haga uso del software de digitalización*".

Se establecen unos *Formatos estándares de uso común*, y se admiten como tales, aquellos que estén publicados en la página web de la

Agencia Tributaria. La técnica de compresión empleada, en su caso, debe ser sin pérdida de información.

Para garantizar la independencia de la plataforma tecnológica y evitar su obsolescencia, los formatos utilizados deben ser autodocumentados y autosuficientes en contenido para asegurar el acceso a las imágenes.

Se establece que el *Nivel de Resolución* de la imagen digital codificada (resolución espacial de la imagen obtenida debe ser como mínimo de 200 ppp (píxeles por pulgada).

Se exige la *Garantía de imagen fiel e íntegra*, *es decir,* un único fichero digital distinto para cada factura. La imagen obtenida debe respetar la geometría del original en tamaños y proporciones.

Para la representación de metadatos, la Agencia Tributaria establece como referencia la especificación estándar denominada XMP (Extensible Metadata Platform). El fichero, con la imagen resultante y sus metadatos, debe permanecer inalterado desde este instante. La validez de la imagen digitalizada de la factura requerirá disponer de los procedimientos y controles necesarios para garantizar la fidelidad de la imagen con el documento digitalizado en el procedimiento de digitalización certificada.

El resultado de la digitalización certificada debe organizarse en torno a una base de datos documental, conservándose por cada documento digitalizado un registro de datos con todos los campos exigibles en la llevanza de los libros de registros incluidos en los artículos 62 y siguientes del Real Decreto 1624/1992, de 29 de diciembre, por el que se aprueba el Reglamento del Impuesto sobre el Valor Añadido, además de un campo en el que se contenga la imagen binaria del documento digitalizado o que enlace al fichero que la contenga, en ambos casos con la firma electrónica de la imagen del documento.

La firma de la base de datos puede ser realizada mediante cualquiera de los sistemas de firma electrónica contemplados en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Las entidades desarrolladoras que deseen homologar software de digitalización deberán presentar una solicitud dirigida al Director del Departamento de Informática Tributaria de la Agencia Tributaria, el cual, una vez verificada la documentación aportada y el cumplimiento de los requisitos establecidos en la Orden EHA/962/2007, procederá a acordar, en su caso, la homologación solicitada. El software de digitalización homologado será incluido en una lista que se hará pública en la página web de la Agencia Tributaria.[57]

9.7. Formato Facturae

Igual que para el Sector Público, en España la e-Factura a la Administración Pública será obligatoria para los proveedores en Noviembre de 2010 (LEY 30/2007 de 30 de Octubre Contratos del Sector Público).

Para este propósito, y en colaboración con la Asociación de la Banca española se ha definido un formato llamado “Facturae”, cuyo esquema de formato en sus distintas versiones está puesto a disposición de las Empresas en la página *web* del Ministerio de Economía y Hacienda.[58]

También la LEY 56/2007 de 28 de Diciembre de Impulso a la Sociedad de la Información (BOE 29/12), en vigor desde el 31 de Diciembre de 2007, ha implantado a partir del 30 de Septiembre de 2008, el Plan para la Generalización de la Factura Electrónica.

9.8. Firma electrónica

[57] http://www.aeat.es
[58] www.facturae.es

Con respecto a la firma electrónica y a las empresas de certificación, me remito al apartado que expresamente les dedico en este trabajo.

No obstante, es importante reseñar aquí que, a nivel internacional, NO SE CONSIDERAN RECONOCIDOS los certificados de PERSONA JURÍDICA admitidos en España y emitidos por Prestadores de certificación, aunque pueden ser utilizados en la firma de Facturas electrónicas.

10. FORMAS DE PAGO EN LA RED

El pago electrónico es el mecanismo mediante el cual se ejecuta la contraprestación de una obligación asumida mediante la contratación (normalmente) electrónica.

El desarrollo de la "Banca electrónica" y otras formas de pago *on line*, resulta primordial en el crecimiento del comercio electrónico, puesto que, garantizar la seguridad del pago en la red, es el primer paso para hacer desaparecer la percepción de inseguridad que existe entre los usuarios de Internet.

Los operadores económicos participan en los mercados en la medida en que detectan que éstos ofrecen buenas oportunidades de negocio en las que los beneficios potenciales superan a los costes. Ningún mercado ofrece unas condiciones de seguridad total en las transacciones económicas entre sus operadores, pero unas condiciones mínimas de seguridad son imprescindibles a fin de que empresas y consumidores se vean incentivados a acudir a ellos.

Este ha sido uno de los objetivos perseguidos por las Autoridades Comunitarias, que ya en el año 1996 presentaron los resultados de las consultas realizadas en relación con el Libro Verde de la Comisión titulado "Servicios financieros: cómo satisfacer las expectativas de los consumidores", y presenta la respuesta de la Comisión a tales consultas.

El principal objetivo del Libro Verde consistía en estimular a todos los interesados a opinar sobre la adecuación del grado de protección del consumidor establecido por la legislación de aquel momento en materia de servicios financieros y sobre la posible conveniencia de adoptar otras medidas.

El Libro Verde se dividía en tres partes. En la primera, la Comisión ponía de manifiesto la atención prestada a los intereses del consumidor dentro

de la legislación comunitaria. En la segunda parte, se señalaban una serie de problemas que habían sido ya detectados. La tercera parte estudiaba brevemente las futuras tendencias de la comercialización de servicios financieros, incluida la venta a distancia.

Como cabía esperar, las respuestas a la consulta mostraron divergencia de opiniones entre los principales interesados en cuanto a las implicaciones para los consumidores y las actuaciones oportunas de cara al futuro.

El *sector de servicios financieros* hacía hincapié en la necesidad de garantizar el pleno funcionamiento del mercado único. Se destacaba, asimismo, la importancia de fomentar el desarrollo de productos y servicios innovadores y de nuevos canales de distribución (electrónicos), la unión económica y monetaria y la sociedad de la información figuraban entre los principales retos a los que el sector debía hacer frente.

Las *agrupaciones de consumidores y usuarios* reconocían, en general, que la estabilidad y la credibilidad del sistema financiero y monetario de la UE que se había logrado gracias a la legislación sobre servicios financieros. No obstante, formularon algunas críticas en relación con las disposiciones destinadas específicamente a proteger al consumidor, y propugnando un papel más destacado para éstos.

El *Parlamento Europeo* aprobó su informe sobre el Libro Verde el 19 de febrero de 1997; el *Comité Económico y Social* (CES) había emitido su dictamen el 30 de octubre de 1996. En él, el Comité solicitaba la adopción de un Libro Blanco sobre la política de protección del consumidor en el sector de los servicios financieros, subrayando las principales necesidades del consumidor (tales como el derecho a la información y la protección jurídica y las posibilidades de recurso), así como las medidas que debían adoptarse.

El planteamiento era el de obtener la estabilidad y la credibilidad del sector de servicios financieros como aspectos primordiales para lograr la confianza del consumidor, puesto que el mercado único se basa en la confianza. Cualquier nuevo medio de pago exige, para poder prosperar, la aceptación y total confianza de los consumidores. Este objetivo sólo podía lograrse mediante una adecuada aplicación de las normas comunes, la implantación del Euro, o la eliminación de las diferencias de estructura fiscal y régimen impositivo.

Los servicios bancarios se liberalizaron, en general, en 1993, y el proceso de transformación ha seguido su curso incorporando progresivamente los aspectos mencionados. Así, muchos de los obstáculos comerciales han sido eliminados, y el objetivo de la libre competencia en el mercado único como estímulo para la competitividad y una economía pujante continúa progresando.

Consecuencia de todo lo anterior y teniendo en cuenta la Resolución del Parlamento de 17 de febrero de 1997, la Comisión presentó una propuesta específica de directiva en relación con los servicios financieros. En cuanto a la falta de información al consumidor y las vías de recurso, la Comisión propuso otras medidas, como, por ejemplo, la referente a las transferencias transfronterizas.

10.1. Legislación

Tras la aprobación de la Directiva 97/7 y de la Directiva sobre Comercio Electrónico (que había excluido de su ámbito material de aplicación los servicios financieros *on line*) se consideró que los servicios financieros eran, por su carácter incorporal, particularmente aptos para la contratación a distancia, y por ello se incorporaron al marco regulador de los servicios a distancia.

En la Directiva 2002/65/CE del Parlamento Europeo y el Consejo de 23 de Septiembre de 2002 relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, se presenta un marco de protección que abarca todos los servicios financieros que pueden prestarse a distancia. No obstante, la Directiva excluye de su ámbito de aplicación las prestaciones de servicios efectuadas con carácter estrictamente ocasional y al margen de una estructura comercial cuyo objetivo sea celebrar contratos a distancia.
Servicio financiero se define como "todo servicio bancario, de crédito, de seguros, de jubilación personal, de inversión o de pago". Y técnica de comunicación a distancia como "todo medio que pueda utilizarse, sin que exista una presencia física y simultánea del proveedor y el consumidor, para la comercialización a distancia de un servicio entre estas partes". En esta definición quedan incluidos los medios telefónicos y electrónicos, y se valora especialmente la información previa a la celebración del contrato para el consumidor.

La Directiva 2002/65/CE en la que se regulan los contratos a distancia de servicios financieros, cubre las actividades prestadas exclusivamente a través de correo, teléfono y medios electrónicos como Internet, e intenta armonizar los siguientes aspectos:

1. El derecho de reflexión del usuario, que se establece en 14 días. En dicho periodo, el cliente puede analizar las condiciones contractuales del servicio financiero y compararlo con otras ofertas antes de manifestar su consentimiento.
2. El derecho de desistimiento del usuario en el caso de que el contrato haya sido firmado antes de recibir todos los términos y condiciones del servicio o cuando el cliente haya sido sometido a una presión desleal durante el periodo de reflexión. El periodo desistimiento será de 14 días para todos los servicios financieros,

excepto para las hipotecas, los seguros de vida y los planes de pensiones, en los que el periodo será de 30 días.

3. Los derechos mínimos del usuario en los casos en que los servicios financieros contratados no estén disponibles de forma total o parcial (por ejemplo, el derecho a la devolución de las cantidades pagadas)
4. El derecho de la entidad financiera a ser indemnizada en el caso de que el usuario decida desistir una vez que la ejecución del servicio haya empezado.
5. La prohibición de suministro de servicios financieros que no han sido solicitados.
6. La limitación en el uso, por parte de la entidad financiera, de sistemas de comunicación en los que el contacto se produce sin previo consentimiento del usuario.
7. El establecimiento de sistemas para la resolución de disputas entre entidades financieras y usuarios.

Esta Directiva complementa la Directiva 97/7/CEE sobre venta a distancia, que, como ya se ha anotado, excluye de forma expresa los servicios financieros.

Hay que destacar también la aprobación del Reglamento 2006/2004 del Parlamento Europeo y el Consejo, de 27 de octubre de 2004, sobre la cooperación entre autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores, el cual pretende fomentar el comercio electrónico transfronterizo, así como su eficacia, al facilitar la solución transfronteriza de litigios relativos al comercio electrónico.

Se ha establecido un nuevo marco jurídico para armonizar la legislación europea sobre pagos. Se trata de la Directiva de servicios de pago (PSD) que fue aprobada en 2007 por el Parlamento Europeo y tiene que

aplicarse en las legislaciones nacionales a más tardar, por el 1 de noviembre de 2009. El objetivo principal de la PSD es el de armonizar la legislación europea de pagos y aumentar la transparencia y eficiencia de los sistemas de pago, así como fomentar la competencia, facilitando a las entidades no bancarias participar en el negocio de los pagos *on line*. Busca, también, proteger los intereses de los consumidores, los minoristas, empresas y Autoridades públicas.

10.2. Sujetos intervinientes en las operaciones de pago electrónico

Para una buena comprensión del proceso de pagos *on line*, es importante comprender cada sujeto participante y su papel individual en el proceso de pago. Se incluyen en este punto algunas referencias sobre el análisis ofrecido por Innopay[59] sobre las formas de pago en la Red para el año 2009. En él se destaca la actividad de las empresas suministradoras de servicios de pago (PSP). [60]

En el supuesto de un consumidor que desea realizar una compra y desea pagar, ha emitido un dispositivo de pago (como una tarjeta de pago) por un emisor. El comerciante debe ser capaz de aceptar el pago del comprador. Tanto el comprador como el emisor están autorizados por el titular de una combinación que establece y supervisa las normas de la forma de pago. Las cuatro partes principales son:

— Comerciantes

— Consumidores

— Proveedor que mantiene la relación formal con el comerciante y proporciona la solución de dinero al mismo. Están autorizados para aceptar sus transacciones. (PSP)

[59] Innopay: Asociación Europea de instituciones financieras
[60] El texto completo se puede encontrar en www.innopay.com

— Emisor, que son instituciones (a menudo los bancos) que emiten tarjetas o cuentas.

La Directiva de Servicios de Pago introduce la "*Payment Institution*" (PI), dando una definición bastante precisa, pero dejando margen para la interpretación. Queda, sin embargo, claro que las instituciones de pago:

- pueden transferir dinero,
- se les aplican restricciones a la celebración de las cuentas de pago y a la concesión de créditos y
- tienen prohibido la toma de depósitos y la emisión de dinero electrónico (art. 16.2-4).
- Para ello, las organizaciones que pretendan aplicar tales servicios financieros necesitarán una licencia (art. 10 §9).

La introducción de las instituciones de pago es especialmente relevante para el sector de los pagos en línea donde PSP (Proveedores de Servicios de Pago) ya están proporcionando una gama amplia de servicios.

10.3. Procedimiento

Para cada transacción que solicita un comerciante, el comprador busca autorización en tiempo real en el emisor, tras lo cual se garantiza la transacción al comprador.

Existe un conjunto de normas y reglamentos que deben cumplir sus licenciatarios. El objetivo general de dicho conjunto de normas es el de garantizar la calidad operativa y la confianza en la forma de pago. Ejemplos de los planes son Visa, MasterCard y planes locales como iDEAL y Giropay (programas en línea para respectivamente en los Países Bajos y Alemania).

El PSP (proveedor de servicios de pago) [61] ofrece métodos de pago propios del entorno del comerciante así como cualquier otro que precise el comerciante en su página web. Esto permite que el comerciante ofrezca varios métodos de pago sin tener que negociar varias conexiones con distintos suministradores. En el ámbito del mercado mundial, ofrecer varias opciones de pago sin un PSP requeriría al comerciante una gran cantidad de contratos individuales de conexión.

Un proveedor de servicio de pago proporciona la conexión entre la cesta de compra del comerciante y las instituciones financieras.

Los PSP comenzaron proporcionando conexiones y procesando los pagos en el canal de Internet y hoy en día ofrecen una amplia gama de servicios financieros adicionales a sus clientes.

Razones a tener en cuenta por parte de un comerciante para hacer negocios con una PSP son:

1. Una sola conexión técnica para todos los métodos de pago que se ofrecen a los consumidores en la web.
2. Acceso a métodos de pago local en países definidos.
3. Una sola conexión administrativa (informes).
4. Un procedimiento de solución única con una frecuencia acordada.
5. Generalmente se necesitan menos contratos, en comparación con tener conexiones individuales. El PSP actúa como el

[61] www.innopay.com, Guía de PSP comprador 2009

comerciante mayorista para poder ofrecer tasas inferiores debido a su mayor poder adquisitivo.

6. Acceso a los conocimientos especializados sobre el proceso de pago.
7. Proporcionan herramientas de prevención de gestión y el fraude/riesgo actualizadas regularmente.

En algunos casos estos suministradores se centran sólo el aspecto de conectividad. El dinero fluye directamente desde el comprador al comerciante. Cuando se utiliza una distribución PSP, el comerciante:

— Ejecuta la conciliación en el back-office (Asociación de pedidos con pagos entrantes).

— Ejecuta su propia gestión de efectivo.

— Configura y gestiona sus propias relaciones con el comprador.

Una gestión PSP ofrece conectividad y la recaudación al mismo tiempo. El comprador paga a la PSP en nombre del comerciante. La PSP agrega todos los pagos y paga en lotes regulares y en cualquier moneda. La gestión colectiva PSP ofrece la información adicional de conciliación, que coinciden con la identificación de pago (generada por la PSP) con la identificación de orden (generado por el comerciante).

Las PSP ofrecen un gran número de pagos con tarjeta y sin tarjeta de pago. Su papel es especialmente importante en la habilitación local no-tarjeta de pago para los comerciantes.

Para el comerciante de web, ofrecer varios métodos de pago, significa que ofrece no sólo varias marcas de tarjetas de crédito, sino otros

métodos de pago diferentes. De acuerdo con un estudio de Cybersource, ofreciendo 3 o más métodos de pago aumenta el porcentaje de ventas en un 14 % sobre los comerciantes que ofrecen sólo 1 o 2 métodos de pago.

Con la investigación realizada por Innopay y Thuiswinkel.org, los comerciantes holandeses con página web ofrecen un promedio 4 métodos de pago. El papel del PSP en la agregación de numerosos métodos de pago por lo tanto, es muy importante para el comerciante en la *web*.

10.4. Formas de pago en Internet

Uno de los requisitos más importantes del comercio y de la banca electrónica es el de la confidencialidad, junto con las garantías de autentificación, integridad de la información, e imposibilidad de repudio; el contenido de las transacciones y operaciones bancarias realizadas en un entorno electrónico y la identidad de las partes deben mantenerse, en todo momento, inaccesibles a terceros.

Esta garantía de confidencialidad se refiere claramente a aspectos como:

- control de accesos
- cifrado de la información
- clave pública y clave privada

Las técnicas de autenticación ya han sido presentadas en el apartado de “Firma electrónica”. En particular, la criptografía simétrica es la técnica de autenticación y la emisión documental utilizada en el ámbito de la banca electrónica.
Esa técnica funciona por medio de la combinación de claves, una

clave secreta elaborada por el banco e incorporada en la banda magnética que figura en el dorso de nuestras tarjetas bancarias, de modo que introduciendo la tarjeta con ese código digital incorporado en la banda magnética se tiene acceso al sistema aunque todavía no se pueda operar con él; es decir, el sistema nos permite ingresar, nos saluda, nos reconoce, pero nos impide hacer ningún tipo de operación a partir de ahí, sino que nos requiere otro tipo de clave que cada uno de nosotros elabora para operar con el cajero automático y esa combinación de claves es la que efectivamente nos permite no solo ingresar al sistema sino operar con él.

Actualmente los bancos han añadido nuevos sistemas de seguridad para garantizar la autenticidad de las transacciones en medios electrónicos. Por ejemplo, al realizar una transferencia y una vez firmada con nuestra clave personal, el sistema nos envía al teléfono móvil que hayamos asignado un mensaje SMS con una segunda clave adicional que debemos introducir en el espacio previsto para ello en la página web en un corto espacio de tiempo.
También es cada vez más frecuente la opción de acceder a Banca electrónica mediante DNI electrónico.

La forma más habitual de pago en la Red es a través de las tarjetas de crédito y débito como Visa, Mastercard, American Express, etc. "Es un sistema fácil de usar, aceptado universalmente, muy líquido, fraccionable, incorruptible, seguro, puede realizarse el pago con intimidad y a la vez "deja huella", de forma que a través del sistema bancario el comprador puede demostrar que ha hecho el pago y saber en qué cuenta ha hecho el abono".[62] Para encriptar los datos de las tarjetas de crédito en la Red, se utiliza el sistema de encriptación SSL (*Secure Sockets Layers*) que combina encriptación simétrica y

[62] MARTINEZ COLL, J.C. http://cursos.asmoz.org/file.php/129/jcmc/12CE/tarjetas.htm

asimétrica, fácil de usar e incorporado de serie en todos los navegadores de Internet. La transacción en Internet es similar a la realizada por medios tradicionales e igualmente segura. El punto débil en la seguridad del sistema no está en la transmisión de los datos sino en su almacenamiento, lo que exige un alto grado de confianza del cliente en el vendedor, pues éste puede hacer un uso fraudulento de los datos o no poner las medidas necesarias para garantizar la protección de los datos de sus clientes.[1]

SSL (*Secure Sockets Layers*)

El protocolo de seguridad SSL puede ser utilizado en tiendas virtuales que dispongan del software correspondiente. El vendedor debe disponer de un par asimétrico de claves certificadas.

El comprador no necesita ni claves ni certificados.

Cuando el usuario accede a la tienda virtual con SSL, inicia automáticamente una fase de saludo. El servidor envía su clave pública y certificación. El navegador cliente recibe estos datos y se prepara para la comunicación con sistema de seguridad.

El usuario envía sus datos sin ser necesariamente consciente de los intercambios que se han producido. El navegador codifica esto datos mediante clave simétrica. La función resumen de los datos y la clave simétrica son codificadas con la clave pública que acaba de recibir el vendedor. El resultado de estas operaciones es enviado al vendedor. Los datos viajan a través de Internet encriptados, de forma que sólo la tienda virtual podrá interpretarlos.

MARTINEZ COLL, J.C. http://cursos.asmoz.org/file.php/129/jcmc/12CE/ssl.htm

No obstante, se han creado otras maneras alternativas que pretenden aportar una mayor seguridad y mitigar los miedos que puedan existir hacia la compra en Internet, entre ellos:

- Paypal
- Google Checkout
- Amazon Payments
- Bill Me Later: crédito por transacción.
- Tarjetas pre-pago: Continúan su desarrollo
- Web 2.0 pagos

Las tarjetas de crédito como VISA, MasterCard y American Express han sido tradicionalmente las más populares para las compras *on line*, especialmente en los Estados Unidos. En los últimos años, sin embargo, otros métodos de pago se han hecho cada vez más habituales, como por ejemplo:

- tarjetas de débito
- tarjetas de prepago, que son utilizadas generalmente como tarjetas de regalo o encaminadas a aquellos con poco o ningún acceso a otros métodos de pago.
- La banca electrónica permite habilita a sus clientes / consumidores a pagar en línea directamente desde su portal en Internet. Especialmente en Europa, estos métodos de pago están creciendo rápidamente. Ejemplos son los pagos de Vault de iDEAL, Giropay, seguro y Interac.
- E-carteras son métodos de pago por los cuales se carga un monedero en línea con fondos desde el que se pueden pagar compras posteriores. Algunos ejemplos son PayPal o WallieCard.
- Los pagos de SMS son los que se realizan compras a través de un mensaje SMS enviado desde un teléfono móvil.
- Existen otros métodos que pueden ofrecer los PSP, como por ejemplo, proporcionar crédito instantáneo o TrialPay que ofrece un método de publicidad transaccional.

Pagos en línea / métodos de pago fuera de línea

- Métodos de pago en línea:

  Proporcionan al comerciante información inmediata sobre la situación de pago. Cuando el pago es autorizado, el comerciante puede iniciar directamente el cumplimiento de la

orden. Ejemplos son: las tarjetas de crédito, PayPal y pagos de internet del tipo “banca electrónica”.

- Métodos de pago fuera de línea:

  Son métodos que precisan cierto tiempo entre orden y la confirmación por la institución financiera que de que se acepta el pago. Ejemplos son: la transferencia bancaria regular o de débito directo. Durante esta etapa, la transacción tiene el estado de “pendiente”. Estos tipos de transacciones tienen una mayor probabilidad de fracasar porque los compradores tienen la posibilidad de cambiar de idea durante el proceso. Para ellos este también es un proceso manual, que es más complicado y propenso a errores. Para el comerciante conlleva costos más altos de back-office debido una tasa mayor de los pagos no identificables.

Modelo de servicio directo o redirigido

- En el modelo de redirección el consumidor es reenviado desde la página web del comerciante a la pantalla de selección de pago en el entorno de PSP, donde se puede iniciar el pago.

- En el modelo directo es en el sitio Web de la tienda donde se ofrecen los métodos de pago, y toda la información se recoge en el sistema de la tienda.

Una ventaja del modelo de redirección es que todos los métodos de pago proporcionados por el PSP están disponibles. La evaluación de riesgo está activa y se transfieren los datos confidenciales, como los detalles del pago, de una forma segura.

Una ventaja del modelo directo es que, dado que los datos de orden y el pago se almacenan en el sistema de la tienda, el comerciante puede ofrecer pagos recurrentes para los clientes que compren más de una

vez. Un ejemplo son las suscripciones mensuales. Los consumidores sólo deben introducir sus datos una vez.

No obstante, en el modelo directo la seguridad es un gran problema: la recogida y el almacenamiento de información como números de tarjeta debe hacerse en un entorno seguro y cumplir con las reglas PCI.

En general cada PSP proporciona herramientas contra el fraude, tales como:

- Abordar la comprobación de servicio (AVS), que compara los datos del comprador con datos de la institución emisora.

  Código de verificación — tarjeta (CVC, también CVN)

- Módulo de gestión del fraude, que ayuda a los comerciantes a detectar pagos fraudulentos por medio de módulos de software. Estas incluyen listado blanco y negro, período de cheques de sesiones, cheques de velocidad o un registro del país de origen-dirección IP.

10.5. La armonización de las formas de pago *on line* en la Comunidad Europea: la directiva de servicios de pago (PSD) y SEPA [63]

En los últimos años, los bancos europeos han estado bajo la presión de los responsables políticos europeos para abordar la fragmentaria situación de los pagos en Europa. En 2002, esto condujo a la introducción de la "Directiva Bolkestein", que estipula que el coste de una transferencia transfronteriza de dinero debe ser el mismo que los gastos de una transferencia de dinero nacional. En años posteriores, se han hecho importantes esfuerzos políticos para lograr una plena armonización de los pagos del euro. Esto se denomina SEPA: "*Single Euro*

[63] www.innopay.com, Guía de PSP comprador 2009

Payment Area". Esta visión de la Comisión Europea que fue adoptada por la industria bancaria, significa que los ciudadanos y empresas dentro de Europa pueden tener acceso a un solo conjunto de instrumentos de pago. Este conjunto es la combinación de una cuenta bancaria y de instrumentos como la transferencia de crédito, débito directo y tarjetas. En enero de 2008, la transferencia de crédito SEPA entró en vigor, lo que significa que actualmente no se hace ninguna diferencia si se transfiere el dinero a nivel interno o dentro de la región SEPA.

En concreto, esto significa que se están desarrollando nuevos instrumentos de pago estándar. Son transferencias de crédito y débito directo. En lo que a las tarjetas de crédito y débito se refiere, no se están desarrollando nuevos instrumentos, pero en su lugar están las reglas para el marco de tarjeta SEPA. Esto quiere decir que las tarjetas de débito local en varios países (incluyendo la tarjeta PIN holandés y la tarjeta de efectivo de la CE alemán actual) pueden desaparecer en su forma actual, cambiar o enlazar a otras redes internacionales. Las redes internacionales existentes de MasterCard y Visa desempeñan un papel importante en la consecución SEPA para tarjetas, pero también es probable que surjan otras tales como EAPS, PayFair y la iniciativa de franco-alemán Monet, productos alternativos de tarjeta SEPA.

Los instrumentos existentes no desaparecerán inmediatamente, pero en los próximos 5 a 10 años, todo el sector bancario migrará hacia nuevos métodos de pago, pues mantener los diferentes productos locales resultará demasiado caro.

10.5.1. E-SEPA

En la primera categoría de e-SEPA encontramos servicios directamente relacionados con instrumentos de pago, como la e-mandatos, los pagos

en línea y servicios seguros 3D para tarjetas, tales como Verified by Visa y MasterCard Securecode.

E-mandatos son mandatos desmaterializados utilizados para domiciliación bancaria. Los compradores podrán emitir un mandato en línea, por ejemplo, haciendo uso de sus credenciales de banca en línea. Esto proporcionará un servicio nuevo a los comerciantes, porque ahorrarán costos con respecto a los mandatos de papel.

Tanto el E-mandato como el pago de SEPA en línea no son obligatorios, por lo que dependerá de los bancos individualmente ofrecer estos productos a sus clientes.

La Factura electrónica es también un medio para apoyar la migración al SEPA, basado en la futura automatización de pagos.

La desmaterialización del comercio de documentos en papel es una prioridad en la agenda política por el potencial de ahorro para agregar a la competitividad de Europa como parte de la estrategia de Lisboa. Sin embargo, e-facturación no es el dominio originario de la industria bancaria, por lo que se necesita un esfuerzo de todas las partes interesadas. La Comisión Europea tomó medidas al respecto creando un grupo de expertos en facturación electrónica [64]que comenzó el trabajo en el primer trimestre de 2008 por un período de dos años.

E-SEPA debe considerarse como una oportunidad para el sector de e-commerce, porque contribuirá a una mayor eficiencia y a la creación de servicios centrados en el cliente.

10.6. El crecimiento de los proveedores no bancarios

En general, el uso de la alternativa de métodos de pago diferentes a las tarjetas de crédito y Banca on-line “no-tarjeta y no-Banco. En 2007 el 30 % de los comerciantes de la web en Estados Unidos los ofrecían, lo que

[64] Ver apartado de “Factura electrónica” en este trabajo.

supone un aumento del 25 % en comparación con respecto al año anterior. La compañía de créditos instantáneos Lista-me señaló que el 21 % de los comerciantes que participaron en la encuesta había aprobado su método. El 19 % tenía PayPal, seguido de un 10% de Google Checkout.

Los comerciantes de la Web consideraron que proporcionar más opciones de pago conduce a un aumento de sus ventas. Especialmente ofrecer PayPal puede ayudar a convencer a los compradores que tienen miedos de posible fraude con sus datos de tarjeta de crédito. La proporción general de métodos alternativos de pago en los Estados Unidos era el 14 % en 2007. Se espera que este recurso compartido aumente al 30 % en 2012.

10.6.1. Paypal (pertenece a Ebay)

Utiliza el sistema del dinero de plástico sin que el comercio sepa cuál es el verdadero número, reemplazando los dígitos por una dirección de correo electrónico.

Los usuarios comunican esta información a Paypal, que después intermedia en todo el proceso de pago, de forma que ni el que vende ni el que compra conocen nunca los datos reales de la tarjeta o de la cuenta corriente de la otra persona. En esta forma de pago no hay coste para el comprador y éste se repercute al vendedor en forma de porcentaje sobre cada transacción.[65]

Mediante este sistema también se pueden realizar tareas como el envío de dinero a otras personas, el cobro de facturas o realizar micropagos. Se puede ingresar dinero en la tarjeta y mantener un saldo disponible. Un comprador también puede utilizar este sistema sin tener que abrir una cuenta. Sólo da su tarjeta de crédito y detalles de nombre para

[65] ARREGOCÉS CARRERE, Benyi, CONSUMER EROSKI. "Pagar en Internet sin utilizar tarjetas de crédito"
www.consumer.es/web/es/tecnologia/internet/2009/02/04/182837.php

cada transacción. PayPal también tiene una función de tarjeta de débito en línea, permitiendo que los compradores a utilizar PayPal con comerciantes que no ofrecen este método de pago.

Ofrece también la funcionalidad PSP. El modelo de negocio de PayPal es un costo variable por transacción, lo que puede resultar atractivo para la gran cantidad de pequeños comerciantes que no se pueden justificar los altos costos fijos de una conexión de pago.

PayPal continúa creciendo con más de 165 millones de cuentas en todo el mundo, de los cuales más de 40 millones están en Europa. Se ofrece en 190 países y en 19 monedas. La huella Europea local está aumentando con oficinas de varios países incluidos en el Reino Unido, Alemania, Italia y el Benelux. En el Benelux PayPal tienen más de 3 millones de cuentas y se abren cada semana 17.000 nuevas cuentas. [66]

10.6.2. Google Checkout [7y 8]

Se centra únicamente en las compra-ventas en Internet. Ofrece a las empresas una forma de pagar sus servicios publicitarios y al mismo tiempo éstas lo pueden utilizar para cobrar la venta de sus productos, insertando en sus anuncios un botón que permite a los visitantes adquirir algún producto directamente.

A principios de 2006, Google reveló su solución de pago, introduciendo una nueva categoría de los proveedores de pago: "busca y compra". Con el 65 % de las intenciones de compra que empiezan con una búsqueda en Google la iniciativa puede transformar la clasificación de las formas de pago *on line*. Con el sistema de Google los consumidores pueden buscar productos en varias tiendas de web que se localizan a través de la Web de Google. Los consumidores pueden ordenar los productos con precios y, en el caso de los libros, pueden hojear una

[66] www.innopay.com, Guía de PSP comprador 2009

gran parte del libro *on line*. Los consumidores, a continuación, se reenvían directamente a la página web del comerciante del producto en la que pueden seleccionar para pagar con Google Checkout. Google Checkout permite a los consumidores vincular tarjetas de crédito a su cuenta de Google, permitiéndoles pagar de forma segura y teniéndose que registrar en solamente en Google.

Este sistema ofrece la posibilidad de comparar productos de comerciantes diferentes. La transacción de pago, por lo tanto, es parte de un proceso completo de compra. Google también ha diseñado un sistema de lealtad para los comerciantes ofreciendo descuentos en los costos de transacción cuando un comerciante compra publicidad de Google y descuentos en los gastos de envío cuando los comerciantes utilizan FedEx. Se trata de un desarrollo interesante para los comerciantes, ya que la posición dominante de los motores de búsqueda es cada vez más fuerte.

El servicio "busca y compra" puede considerarse como un valor añadido para ciertos comerciantes que tratan con rápidos movimientos de bienes de consumo que son estandarizados globalmente (por ejemplo, electrónica o libros). Otros proveedores de búsqueda-a-compra son Yahoo y Baidu.

10.6.3. Amazon: servicio de pago flexible[67]

Amazon ha lanzado su propio sistema de pago electrónico vinculándolo automáticamente a las cuentas de usuario de su comercio en la web. Amazon amplió sus servicios con el Servicio de Pago Flexible de Amazon (AFP). Se trata de un servicio de pago basado en la infraestructura ya existente de pago donde ya está habilitado el intercambio de dinero.

[67] ARREGOCÉS CARRERE, Benyi, CONSUMER EROSKI. "Pagar en Internet sin utilizar tarjetas de crédito" www.consumer.es/web/es/tecnologia/internet/2009/02/04/182837.php
[67] www.innopay.com, Guía de PSP comprador 2009

Esto puede hacerse mediante tarjeta de crédito, transferencia de saldo de cuenta bancaria o los pagos de Amazon. También se pueden especificar instrucciones de pago en detalle. Un ejemplo es la posibilidad de un remitente de establecer un límite de gasto por semana para un destinatario. Otras funcionalidades son la especificación de un monto máximo o mínimo para una transacción, los pagos recurrentes o la especificación de los destinatarios que puede tener acceso o recibir fondos. También en entornos complejos de business-to-business esto puede agregar valor, facilitar la ejecución de las normas administrativas o autorizaciones de conformidad con la organización interna.

10.6.4. TrialPay y publicidad transaccional

Empresa estadounidense TrialPay ha sido pionera en lo que puede llamarse transaccional de publicidad. Los fundadores de la empresa habían notado que las personas no están dispuestas a pagar por algunos productos *on line*, como el software o suscripciones, pero están dispuestos a pagar por otros bienes tangibles.

TrialPay ofrecer al cliente el primer bien gratuitamente si compra un segundo en otro proveedor. En la desprotección del proveedor original, el cliente elige TrialPay entre las opciones de pago. Posteriormente, se ofrece una serie de ofertas de compra de otros proveedores, desde la cual el cliente puede seleccionar uno. Después de completar esa segunda compra, se envía al cliente un correo electrónico proporcionándole los detalles de cómo aceptar el producto original, ahora gratis. Por ejemplo, un cliente puede ofrecerse el programa WinZip gratuitamente si también compran por un valor de 50 dólares en la ropa en Gap.com.

Parece como una situación de “todo el mundo gana”: El cliente obtiene un producto gratuitamente. El comerciante original, WinZip por ejemplo, hace una venta que de lo contrario podía no haber hecho. Y Gap.com adquiere a un nuevo cliente. Es este segundo comerciante que reembolsa el comerciante original el producto gratuito para poder obtener un nuevo cliente.

El comerciante del segundo producto es, en esencia, el que participa en la publicidad de los patrocinadores del producto libre a fin de adquirir un nuevo cliente. El nuevo cliente se encuentra utilizando una transacción financiera.

Existen otros sistemas que también permiten realizar pagos sin dar los datos de la tarjeta de crédito, como:

- Moneybookers.com
- ClickandBuy, que permite agrupar las compras realizadas durante un mes y pagarlas a través de una tarjeta de crédito, mediante transferencia o con domiciliación de recibo.

10.6.5. Web 2.0 de pagos

Web 2.0 durante mucho tiempo se ha anunciado como la siguiente fase para pagos en línea y e-commerce. Web 2.0 hace referencia a las comunidades en línea, con colaboración o generación por parte de los usuarios de páginas web, tales como-redes sociales, wikis o blogs.

Facebook es un sitio red internacional líder, y que aparece como la quinta web más visitada del mundo, con más de 150 millones de usuarios. Facebook posibilitando a los individuos hacer su propia página y conectarse de uno al otro, formando una red social. Para enriquecer esta experiencia, Facebook permite a los desarrolladores crear aplicaciones para la red y se han desarrollado varias aplicaciones de pago.

Por ejemplo, iCoins, de la compañía de monedero electrónico, ha desarrollado la aplicación de COINJARS, que permite a los usuarios de Facebook transferir fondos entre cada uno de los otros de forma gratuita.

Aplicaciones similares están disponibles para otras carteras como MoneyBookers, Obopay, WebMoney, cambio de repuesto y varios de PayPal. Además hay numerosas aplicaciones de compras en línea tales como uno para cy-Mall y varios para recuperar las ofertas de eBay. A finales de 2007 Facebook anunció que estaba trabajando en una plataforma de pagos de propia para que los usuarios no se tengan que utilizar métodos de pago de terceros. Pero, a finales de 2008 la compañía anunció la plataforma quedaba aplazada indefinidamente.

Otra red social que está creciendo rápidamente es Twitter. Twitter permite a los usuarios crear un micro-blog. Sus métodos de pago como Tipjoy y Twippr son e-carteras destinadas principalmente a micro-pagos. Estos sistemas habilitan fondos para ser cargados y debitados sólo a través de PayPal. El alcance de los métodos de pago de Twitter es actualmente muy limitado y esto puede afectar su popularidad.

El hecho de que hay una gran variedad de opciones de pago para la Web 2.0 es posible gracias a la capacidad y a la relativa facilidad para los usuarios de crear sus propias aplicaciones. Pese al número, las aplicaciones de pago no parecen ser muy populares. Por ejemplo, Moneybookers tiene más de 6 millones de usuarios, pero la aplicación de Moneybookers en Facebook tenía sólo 16 usuarios activos en enero de 2009. Coinjars es ligeramente más popular con 49 de los usuarios en el mismo mes.

11. CONCLUSIONES / PERSPECTIVAS DE FUTURO.

El desarrollo de las nuevas tecnologías, y en particular de Internet, ha provocado un cambio sustancial en la forma de relacionarnos a todos los niveles.

El comercio en concreto es uno de los ámbitos que más rápidamente ha tomado partido aprovechando las indudables ventajas que los medios electrónicos aportan, en todos sus procesos, a las relaciones comerciales, desde la publicidad de productos y servicios hasta la contratación, la facturación o el pago electrónico.

También las Administraciones públicas no sólo han adaptado las normativas nacionales e internacionales (Europeas en particular) a la nueva situación, sino que están propiciando su implantación con todo tipo de actuaciones:

- Legislación abundante y variada
- Promoción del uso de las nuevas tecnologías para relacionarse con las Administraciones
- Facilitando instrumentos para ello: DNI electrónico, acceso a las Instituciones a través de las páginas *web* oficiales, etc.

Esta actividad de las Administraciones está provocada, no sólo por un deseo de modernización de la Sociedad, sino también como una medida de ahorro en recursos económicos, como el papel y todo lo que conlleva su fabricación, manipulación, etc., y ecológicos, como la disminución en la tala de árboles, etc., que supone[68].

La simplificación y automatización de los distintos procesos favorece la reducción de costes y, por tanto, convierte a las empresas en más competitivas.

[68] Ver apartado de Factura electrónica

Junto a las ventajas indudables que ofrecen las nuevas tecnologías, la globalización está aportando también nuevas situaciones de conflicto que requieren de soluciones adecuadas. Por ejemplo, el llamado "efecto mariposa" ha pasado de ser una interesante teoría del caos a un hecho fácilmente verificable. El aleteo de las "hipotecas basura" iniciado en EE.UU. ha desencadenado una crisis de carácter mundial que afectará en mayor o menor medida a todos los países del planeta. Como manda la lógica, a crisis globales respuestas globales.[69] Las sucesivas Conferencias o reuniones de todo tipo que se están sucediendo estos últimos meses, traerán como consecuencia, sin duda, nuevas medidas políticas que posiblemente nos aporten cambios en lo que a la globalización y a las "relaciones electrónicas" se refiere.

Si bien no parece que el tema de las "hipotecas basura" se esté considerando como un "crimen", la Red sí que ha propiciado la aparición de nuevas formas delictivas.
Junto a los delitos convencionales que pueden ser cometidos amparados en las nuevas tecnologías, como los que afectan al derecho a la intimidad, a la libertad de expresión o al uso indebido de patentes y marcas, aparecen otros que atentan contra la seguridad de las transmisiones y sus contenidos en Internet, como la piratería informática, los ciberokupas o tantos otros.

El llamado Código Penal del siglo XXI incorpora nuevos bienes jurídicos que van a ser objeto de tutela a partir de ahora, al tiempo que refuerza bienes jurídicos tradicionales que se trasladan al nuevo ámbito jurídico del ciberespacio. El Código Penal anterior no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de la persona o para violar

[69] Published by *Jokin G.* on Octubre 26, 2008 in Economía and Globalización. Tags: e-business.

acceder y descubrir sus secretos.[70]

Así por ejemplo:

- Usurpación y cesión de datos reservados de carácter personal, por el que quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.
- Las estafas electrónicas. El nuevo CP introduce el concepto de la estafa electrónica, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.
- Daños informáticos. En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos.
- Delitos contra la propiedad intelectual. Respecto a los delitos contra la propiedad intelectual, no se introducen cambios significativos. Con la proliferación de la obras multimedia y el uso de la red, este tipo se aplicará no sólo a los programas de ordenador, sino también a los archivos con imágenes, gráficos, sonido, vídeo, texto, animación, etc. que incorporan las webs y las bases de datos accesibles a través de Internet.
- Pornografía infantil
- Difusión de mensajes injuriosos o calumniosos
- Publicidad engañosa en Internet
- Etc.

Con respecto al delito contra la propiedad intelectual, me parece

[70] Xabier Ribas, www.onnet.com

interesante destacar la iniciativa de ley del Presidente de la República Francesa, Nicolas Sarkozy, "Création ou Internet", más conocida como Ley Hadopi. Su finalidad originaria, hace ahora dos años, era la de limitar el intercambio de ficheros audiovisuales en la Red (definida como "piratería") mediante la supresión del abono para las cuentas que acudan a las plataformas de "compartir" para descargar y difundir los contenidos protegidos por el "derecho de autor". Durante este tiempo la actividad de intercambio de ficheros sin control ha crecido enormemente y Hadopi pretende que la industria de las telecomunicaciones, ponga a disposición de la Administración las bases de datos de las conexiones de los usuarios. Gracias a esta herramienta (valorada en más de 70 millones de Euros) los servicios del Estado dispondrían de medios sin precedentes para el control de los intercambios *on line.* "Ante la insistencia de los poderes públicos en criminalizar Internet, es de temer que sirva como terreno de experimentación para extender el control del último medio de comunicación libre".[71]

Aunque esta proposición de ley no ha sido todavía aprobada, está previsto que lo sea a finales del verano, lo que, no cabe duda, tendrá repercusiones en nuestra legislación. (Como dice el refrán: "Cuando las barbas de tu vecino veas cortar, pon las tuyas a remojar)

Junto a las medidas disuasorias y de protección que ya se han tomado, o haya todavía que tomar, hay que destacar la defensa de los consumidores, particularmente en la legislación Comunitaria. Las compras a través de Internet crecen de manera importante cada año; Internet se consagra como el gran canal de distribución a distancia en

[71] Hadopi : surveiller et punir Internet, 12 marzo 2009. www.lemonde.com (La valise diplomatique)

detrimento de otros canales como la compra telefónica, por correspondencia, o a través de agentes comerciales, lo que convierte su regulación en algo fundamental.

En el mismo sentido, la confianza es un elemento esencial de la Sociedad del Conocimiento en el Comercio electrónico.

Para conocer la opinión de los consumidores y empresarios, se han realizado distintas encuestas entrevistando a los gerentes de empresas comerciales minoristas sobre sus experiencias en transacciones transfronterizas, así como sobre sus opiniones sobre ciertas medidas de política de consumidor.

Los medios utilizados son:

- El Eurobarómetro 298 (EB298), que se dirige a medir las actitudes de los consumidores y sus experiencias en transacciones transfronterizas y también a conocer cómo el consumidor ve las medidas específicas que apuntan a la protección de sus derechos, y
- El Eurobarómetro Flash 224 (EB224) se dirige a asesorar al comercio transfronterizo desde una perspectiva minorista.

Según el EB298, el 33% de consumidores en la Unión Europea de 27 países (EU27) ha comprado bienes, mercancías o servicios, a través de Internet en los últimos 12 meses, en su país de origen o en algún otro lugar (en 2006 se cifraba en el 27%). En España el porcentaje desciende al 20%. Existe una variación significativa en estas cifras dependiendo del país: El 68% de individuos en los Países Bajos ha efectuado una compra en línea en los últimos 12 meses, mientras que en Bulgaria esta cifra es solamente del 4 %. El 30% de consumidores de Unión Europea ha efectuado compras en un minorista de su propio país, mientras que el 7% ha hecho una compra en línea a un vendedor o un proveedor en

otro país de la Unión Europea.

Las diferencias entre los Estados son la regla general.

Las principales barreras al comercio electrónico detectadas en la Unión Europea son:

- Rechazo a vender fuera de las propias fronteras, por parte de los minoristas
- Idioma
- Acceso a Internet
- Falta de confianza: el 37% de encuestados dijo que confiarían más en operaciones realizadas a través de vendedores/proveedores localizados en su propio país, lo que se podría mostrar como barrera significativa al comercio electrónico transfronterizo. Sin embargo, el 34% estimó que la confianza es similar tanto si las transacciones se realizan en su propio país como en otro país de Unión Europea.

  En España solamente el 17% de los encuestados confían más en el comercio nacional lo que supone un descenso notable de la confianza en relación al promedio de la Unión Europea

  Un 6 % dijo que confiarían más en operaciones realizadas en otro país de Unión Europea distinto del propio, y este porcentaje baja al 5% en el caso de España.[72]

Con todo, la situación de confianza deberá mejorar considerablemente en los próximos tiempos puesto que continúa vivo el objetivo estratégico de la UE de convertirse en 2010 "en la economía basada en el conocimiento más competitiva y dinámica del mundo, capaz de crecer económicamente de manera sostenible con más y mejores empleos y con mayor cohesión social" alude directamente a la importancia de la

[72] http://europa.eu/rapid/pressReleasesAction.o?reference=MEMO/08/426

[6] Telecomunicaciones y Sociedad de la Información. www.mae.es

sociedad de la información en el contexto comunitario.[73]

Las políticas europeas en el sector de las Telecomunicaciones y de la Sociedad de la Información empezaron a desarrollarse a mediados de la década de los 80. Por un lado, las primeras actividades de investigación y desarrollo en el campo de las tecnologías de la información se realizaron en 1984 dentro del Programa ESPRIT, al que siguieron en 1986 programas de aplicaciones telemáticas especializados y el Programa RACE. Por otro lado, la política de telecomunicaciones se inició en 1987 por medio del Libro Verde sobre la liberalización de dicho sector. Los tres objetivos de aquel momento siguen siendo válidos actualmente:

- liberalizar los segmentos sometidos a monopolio
- armonizar el sector europeo de las telecomunicaciones mediante normas comunes y
- aplicar con rigor normas de competencia a los segmentos liberalizados.

El progreso tecnológico, la innovación en la oferta de servicios, la rebaja de los precios y las mejoras de la calidad producidos por la introducción de la competencia en el sector de las telecomunicaciones constituyen la base para la transición en Europa a la sociedad de la información. La convergencia de los sectores de las telecomunicaciones, la radiodifusión y las tecnologías de la información está dando una configuración nueva al mercado de las comunicaciones, incluida la convergencia de las comunicaciones fijas, móviles, terrestres y por satélite, y la convergencia de los sistemas de comunicaciones y de localización.

Elemento clave del pacto en pro del crecimiento y el empleo de Lisboa, “i2010” promueve una economía digital abierta y competitiva y hace

hincapié en las TIC en tanto que impulsoras de la inclusión y la calidad de vida. Apoyándose en un análisis completo de los retos asociados a la sociedad de la información y en una amplia consulta con las partes interesadas sobre iniciativas e instrumentos previos. Se proponen tres prioridades para las políticas europeas de sociedad de la información y medios de comunicación:[74]

- La construcción de un espacio único europeo de la Información que promueva un mercado interior abierto y competitivo para la sociedad de la información y los medios de comunicación.
- El refuerzo de la innovación y la inversión en la investigación sobre las TIC con el fin de fomentar el crecimiento y la creación de más empleos y de más calidad
- El logro de una sociedad europea de la información basada en la inclusión que fomenta el crecimiento y el empleo de una manera coherente con el desarrollo sostenible y que da la prioridad a la mejora de los servicios públicos y de la calidad de vida.

Por otra parte, hay que tener en cuenta que el carácter "internacional" de Internet y del comercio electrónico, no sólo afecta al entorno europeo. Por ello, la Comisión trabaja con varias organizaciones multilaterales tales como la Unión Internacional de Telecomunicaciones (UIT), la Organización Mundial del Comercio (OMC), la Organización Mundial de la Propiedad Intelectual (OMPI), o la Organización de Cooperación y Desarrollo Económicos (OCDE), entre otras.

A este respecto, uno de los resultados más importantes a escala mundial es el Acuerdo General de la OMC sobre el Comercio de Servicios (AGCS/GATS) en Telecomunicaciones, que abre a la competencia una parte importante del mercado mundial de los servicios de

[74] Telecomunicaciones y Sociedad de la Información. www.mae.es

telecomunicaciones.

Del análisis anteriormente presentado se puede concluir que, el ámbito del comercio electrónico y de las telecomunicaciones se ha desarrollado en muy poco tiempo y continúa su marcha imparable a gran velocidad.

Es de prever que el modelo de la segunda generación de Internet (Internet2), anunciado y puesto en marcha en 1996 por el Presidente de EEUU Bill Clinton y su vicepresidente Al Gore, aporte novedades significativas a los usuarios de la Red. Un objetivo básico de Internet2 es desarrollar la próxima generación de aplicaciones telemáticas para facilitar las misiones de investigación y educación de las Universidades. Se refiere, en particular, al trabajo cooperativo en un entorno multimedia de alta velocidad.

Los objetivos previstos en aquellos momentos fueron:

1. Proporcionar a sus usuarios un entorno lo suficientemente potente y adaptable para poder realizar negocios y acceder a programas educativos y a espacios culturales de forma segura y privada.
2. Conseguir un banco de pruebas de investigación científica y redes gubernamentales.
3. Poner en funcionamiento una red global que conecte el sector de la investigación y de la enseñanza, la administración, la industria y el sector residencial.

El proyecto Internet2 es administrado por la Corporación Universitaria para el Desarrollo Avanzado de Internet (UCAID). El *backbone* puede superar los 2 Gbps, y las conexiones de las universidades varían entre 45 Mbps y 622 Mbps. Sin embargo, Internet2 no tiene como objetivo reemplazar a Internet sino que pretende ser una nueva red y que toda la tecnología, aplicaciones y desarrollos puedan ser transferidos en su momento hacia todos los centros educativos del mundo, posteriormente a la industria y, en último lugar, a Internet. I2 e Internet

acabarán por complementarse tras una etapa de funcionamiento en paralelo.[75]

En lo que respecta al estricto ámbito del Derecho, aunque en tiempos recientes se han producido avances importantes en cuanto al derecho a la identidad electrónica y al uso de la firma electrónica, y en su aplicación a las relaciones entre las Administraciones Públicas, y entre éstas y los ciudadanos, resultan insuficientes para cubrir todas las necesidades derivadas de la comunicación electrónica, especialmente a la luz de las restricciones impuestas por la legislación de protección de datos personales.

Cabe, por ello, trabajar en nuevos modelos, que con base en la innovación jurídica, nos permitan convertir al ciudadano en actor del sistema, con base en el uso de su identidad y su firma electrónica, de forma que podamos obtener un sistema de comunicación electrónica holístico e interoperable, con base en las técnicas de gestión de identidad y de las redes sociales del Web 2.0.[76]

[75] Rodrigo González, Oscar: "Guía práctica del Comercio electrónico", Editorial Anaya, 2008.

[76] Guisado Moreno, Ángela: "Formación y perfección del contrato en Internet", Marcial Pons.

12. BIBLIOGRAFIA

Autores

- ABADIA, Leopoldo, “La crisis NINJA y otros misterios”,
- ALAMILLO DOMINGO, I., “Derecho del Comercio electrónico”, La LEY, Biblioteca de los negocios, 2003
- ALDRICH, DOUGLAS F., “Dominio del Mercado Digital”. Editorial Oxford
- Anteproyecto de LEY de Servicios de la Sociedad de la Información y de Comercio Electrónico (ALCE)
- ARREGOCÉS CARRERE, Benyi, “Pagar en Internet sin utilizar tarjetas de crédito”
- ARRIOLA, Joaquin y GUERRERO, Diego, “La nueva economía política de la globalización”. Universidad del País Vasco.
- ASPECTOS MERCANTILES Y FISCALES. (* Rafael García del Poyo)
- BARCELÓ JULIÀ, R. Comercio Electrónico entre empresarios. La formación y prueba del Contrato Electrónico (EDI). Tirant lo blanch, Valencia, 2000.
- BONET CORREA, J. Código Civil concordado y con jurisprudencia, ed. Civitas, Madrid, 1993.
- CARIDAD SEBASTIAN, Mercedes, “Teletrabajo y comercio electrónico en la sociedad de la información” , Edit. Centro de Estudios Ramón Areces. Universidad Carlos III
- CASTAÑEDA RIVERO, J.M., RAZON Y PALABRA Nº 20 www.razonypalabra.org.mx
- Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales 9 de diciembre de 2005
- DÍEZ PICAZO, L., Fundamentos de Derecho Civil Patrimonial, Madrid, 4ª ed., 1993.
- Dirección General de la Policía. El Periódico, 5 de Abril de 2006
- FLORES DOÑA, M.S. “Impacto del comercio electrónico en el Derecho de la Contratación”; María Claudia Cambi y José Carlos Erdozain, “Derecho del Comercio electrónico”, La LEY, Biblioteca de los negocios, 2001
- GUISADO MORENO, Ángela: “Formación y perfección del contrato en Internet”, Marcial Pons, 2004

- ILLESCAS ORTIZ, R. “Contratación y Comercio electrónico” 195-137: La responsabilidad civil de los intermediarios en Internet y otras redes, J Plaza Penades; “Derecho sobre internet”
- INTECO Instituto Nacional de Tecnologías de la Comunicación
- Internacional-EC Expert Group on eInvoicing

- J.GÓMEZ CALERO, “El contrato mercantil: nociones generales”
- J.M. EMBID IRUJO “Eficacia de la voluntad suplantada por utilización de la firma digital”. Revista de la contratación electrónica nº 14, 2003.
- Jokin G. on Octubre 26, 2008 in Economía and Globalización. Tags: e-business
- LESSING, Lawrence, The future of ideas, 2001
- MARTINEZ COLL, J.C. http://cursos.asmoz.org
- MENÉNDEZ MATO, Juan Carlos. La Oferta Contractual, ed. Aranzadi, Pamplona, 1998.

- OMPI: Organización Mundial para la Propiedad Intelectual

- RODRIGO GONZALES, Oscar: “Guía práctica del Comercio electrónico”, Editorial Anaya, 2008.

- ROGEL VIDEL, C. Contratos Electrónicos, sus tipos y el momento de su perfección. BSCH

- ROGEL VIDEL, C. Lugar y perfección del contrato, Revista La LEY, 1982

Legislación

- DIRECTIVA (2006/112/EC) relativa al sistema común del I.V.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

- DIRECTIVA 1999/93/CE del Parlamento Europeo y del Consejo, de 13 diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- 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)

- 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

- DIRECTIVA 2001/115/CE DEL CONSEJO de 20 de diciembre de 2001 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 I.V.A.
- 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

- DIRECTIVA 2002/58/ce sobre la privacidad de las comunicaciones electrónicas

- DIRECTIVA 2002/65/CE del Parlamento Europeo y el Consejo de 23 de Septiembre de 2002 relativa a la comercialización a distancia de servicios financieros destinados a los consumidores),
- DIRECTIVA 2006/2004 sobre cooperación entre autoridades

- DIRECTIVA 93/13 del Consejo, sobre Cláusulas Abusivas en los Contratos Celebrados con Consumidores

- DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

- 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

- DIRECTIVA 97/5 relativa a la Transferencias transfronterizas

- DIRECTIVA 97/7 del parlamento Europeo y el Consejo de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia

- 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

- DIRECTIVA 98/34/CE del Parlamento Europeo y el Consejo, de 28 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.
- L.O. de Protección de Datos
- Código Civil. Ed. Civitas. 1997
- Código de Comercio y LEYes complementarias. Ed. Civitas. 1999
- Constitución Española de 1978
- LEY 1/92 de Protección de Seguridad Ciudadana
- LEY 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- LEY 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.
- LEY 30/2007 de30 de Octubre Contratos del Sector Público
- LEY 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, LSSICE
- LEY 59/2003 de 19 de diciembre, de firma electrónica
- LEY 7/1998, de 13 de abril, "sobre Condiciones generales de la Contratación" (LCGC)
- LEY Enjuiciamiento civil
- LEY Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.
- Loi Hadopi : surveiller et punir Internet, 12 marzo 2009. www.lemonde.com (La valise diplomatique)

- RD 1/1996, Texto refundido de la LEY de Propiedad Intelectual
- RD 1163/2005 que deroga el RD 292/2004 sobre fomento de la confianza en los servicios de la sociedad de la información
- RD 1496/2003 del 28 de noviembre, aprueba el Reglamento, por el que se regulan las obligaciones de facturación y se modifica el Reglamento del Impuesto sobre el Valor Añadido.

- RD 1553/2005 de 23 de diciembre por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
- RD 994/1999, de 11 de junio, Reglamento medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal
- Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información
- Reglamento (CE) n° 460/2004, de 10 de marzo de 2004 por el que el Parlamento Europeo y el Consejo han creado la Agencia Europea de Seguridad de las Redes
- Reglamento 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004, sobre la cooperación entre autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores
- Reglamento 2560/2001 sobre pagos transfronterizos en euros
- 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
- Resolución del Consejo de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información

Páginas web

- http://blog.inza.com
- http://europa.eu.int/rn/record/green/gp9611/index.htm
- http://europa.eu/rapid/pressReleasesAction.o?reference=MEMO/08/426
- http://publications.europa.eu/index_es.htm, Oficina de Publicaciones Oficiales de las Comunidades Europeas
- http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html
- http://www.invenia.es/oai:dialnet.unirioja.es:ART0000019408
- servicio.estudios@eVeritas.com Web Trust Technologies, S.A.
- www.ace.es, ACE (Agencia de Certificación electrónica)

- www.aeat.es, Agencia Tributaria
- www.aecem.org, Asociación española de comercio electrónico
- www.alfa-redi.org, REVISTA DE DERECHO INFORMÁTICO
- www.camaraguipuzcoa.com, Cámara de Comercio de Guipúzcoa
- www.camerfirma.com, Camerfirma
- www.cecu.es
- www.ceres.fnmt.es Departamento CERES Política de Certificación
- www.confianzaonline.com
- www.consumer.es/web/es/tecnologia/internet/2009/02/04/182837.php
- www.consumer.es: IGNACIO FOSSATI, CONSUMER EROSKI
- www.dni.es
- www.dni.org.es
- www.dni.org.es
- www.dnielectronico.es
- www.dnielectronico.es
- www.dnielectronico.eu
- www.edatalia.com, EDATALIA
- www.efactura.org.es/
- www.Epagado.com
- www.euskadi.net/ona, Gobierno Vasco
- www.facturae.es
- www.facturae.es/
- www.feste.es, FESTE: Certificados notariales
- www.fnmt.es, Fábrica Nacional de Moneda y Timbre
- www.gipuzkoa.net, DIPUTACION FORAL DE GUIPUZCOA
- www.hispadata.com, HISPADATA SOLUTIONS
- www.indra.es
- www.injef.com/derecho/derecho-de-las-tic/414.html
- www.innopay.com Innopay: Asociación Europea de instituciones financieras

- www.inteco.es/Seguridad/DNI_Electronico
- www.interactiva.com., ABALIA INTERACTIVA
- www.ipsca.es
- www.izenpe.com
- www.mae.es, Telecomunicaciones y Sociedad de la Información.
- www.mir.es, Ministerio del Interior. Gobierno de España.
- www.monografias.com/trabajos13/contelec/contelec.shtml
- www.onnet.com, Xabier Ribas
- www.red.es
- www.revistajuridicaonline.com
- www.unece.org/cefact
- www.ventanalegal.com
- www.vlex.com