E-Comercio

Grupo Negocios

Libro III

E-comercio seguro

Gustavo Matías, Patricio Ramírez y José E. Sanz

Este libro ha sido coeditado con **Editores Asociados I+D**. Isaac Newton 2, Parque Tecnológico de Madrid. Tres Cantos. CP 28760. Teléfono + 34 + 91 803 48 56 – Fax + 34 + 91 803 49 53. www.portal3cantos.com. *Web*master@cteletrabajo.com.

Información Adicional:

D. Patricio José Ramírez B.: pjrb17@hotmail.com

D. Juan M. Marqués : juan@cteletrabajo.com

ÍNDICE

1.- Seguridad jurídica y seguridad técnica 5

1.1 El marco legal: tarea de las organizaciones internacionales 7
1.2 Otras iniciativas internacionales 12
1.3 Iniciativas en España 15

2.- Marco legal: una perspectiva europea 17

2.1 Mercado interior: necesidad de un marco jurídico 19
2.2 Opacidad del marco actual 20
2.3 Importantes costes económicos 21
2.4 Impacto en las inversiones y competitividad de las empresas europeas 21
2.5 Barreras jurídicas 22
2.6 Mínima interferencia con los regímenes nacionales 27

3.- Principales aspectos jurídicos del E-comercio: una visión española 35

3.1 Formas de obtención de las obras 37
3.2 Dispersión de obras, derechos y titulares 39
3.3 Requisitos de la oferta 44
3.4 Formulario de pedido 44
3.5 Normativa sobre la venta a distancia 45
3.6 Normativa sobre facturación telemática 45
3.7 Prueba de la aceptación: Entidades certificadoras 50
3.8 La firma digital: primeras experiencias legislativas 51
3.9 Contenido de la ley alemana sobre firma digital 54
3.10 Prevención de la responsabilidad civil 55

4. La seguridad técnica: el Protocolo SET 61

4.1 El pago de bienes y servicios en Internet 61
4.2 La especificación SET 63
4.3 Características de la especificación SET 65
4.4 Componentes de seguridad 73
4.5 Arquitecturas de E-comercio 79
4.6 Arquitectura SEMPER 83

5. Bibliografía 84

1 Seguridad jurídica y seguridad técnica

El E-comercio, a pesar de sus innumerables ventajas, no está exento de ciertos problemas, que dificultan su utilización, como son principalmente los siguientes:

- La falta de seguridad, confidencialidad, fiabilidad, integridad y autenticación de los datos.
- La escasa utilización de nuevos medios de pago (dinero digital, moneda virtual, tarjetas inteligentes), en gran parte debida a las reservas sobre su seguridad.
- La disponibilidad de infraestructuras que permitan realizar las transacciones con mayor velocidad y seguridad.
- El coste de introducción para la empresa y el cliente: equipamiento, suministro del servicio y gasto en comunicaciones.
- El tratamiento de los derechos de propiedad, protección legal y técnica.

En suma, todos esos problemas se pueden resumir en dos, aunque ambos están estrechamente interrelacionados: la seguridad jurídica y la seguridad tecnológica o, para simplificar, seguridad técnica de las aplicaciones disponibles. De ahí que vayamos a dedicar íntegramente a ellos este volumen, empezando por la perspectiva de los consumidores.

Las demandas del consumidor conducen de una u otra forma a la necesaria regulación del E-comercio como condición imprescindible para su éxito. Así lo ha visto el Consejo de la Unión Europea[1], cuyas consideraciones parten de los principales frentes de interés de los consumidores para deducir de ellas la necesaria protección.

- En efecto, esta Resolución del Consejo de la UE señala que los consumidores están especialmente interesados en temas relacionados con:

[1] RESOLUCIÓN DEL CONSEJO de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información. *Diario Oficial n° C 023 de 28/01/1999 P. 0001 - 0003*

1. La accesibilidad y la asequibilidad
2. La facilidad de uso de equipos y aplicaciones
3. La transparencia, la cantidad y la calidad de la información
4. La equidad de las prácticas comerciales, las ofertas y las condiciones contractuales
5. La protección de los niños frente al contenido inadecuado
6. La seguridad de los sistemas de pago, incluida la firma electrónica
7. El régimen jurídico aplicable a las transacciones que los consumidores efectúen en el nuevo entorno con respecto tanto a la elección del régimen jurídico como a la viabilidad de las disposiciones existentes
8. La atribución de responsabilidades
9. La intimidad y la protección de los datos personales
10. El acceso a unos sistemas eficaces de recurso y resolución de litigios
11. La tecnología de la información como instrumento informativo y educativo

Para instaurar confianza, concluye el Consejo de la UE, es necesario que exista en las nuevas tecnologías un nivel de protección equivalente al que rige en las transacciones tradicionales:

1. La transparencia y el derecho a recibir, antes de la transacción y en su caso después de ella, información suficiente y fiable para probar la autenticidad de cada uno de los elementos de una transacción.
2. La no discriminación en el acceso a productos y servicios.
3. La protección de los consumidores frente a las prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad.
4. La protección de los intereses económicos de los consumidores, con una distribución equitativa de riesgos.
5. La protección de la salud, seguridad e intimidad de los consumidores, incluida la protección contra la utilización abusiva de datos personales.
6. La información y educación del consumidor, a fin de posibilitar la adquisición de las competencias adecuadas.
7. La consulta de los consumidores a la hora de desarrollar nuevas políticas o mecanismos reglamentarios.

8. La representación de los intereses de los consumidores en los órganos de control y vigilancia pertinentes.

1.1 El marco legal: tarea de las organizaciones internacionales

Esa visión organizada de los problemas ya inspiró la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del E-comercio en el mercado interior[2], donde se puede leer:

"El E-comercio ofrece a la Comunidad una oportunidad única de estimular el crecimiento económico, aumentar la competitividad de la industria europea y fomentar las inversiones innovadoras y la creación de puestos de trabajo. No obstante, sólo se podrá obtener el máximo provecho si se suprimen los numerosos obstáculos jurídicos que persisten en el sector de la prestación de servicios en línea —especialmente importante para los intercambios transfronterizos y las PYME—. Con la presente propuesta de Directiva se pretende eliminar dichos obstáculos y, de esta manera, permitir a los ciudadanos y empresas de la Unión Europea que saquen el máximo rendimiento del desarrollo del E-comercio en Europa".

En una Comunicación de la Comisión sobre el E-comercio[3], que fue publicada en 1997, ya se fijó un objetivo claro: la creación para el año 2000 de un marco jurídico coherente a escala europea, en el sector del E-comercio. En la misma Comunicación se plantean cinco cuestiones que pueden ser problemáticas:

1) Lugar de establecimiento de los prestadores de servicios de la sociedad de la información.
2) Comunicaciones comerciales (publicidad, marketing directo, etcétera.)
3) Celebración de contratos en línea
4) Responsabilidad de los intermediarios
5) Aplicación de las normativas.

La necesidad de dar respuestas a estos problemas revela que el E-comercio no tiene ante sí un camino de rosas. No solo para las empresas, sino también para los consumidores. Es necesario que los organismos oficiales

[2] Bruselas, 18.11.1988, COM(1998) 586 final. 98/0325 (COD).

[3] "Iniciativa europea de E-comercio", COM(97) 157 final, 16.04.1997.

establezcan, sea a nivel internacional o comunitario –y luego en su caso a nivel nacional-- un marco de protección del consumidor contra lo que puede ser un entorno propicio para las actuaciones ilícitas de ciertas empresas o particulares. De esta regulación depende gran parte del éxito del E-comercio, tarea que pasa por ganar la confianza de los agentes implicados en las transacciones, y en primer lugar de los consumidores.

Con vistas a ese objetivo, el mismo Consejo de la Unión Europea[4], en su resolución del 19 de enero de 1999, realiza una serie de consideraciones:

- El continuo desarrollo de nuevas tecnologías para la transmisión y almacenamiento de información conduce a innovaciones de orden organizativo, comercial, técnico y jurídico que están teniendo un profundo impacto en la sociedad en general.

- Las nuevas tecnologías de la comunicación tendrán una incidencia notable en la vida cotidiana de todos los ciudadanos tanto si adoptan una actitud activa como pasiva ante esta evolución.

- Las nuevas tecnologías de la información y de la comunicación y el desarrollo de la sociedad de la información con ellas asociado pueden ofrecer numerosas ventajas a los consumidores pero dan también lugar a nuevos contextos comerciales con los que no están familiarizados y que pueden poner en peligro sus intereses.

- Los consumidores están especialmente interesados en temas relacionados con la lista que ya señalamos unas páginas antes.

- La confianza de los consumidores constituye un requisito indispensable para que éstos acepten la sociedad de la información y tomen parte en ella.

- Para instaurar esta confianza es necesario que exista en las nuevas tecnologías un nivel de protección equivalente al que rige en las transacciones tradicionales de los consumidores, aplicándose a los

[4] RESOLUCIÓN DEL CONSEJO de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información. *Diario Oficial n° C 023 de 28/01/1999 P. 0001 – 0003.*

nuevos productos y servicios que ofrece la sociedad de la información los principios vigentes en materia de política de los consumidores, especialmente los que indicamos anteriormente sobre transparencia, no discriminación en el acceso a productos y servicios, protección frente a las prácticas de comercialización no solicitadas, engañosas y desleales, protección de la salud, seguridad e intimidad, consulta, representación, etcétera.

- A juicio del Consejo, la mejor manera de garantizar, en la Comunidad Europea, que se tengan plenamente en cuenta los intereses de los consumidores en la sociedad de la información consiste en integrar la dimensión relativa a los consumidores y, en particular, los principios antes mencionados en materia de política de los consumidores, en las correspondientes iniciativas de la Comunidad.

- La legislación comunitaria y las legislaciones nacionales de aplicación pertinentes son aplicables a las transacciones de los consumidores en el nuevo entorno de la sociedad de la información.

- En especial la 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 ya establece, entre otras cosas, una protección en el ámbito del E-comercio.

- En el caso de las transacciones transfronterizas efectuadas por medio de las tecnologías de la información, los consumidores deben poder, en el marco del Derecho comunitario y de los Convenios de Roma y Bruselas, acogerse a la protección que ofrece la legislación de su país de residencia habitual y poder acceder fácilmente a los procedimientos de recurso, en particular en su país de residencia habitual; la Comisión ha propuesto una Directiva relativa a la comercialización a distancia de los servicios financieros para el consumidor y considera otras posibles iniciativas de armonización legislativa.

- La política comunitaria en este ámbito debe tener debidamente en cuenta el carácter plurilingüe y multicultural de la Comunidad.

- Las organizaciones de consumidores y los organismos públicos competentes desempeñan un importante papel a la hora de proteger los intereses de los consumidores, así como de facilitar información y

contenidos, y deben cumplir ese cometido a través de una acción coordinada; las empresas también pueden desempeñar un papel importante, en particular mediante códigos de conducta.

- La Comunidad debe desempeñar un papel activo a escala internacional para garantizar el cumplimiento de sus normas aceptadas de protección de los consumidores a la hora de desarrollar la sociedad de la información global.

Tras estas consideraciones, el Consejo de la Unión Europea invita a la Comisión a que:

1. Examine la legislación relativa a los consumidores vigente en la Comunidad Europea en el marco de las nuevas circunstancias derivadas de la sociedad de la información y señale posibles lagunas en problemas concretos.

2. Adopte las medidas necesarias para velar por que se tengan plenamente en cuenta los intereses de los consumidores en las propuestas, actuales o futuras.

3. Haga todo lo posible para, de conformidad con el Derecho comunitario y con las obligaciones internacionales de la Comunidad, velar por que los consumidores puedan acogerse a los derechos que ofrecen ya los Convenios de Bruselas y de Roma, entre otros los relativos a aplicabilidad de los derechos que otorga la legislación del país de residencia y los relativos al fácil acceso a su jurisdicción, y, en su caso, para potenciar tales derechos.

4. Anime a las organizaciones de consumidores a impulsar la utilización de las nuevas tecnologías como medio de ampliar sus servicios.

5. Presente al Parlamento Europeo y al Consejo un informe sobre las acciones emprendidas, acompañado de las pertinentes propuestas.

Con todo esto conviene en:

1. Preparar posiciones comunes o coordinadas de los Estados miembros en relación con debates y negociaciones y, en particular,

el desarrollo de directrices de la OCDE sobre la protección de los consumidores en el contexto del E-comercio.

2. Revisar periódicamente la evolución del papel del consumidor y de los riesgos y oportunidades que supone para éste la sociedad de la información.

Aunque en el libro V nos referiremos con mas detalle al citado papel de la OCDE, los siguientes párrafos resumen sus líneas maestras de actuación en este campo:

a) **Generación de confianza.** La generación de confianza en las transacciones comerciales ha sido tradicionalmente uno de los cometidos de los gobiernos. La OCDE colabora en la tarea de extender esta confianza a las transacciones electrónicas mediante actividades en las áreas de la seguridad y privacidad, y, más específicamente, en los temas de información y protección al consumidor: derechos de renuncia o devolución de artículos comprados electrónicamente, prevención de fraude, información sobre contratos, procedimientos de resolución de disputas que no requieran acudir a los tribunales, etcétera.

b) **Reducción de incertidumbres en la legislación.** La OCDE promueve la colaboración internacional para minimizar las diferencias entre países en el marco legal del E-comercio, incluyendo impuestos, aranceles y derechos de propiedad intelectual.

c) **Asegurar el acceso.** En concreto, la OCDE ha analizado temas como los servicios de acceso condicional, interconexión de redes, tarifas de uso de Internet, nombres de dominio y estándares para interoperabilidad.

En su informe *Business-to-Consumer Electronic Commerce: Survey of Status and Issues, la OCDE* trata los siguientes puntos: reglas sobre el establecimiento de negocios, efectividad de los contratos electrónicos, autenticación, privacidad, contenidos, pagos en Internet, protección del consumidor, impacto de los impuestos y seguridad.

1.2 Otras iniciativas internacionales

Además de la Organización Mundial de Comercio, de la UNCTAD y otras organizaciones del sistema ONU como la de la Propiedad Intelectual, cabe resaltar también otras numerosas e importantes iniciativas internacionales para mejorar la seguridad en el doble sentido ya indicado para generar confianza en el E-comercio.

Así, por ejemplo, y en un plano más práctico que generalista, la Plataforma para Preferencias de Privacidad (P3P) es un conjunto de estándares y protocolos que permiten a los usuarios especificar sus requisitos en cuanto al uso de datos personales. Igualmente, P3P permite a un servidor Web especificar su política de protección de tales datos. La P3P puede avisar al usuario cuando visita un servidor Web cuyos criterios de protección de datos privados no satisface los requisitos especificados previamente.

Igualmente, la Cámara Internacional de Comercio tiene en marcha el proyecto ECP (*Electronic Commerce Project*), cuyo objetivo es definir buenas prácticas comerciales que ayuden a crear confianza en las transacciones comerciales electrónicas. El proyecto, en el que participan especialistas de diversos campos (telecomunicaciones, banca, transporte, etcétera) se centra en tres puntos:

1. Definiciones comunes y reglas para el uso de mecanismos de autenticación electrónica. Esta primera actividad produjo a finales de 1997 el documento denominado *GUIDEC (General Usage for International Digitally Ensured Comerse),* reconocido como uno de los primeros intentos globales de autorregulación empresarial en el sector de E-comercio.

2. Reglas de procedimiento y negociación en transacciones electrónicas. Este grupo de trabajo actúa coordinadamente con miembros de la Cámara Internacional en mas de 130 países, con un doble fin: adaptar las reglas existentes para las transacciones basadas en documentos en papel a las transacciones electrónicas y, además, sacar partido de las nuevas posibilidades que ofrece Internet para simplificar los procedimientos tradicionales.

3. Servicio *E-TERMS*. Repositorio de herramientas para la elaboración de contratos electrónicos, y de reglas y cláusulas que pueden

incorporarse en estos contratos citándolas mediante un identificador único proporcionado automáticamente por el sistema. Durante 1999 se probará un prototipo del sistema con un grupo de usuarios voluntarios.

En cuanto a la Organización Mundial de Comercio, el consejo de la OMC que administra el acuerdo sobre Aspectos Comerciales de los Derechos de Propiedad Intelectual (*Agreement on Trade-Related Aspects of Intellectual Property Rights – TRIPS*) estudia los aspectos del E-comercio que pueden afectar a dicho acuerdo.

Por su parte, la Organización Mundial de la Propiedad Intelectual (OMPI), denominada en inglés WIPO (*World Intellectual Property Organization*) y autosubtitulada recientemente "una organización para el futuro", mantiene un servidor Web sobre E-comercio[5], además incluir entre los tratados internacionales que administra algunos de gran interés para esta actividad, como los siguientes:

-Convenio de Berna para la Protección de las Obras Literarias y Artísticas, Acta de París de 24 julio de 1971 (enmendado el 28 de septiembre de 1979)

-Convención de Roma (1961). Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusion (hecho en Roma el 26 de octubre de 1961)

-Tratado sobre la Propiedad Intelectual respecto de los Circuitos Integrados (adoptado en Washington el 26 de mayo de 1989)

-Arreglo de Madrid relativo al Registro Internacional de Marcas, de 14 de abril de 1891. Texto oficial español establecido en virtud del Artículo 17.1)b) .

-Acuerdo de Viena por el que se establece una clasificación internacional de los elementos figurativos de Las Marcas (Establecido en Viena el 12 de junio de 1973 y enmendado el 1 de octubre de 1985)

[5] http://www.wipo.org/spa/internet/ecommerc/index.htm

-Arreglo de La Haya relativo al depósito internacional de dibujos y modelos industriales (II. Acta de La Haya de 28 de noviembre de 1960).

-Arreglo de Lisboa relativo a la Protección de las Denominaciones de Origen y su Registro Internacional, de 31 de octubre de 1958 (revisado en Estocolmo el 14 de julio de 1967 y modificado el 2 de octubre de 1979)

-Tratado de Cooperación en materia de Patentes (PCT) (elaborado en Wáshington el 19 de junio de 1970, enmendado el 2 de octubre de 1979 y modificado el 3 de febrero de 1984)

- Convenio para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas, de 29 de octubre de 1971

-Tratado de la OMPI sobre Derecho de Autor

-Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas
-Acuerdo entre la Organización Mundial de la Propiedad Intelectual y la rganización Mundial del Comercio (concertado en Ginebra le 22 diciembre de 1995).

La OMPI lanzó en 1998 un proyecto de Red Mundial (conocida como WIPONET) para proporcionar servicios a las oficinas de propiedad intelectual de todo el mundo y facilitar el rápido intercambio entre las mismas. A largo plazo, tiene previsto que también sirva de marco para que las oficinas puedan proponer, examinar y aplicar ideas innovadoras con el fin de promover la protección de la propiedad intelectual.

Por su parte, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL por las iniciales de su nombre en inglés: *United Nations Commission on International Trade Law*) tiene el cometido general de eliminar o reducir las disparidades en legislaciones nacionales que puedan crear obstáculos al comercio internacional. Esta comisión ha elaborado una Ley Modelo de E-comercio, adoptada en 1996. La ley establece un marco para determinar el valor legal de los mensajes electrónicos basado en definir para este nuevo escenario conceptos funcionalmente equivalentes a los conceptos tradicionales de "documento original", "firma", etcétera. Además, la comisión tiene un grupo de trabajo sobre E-comercio que ha producido documentos sobre firmas digitales, autoridades de certificación y aspectos legales relacionados.

1.3 Iniciativas en España

En España, y sin perjuicio tampoco de un mayor detalle en las iniciativas para el desarrollo del E-comercio que se relatan en el libro VI, en 1998 entró en vigor la directiva europea sobre protección de datos y se abrió un proceso de revisión de la legislación española aplicable a este tema (la LORTAD).

Aunque más adelante se describirá con mayor detalle el panorama, cabe destacar que una de las iniciativas más encomiables en esta línea es la elaboración de un código ético sobre el tratamiento de datos personales de consumidores obtenidos a través de Internet. Según la Asociación Española de E-comercio (AECE), entidad promotora, es pionero en Europa y será adoptado en otros países. Ha sido elaborado con la participación de la Agencia de Protección de Datos (APD), Asociación de Autocontrol de la Publicidad (AAP), Confederación de Consumidores y Usuarios (CECU), Organización de Consumidores y Usuarios (OCU) y Unión de Consumidores de España (UCE). En esencia, el código propuesto se basa en el principio de permitir el uso de los datos siempre que los consumidores estén informados de los fines para los que una determinada empresa se propone utilizarlos (por ejemplo, para enviar información de otros productos, para ceder los datos a un tercero, etcéteraétera.) y que se ofrezca al consumidor la posibilidad de restringir o prohibir dicho uso. AECE defiende por tanto el principio de uso de los datos en ausencia de negación expresa, frente al principio, más restrictivo, de usar los datos sólo cuando hay consentimiento expreso. Para organizar su cumplimiento, se ha creado un comité de control, que se ocupará de las reclamaciones de consumidores y realizará auditorias periódicas aleatorias para comprobar que todas las empresas que tienen el símbolo de garantía en su Web cumplen con las obligaciones del código.

La otra gran asociación española, CommerceNet Español, mantiene un círculo de expertos y consultores que ofrece asesoramiento en temas legales y seguridad, criptografía y certificación digital, entre otros.

Por su parte, la Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE), integrada por los consejos generales del Notariado, Corredores de Comercio y de la Abogacía, realiza estudios y proyectos sobre los mecanismos e instrumentos de seguridad , además de actuar como servicio de certificación de las comunicaciones electrónicas, formando parte de la red europea de seguridad y confianza de las comunicaciones electrónicas. Tiene su origen en un proyecto europeo para

elaborar soluciones jurídicas que permitieran la prueba en juicio de carácter penal de mensajes electrónicos enviados cifrados y firmados digitalmente. A raíz del proyecto, surgió la iniciativa de constituir un proveedor de servicios de certificación de las comunicaciones electrónicas avalado por los notarios y corredores de comercio (que son los fedatarios de las operaciones mercantiles tradicionales). Este servicio de certificación se denomina también FESTE. Asociación Española de Distribuidores de Información Electrónica .

Asimismo, la Asociación Española de Empresas de Tecnologías de la Información (SEDISI), tiene la finalidad de promover y publicar códigos éticos, guías y recomendaciones, además de cooperar con asociaciones internacionales y con la Comunidad Europea en el desarrollo y modificaciones legislativas que afectan al sector de la Informática y de las Telecomunicaciones.

Finalidades similares, aunque más centradas en la difusión entre los abogados, son acometidas por la Asociación Española de Derecho de las Telecomunicaciones y Tecnologías de la Información (ADETI).

Por su parte, la Asociación para la Investigación de Medios de Comunicación (AECOC), además de sus actividades en la identificación automática de productos (código de barras), la logística, el merchandising y el medio ambiente (envases y embalajes), lleva más de 10 años trabajando en el Intercambio Electrónico de Datos (EDI), tanto en la definición de estándares sectoriales como en la prestación de servicios.

2 Marco Legal del E-comercio: una perspectiva europea

El marco legal se ha convertido especialmente en una obsesión desde la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del E-comercio en el mercado interior[6], que decía:

"El E-comercio ofrece a la Comunidad una oportunidad única de estimular el crecimiento económico, aumentar la competitividad de la industria europea y fomentar las inversiones innovadoras y la creación de puestos de trabajo. No obstante, sólo se podrá obtener el máximo provecho si se suprimen los numerosos obstáculos jurídicos que persisten en el sector de la prestación de servicios en línea —especialmente importante para los intercambios transfronterizos y las PYME—. Con la presente propuesta de Directiva se pretende eliminar dichos obstáculos y, de esta manera, permitir a los ciudadanos y empresas de la Unión Europea que saquen el máximo rendimiento del desarrollo del E-comercio en Europa".

En una Comunicación de la Comisión sobre el E-comercio[7], que fue publicada en 1997, se fijó un objetivo claro: la creación para el año 2000 de un marco jurídico coherente a escala europea. Ya entonces planteaban cinco cuestiones problemáticas:

1) Lugar de establecimiento de los prestadores de servicios

"La propuesta permite eliminar la inseguridad jurídica que existe actualmente en la materia al definir el lugar de establecimiento de conformidad con los principios enunciados en el Tratado y la jurisprudencia del Tribunal de Justicia. Es éste un punto esencial para el buen funcionamiento del mercado único. En la propuesta también se prevé la prohibición de regímenes específicos de autorización para los servicios de la sociedad de la información y, en cuanto a la información, se fijan determinados requisitos que el prestador de servicios deberá cumplir para garantizar la transparencia de sus actividades".

---

[6] Bruselas, 18.11.1988, COM(1998) 586 final. 98/0325 (COD)

[7] "Iniciativa europea de E-comercio", COM(97) 157 final, 16.04.1997.

2) Comunicaciones comerciales (publicidad, marketing directo, etcétera)

"Las comunicaciones comerciales constituyen un aspecto esencial de la mayoría de los servicios de E-comercio. Por lo tanto, es importante precisar y facilitar su utilización. Así pues, en esta propuesta se define el concepto de "comunicaciones comerciales" y, en relación con ellas, se fijan determinados requisitos de transparencia para garantizar la confianza de los consumidores y fomentar las prácticas comerciales leales. Con el fin de que los consumidores puedan reaccionar con mayor rapidez en caso de injerencia perjudicial, en la propuesta se dispone que las comunicaciones comerciales realizadas por correo electrónico deberán ser claramente identificables. Además, por lo que se refiere a las profesiones reguladas (como la abogacía), las legislaciones nacionales relativas a la comunicación comercial deberán permitir la prestación de servicios en línea siempre que se respeten las normas de deontología. Con este fin, las organizaciones profesionales deberán elaborar códigos de conducta".

3) Celebración de contratos en línea

"El E-comercio no se podrá desarrollar completamente si se dificulta la celebración de contratos en línea mediante la existencia de determinadas condiciones, sobre todo de tipo formal, que no son adecuadas para este tipo de entorno. Los Estados miembros deberán revisar su legislación en este sentido. Además, la propuesta permite también eliminar la inseguridad jurídica: en efecto, en la propuesta se precisa cuál es, en determinados casos, el momento de la celebración del contrato, sin dejar de respetar plenamente la libertad contractual".

4) Responsabilidad de los intermediarios

"Está generalmente admitido que, si se quiere facilitar el E-comercio, conviene precisar qué responsabilidad incumbe a los prestadores de servicios en línea por lo que se refiere a la transmisión y almacenamiento de datos pertenecientes a terceras personas (dichos prestadores de servicios actúan, pues, como "intermediarios"). Para eliminar la actual inseguridad jurídica y dar coherencia a los distintos enfoques que están saliendo a la luz en los Estados miembros, en la propuesta se prevé una excepción para los casos en que los prestadores de servicios realicen un "mero transporte" y se limita su responsabilidad en lo que se refiere a las demás actividades de "intermediario". Se intenta conseguir un equilibrio prudente entre los distintos

intereses que están en juego, de forma que se fomente la cooperación entre las partes y, de esta manera, se limite el riesgo de que haya actividades ilícitas en línea".

5) Aplicación de las normativas

"En vez de elaborar nuevas normas, la Comisión ha querido garantizar la aplicación real de la normativa comunitaria y de las legislaciones nacionales existentes. La consolidación de los mecanismos necesarios para este fin favorece la creación de un auténtico mercado interior basado en la confianza mutua entre Estados miembros. Para llevar a cabo esta consolidación, está previsto fomentar la elaboración de códigos de conducta a escala comunitaria, estimular la cooperación administrativa entre Estados miembros y facilitar la creación de otros sistemas eficaces para solucionar litigios transfronterizos. Por parecidas razones, en la propuesta se dispone que los Estados miembros estarán obligados a instaurar un sistema de recurso judicial rápido y eficaz, adaptado al entorno en línea".

2.1 Mercado interior

Mientras no se apliquen las normas mundiales en diferentes ámbitos, la Unión debe actuar para establecer en Europa un auténtico mercado interior para el E-comercio. Este mercado único debe garantizar a los ciudadanos y a los operadores europeos el disfrute y la prestación de los servicios de la sociedad de la información en toda la Comunidad sin consideración de fronteras. En efecto, el marco jurídico del mercado interior es una importante baza para el E-comercio y el E-comercio es un triunfo importante del mercado interior:

- De cara a la *construcción europea*, el E-comercio en el espacio sin fronteras favorecerá el acercamiento y los intercambios entre los pueblos europeos, así como el conocimiento de su diversidad cultural.

- En cuanto a los *ciudadanos y consumidores europeos*, el E-comercio les permitirá acceder a más servicios y productos de mejor calidad a menor coste y generará una mayor preocupación por la protección del ciudadano a escala comunitaria y no solamente a escala nacional.

- Para las *empresas europeas*, en concreto las PYME, el E-comercio ofrecerá considerables oportunidades de crecimiento y fomentará las inversiones en innovación.

- Para el *crecimiento del empleo en la Comunidad*. Aunque no es posible evaluar la cantidad total de personas empleadas actualmente en las actividades de E-comercio, dichas actividades representan una verdadera oportunidad para el empleo. Por ejemplo, según determinadas estimaciones se crearon en la Comunidad entre 1995 y 1997 más de 400 000 empleos vinculados a la sociedad de la información. Asimismo según dichas estimaciones, uno de cada cuatro empleos nuevos en la Comunidad procede de dichas actividades; las estimaciones muestran que actualmente existen unos 500 000 puestos de trabajo por ocupar en oficios de la sociedad de la información y que el 60% de estas posibilidades de empleo se hallan en las PYME que desean desarrollar sus actividades de E-comercio.

Una actividad de servicios de la sociedad de la información se basa en el E-comercio. Se trata de servicios en línea consistentes, por ejemplo, en vender mercancías o servicios o en proporcionar gratuitamente información financiada por la comunicación comercial. Estos servicios no se desarrollan en un vacío jurídico. Bien al contrario, ya están sometidos a una serie de normativas nacionales, comunitarias o internacionales. Sin embargo, en relación con los objetivos del mercado interior y los principios de libertad de establecimiento y de libre prestación de servicios determinados aspectos del marco jurídico actual deben aclararse para aumentar la seguridad jurídica. Efectivamente, cierto número de barreras jurídicas entorpecen o hacen menos atractivo el ejercicio de estas libertades para los prestadores de servicios de la sociedad de la información y para los ciudadanos que utilizan estos servicios.

2.2 Opacidad del marco actual

La disparidad de determinadas disposiciones legislativas. Esto significa que un prestador que desea ofrecer sus servicios a la totalidad del mercado interior y que respeta la normativa del país donde está establecido debe también garantizar que sus actividades son compatibles con la legislación de los otros 15 Estados miembros.

Importante inseguridad jurídica. La inseguridad se manifiesta en la legalidad de las medidas que puede tomar un Estado miembro contra los servicios

facilitados por prestadores establecidos en otro Estado miembro (¿están justificadas en relación con el principio de libre circulación de servicios o con el derecho comunitario derivado que pone en práctica este principio?).

En algunos Estados miembros se obserba *cierto movimiento* destinado a proponer nuevas normativas, movimiento que ya muestra diferentes enfoques y que plantea a corto plazo el riesgo real de fragmentación del mercado interior.

2.3 Importantes costes económicos

- Importancia de los costes jurídicos: Los costes jurídicos calculados para poner en marcha un nuevo servicio de la sociedad de la información varían mucho. Pero en general son elevados debido a la diversidad jurídica.

- Especificidad de los costes jurídicos para el E-comercio: no menos de un 40% de las empresas que han realizado una evaluación jurídica de su actividad estiman que la inseguridad jurídica que caracteriza el E-comercio es más importante que en otros tipos de actividades.

- Principales ámbitos que generan costes jurídicos: las encuestas permiten mostrar los ámbitos jurídicos en los que se presentan los problemas más importantes:

2.4 Impacto en las inversiones y la competitividad de las empresas europeas

Un operador que desee realizar operaciones de E-comercio en la totalidad del mercado interior casi nunca tiene la seguridad de que su servicio no vaya a someterse al control o a medidas restrictivas directas o indirectas por parte de Estados miembros distintos al de establecimiento. Esto hace que los operadores deban acudir a expertos jurídicos (abogados, consultores, etcétera.) en cada Estado miembro, e iniciar negociaciones con las autoridades de estos países para recibir la «luz verde» sobre la legalidad de su actividad. Ello genera una serie de impactos:

- *Impacto en las inversiones*: los operadores, especialmente las PYME y las microempresas, que no poseen los medios necesarios para hacer frente a los

costes de una asistencia jurídica eficaz, renuncian a explotar las oportunidades del mercado interior y a invertir en el desarrollo europeo de sus actividades.

- *Impacto en la competitividad de las empresas europeas*: los operadores deben diseñar su servicio de manera que sea compatible en todos los Estados miembros. Esto les disuade de toda inversión en innovación y puede provocar que se midan los servicios según el nivel del Estado miembro que imponga las mayores limitaciones.

- *Desconfianza de los consumidores.* Debido a esta serie de incertidumbres el consumidor se siente en un entorno poco claro y confuso, y al tener pocas garantías en cuanto a la calidad de la protección facilitada, el consumidor y, más generalmente, el destinatario de los servicios, puede desistir de formalizar contratos en línea y de beneficiarse de las nuevas oportunidades. De ahí la importancia de acotar y superar las barreras jurídicas.

2.5 Barreras jurídicas

Las barreras jurídicas en su sentido más extenso han de tipificarse y superarse en cada uno de los siguientes ámbitos:

- Establecimiento de los operadores

Existen grandes divergencias entre los diversos enfoques, así como numerosos aspectos jurídicamente dudosos:

- *Determinación del lugar de establecimiento* de un servicio en línea. Esta es especialmente confusa: ¿Es el servidor que alberga un sitio o el hecho de poder acceder a un sitio en un Estado miembro, o es un simple buzón?

- R*egímenes de autorización o de declaración*. En la mayoría de los Estados miembros, los servicios que pueden incluirse en la categoría de servicios de la sociedad de la información generalmente no están sometidos a autorización específica. En varios Estados miembros existe un régimen general de declaración, mientras que en otros no se exige ninguna formalidad. Las dudas van surgiendo a medida que se crean nuevos tipos de servicios que pueden originar problemas de

clasificación de actividades respecto a las categorías existentes (prensa, telecomunicaciones, audiovisual, etcétera).

Respecto al principio de la libertad de establecimiento (artículo 52 del Tratado), debe beneficiar a toda persona que desea acceder a las actividades de prestación de servicios a través de Internet. Pero esa situación es necesario esclarecerla para facilitar el ejercicio de dicha libertad.

- Comunicaciones comerciales

Desde la perspectiva de las comunicaciones comerciales, los obstáculos para el mercado interior son especialmente importantes:

- Las definiciones existentes relativas a la comunicación comercial (por ejemplo, sobre «publicidad» o «patrocinio») son fuentes de incertidumbre desde el momento en que se aplican a los servicios en línea; por ejemplo, en la mayoría de los Estados miembros, no es posible lograr una respuesta definida a la pregunta de si el simple hecho de tener un sitio Internet, establecer un vínculo de hipertexto o utilizar un nombre de dominio constituye comunicación comercial. Esto es especialmente perjudicial porque, según la interpretación que se haga de las definiciones existentes, se aplicarán regímenes más o menos adaptados.

- La disparidad de las normativas sobre la *publicidad de las profesiones reguladas* constituye uno de los obstáculos declarados para el desarrollo de las actividades de servicios profesionales en Internet. Efectivamente, el uso de un sitio Internet por parte de un servicio profesional con frecuencia se considera comunicación comercial y las legislaciones relativas a las profesiones reguladas sufren profundas divergencias sobre esta cuestión: por ejemplo, en numerosos Estados miembros, la publicidad está estrictamente prohibida (por ejemplo, para los *abogados* y los *médicos*); en otros Estados miembros el régimen es mucho más flexible, especialmente para las profesiones jurídicas.

- Las normativas nacionales sobre la *competencia desleal* pueden tener efectos muy restrictivos, dado que su interpretación puede llevar a prohibiciones o limitaciones de determinadas prácticas comerciales como las ofertas promocionales (por ejemplo, descuentos o primas). Estos efectos son especialmente graves para las nuevas prácticas de

márketing de carácter innovador y la necesidad de utilizarlas en Internet a fin de darse a conocer entre la gran cantidad de servicios disponibles.

- Los requisitos de *transparencia* (por ejemplo, la advertencia de que se trata de publicidad o patrocinio) son muy divergentes o poco claros. En la mayoría de los Estados miembros, no existe ninguna obligación clara y general de indicar en un sitio Internet la existencia de una comunicación comercial o a nombre de quién se realiza. Por el contrario, en algunos Estados miembros, las obligaciones en este sentido pueden derivarse de las normas generales sobre la protección del consumidor o la fidelidad de las operaciones, o bien de normativas específicas.

- Las nuevas prácticas de comunicación comercial *intrusiva*, como el «bombardeo», o la publicidad en los foros de discusión, plantean cierto número de debates que ya han dado lugar a que las jurisdicciones nacionales se pronuncien o a que los Estados miembros intervengan por vía reglamentaria.

- Contratos por vía electrónica

Se han identificado obstáculos específicos cuyo fin es limitar las posibilidades de formalizar contratos en línea traspasando las fronteras:

- Ciertos *requisitos formales* impiden celebrar un contrato en formato electrónico o provocan una gran inseguridad jurídica sobre su legalidad o validez. En el ámbito comunitario, la reciente propuesta de directiva relativa a la firma electrónica no aborda condiciones formales distintas a la firma.

- Los *comportamientos específicos* que adoptan las partes para contratar por vía electrónica provocan una gran inseguridad jurídica respecto a la celebración del contrato. En especial, la propia acción de hacer clic en el icono «Aceptar» puede tener un significado jurídico distinto para cada Estado miembro.

- Responsabilidad de los intermediarios

En lo relativo a la aplicación de sus actuales regímenes de responsabilidad a los prestadores, existe una gran incertidumbre jurídica en los Estados miembros de servicios de la sociedad de la información, cuando estos tienen la función de "intermediarios", es decir, cuando transmiten o albergan información procedente de terceros (suministrada por los usuarios del servicio). Precisamente estas actividades son objeto de distintas iniciativas emprendidas (o en fase de estudio) por los Estados miembros sobre la cuestión de la responsabilidad.

Hay que tener en cuenta el limitado conocimiento que tienen los prestadores de servicios sobre la información que transmiten o almacenan en las redes de comunicación interactiva. La principal dificultad estriba en determinar qué grado de responsabilidad corresponde a los prestadores de servicios en línea que difunden y almacenan información ilícita y cuál a las personas que han colocado inicialmente la información en línea.

Ante el mercado interior europeo, estas divergencias podrían ser una fuente de obstáculos a la prestación transfronteriza de los servicios de la sociedad de la información. Es el caso de si un Estado miembro decide prohibir el acceso a información almacenada en el servidor de un prestador de servicios establecido en otro Estado miembro donde el régimen de responsabilidad aplicable es considerado poco satisfactorio. En algunos Estados miembros, esta situación puede obstaculizar asimismo actividades tales como la prestación de servicios de alojamiento. La situación actual incita, en efecto, a los prestadores de servicios a implantar estas actividades en los Estados miembros dotados de regímenes favorables y expone a una gran inseguridad jurídica a las diferentes partes (prestadores de servicios, proveedores de contenido, personas cuyos derechos se ven violados y consumidores en general).

- Arreglo de las controversias

Para enfrentarse a comportamientos ilícitos o a litigios sobre Internet, las medidas judiciales o extrajudiciales que se pueden tomar en casos transfronterizos no siempre son lo bastante eficaces, ni están suficientemente adaptadas para poder convencer a los prestadores de servicios de que los presten y a los destinatarios, en especial los consumidores, de que los utilicen. Sin embargo, el Tribunal de Justicia ha indicado claramente[8] que el

[8] Sentencia de 26 de septiembre de 1996, Data Delecta y Forsberg, C-43/95 .

acceso a la justicia es el corolario de las libertades del espacio sin fronteras interiores. Por otro lado, el Parlamento Europeo ha subrayado las necesidades en materia de arbitraje[9]. Esta falta de adaptación al carácter específico de Internet y a las situaciones transfronterizas se muestra en numerosos niveles:

- *Lentitud de los medios de actuación*; los comportamientos ilícitos en Internet producen perjuicios caracterizados por su rapidez y su amplitud geográfica. Para enfrentarse a ellos, a veces la eficacia de las medidas de urgencia resulta disuasoria y éstas deben mejorarse.

- *Costes en proporción con la naturaleza de las actividades*: además de los litigios entre profesionales, los problemas relativos a Internet pueden incluir pequeños litigios relativos a importes reducidos (micropagos) o litigios entre particulares que hayan utilizado un servicio de la sociedad de la información (anuncios breves, por ejemplo) que no justifican el recurso a actuaciones judiciales gravosas, decantándose por los mecanismos extrajudiciales de solución de conflictos.

- Los medios de los que disponen las *autoridades nacionales*, la colaboración entre éstas y el acceso a las autoridades no siempre son transparentes y eficaces. Este aspecto debe ser objeto de un estudio más sistemático que cubra la totalidad de los servicios de la sociedad de la información.

- Papel de las autoridades nacionales y principio del país de origen

Existe una gran incertidumbre a la hora de determinar qué Estado miembro es competente para el control de las diversas actividades. En algunos casos, una misma actividad se puede someter al control y al régimen jurídico de varios Estados miembros: si se tiene en cuenta que los diversos elementos de la cadena económica de una actividad determinada (contenidos suministrados, alojamiento de datos, acceso a Internet, comunicación comercial, etcétera.) se pueden vincular al territorio de varios Estados miembros, esto podrá dar lugar a una multiplicación de los puntos de control y, por consiguiente, de las fronteras jurídicas. En otros casos, por el contrario, algunas actividades no son controladas por el Estado miembro en cuyo territorio se encuentra establecido el prestador de servicios.

9 Resolución del Parlamento de 14.05.1998, punto 32.

La indefinición sobre «quién controla qué» es perjudicial a la vez para la libre circulación de los servicios de la sociedad de la información y para el control de los servicios. Por ello es necesario mejorar el *nivel de confianza mutua* entre las autoridades nacionales clarificando la aplicación del principio de libre circulación de servicios. Efectivamente, este principio (artículos 59 y 60 del Tratado) implica que el control corresponde al país en el cual está establecido el prestador (porque, salvo excepciones, los Estados miembros no pueden imponer restricciones a los servicios procedentes de un prestador establecido en otro Estado miembro).

La incertidumbre sobre la definición de "*establecimiento*" impide, en particular, esclarecer con precisión las responsabilidades de las autoridades nacionales. Por otra parte, *la falta de información* sobre el origen del prestador de servicios y sus actividades. En efecto, el análisis de las normativas pone de manifiesto que en la mayoría de los Estados miembros no existe como tal la obligación sistemática de informar sobre el sitio (es decir, de manera independiente respecto a una oferta comercial contractual). Por último, también exige una clarificación el hecho de que los operadores *no tengan la certidumbre de que su servicio no estará sujeto a medidas restrictivas* en otro Estado miembro.

2.6 La mínima interferencia con los regímenes judiciales nacionales

Para que la interferencia de las normas supranacionales, sean comunitarias o internacionales, no se convierta en barrera se ha de cumplir las siguientes normas:

- Tratar sólo lo estrictamente necesario para el mercado interior

Consiste en interferir lo menos posible con los regímenes jurídicos nacionales e intervenir únicamente donde sea estrictamente necesario para el buen funcionamiento del espacio sin fronteras. En efecto, el reconocimiento mutuo y el acervo del Derecho comunitario existente permiten reducir la necesidad de nuevas intervenciones reglamentarias.

- Cubrir todos los servicios de la sociedad de la información

La Directiva se aplica a los «servicios de la sociedad de la información», es decir, a todo servicio prestado, normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario del mismo. Esta definición ya ha sido adoptada por la Directiva 98/34/CE del Parlamento Europeo y del Consejo, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas[10] y por la propuesta de directiva relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso[11]. Esta definición abarca *multitud de actividades económicas* muy diversas que se pueden efectuar en línea. Puede tratarse de las siguientes:

- Servicios de empresa a empresa o de empresa a consumidores.

- *Servicios de venta* de bienes o servicios, así como *servicios gratuitos*[12] para el destinatario (cuya financiación está garantizada frecuentemente por la comunicación comercial).

- Servicios que permitan realizar o*peraciones electrónicas en línea para comprar mercancías*, tales como la telecompra interactiva, los centros comerciales electrónicos, etcétera. (el hecho de que la mercancía no se entregue en línea no obsta para que la telecompra interactiva constituya un servicio de la sociedad de la información).

---

[10] DO L 204, de 21.7.1998 p. 37, modificada por la Directiva 98/48/CE del Parlamento Europeo y del Consejo, del 20.07.1998, que modifica la Directiva 98/34/CE por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, DO L 217, de 5.8.1998, p.18.

[11] Posición común 43/98 aprobada por el Consejo el 29.06.1998 con vistas a la adopción de la Directiva 98/.../CE del Parlamento Europeo y del Consejo relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso, DO C 262, de 19.8.1998, p. 34.

[12] La definición del servicio no exige, en efecto, un pago del destinatario. Conforme a la jurisprudencia del Tribunal de Justicia, la noción de prestación realizada «normalmente a cambio de una remuneración» (que se encuentra en el artículo 60 del Tratado por el que se define lo que es un servicio) no hace referencia a las modalidades concretas de financiación del servicio dado («el artículo 60 no exige que el servicio sea pagado por sus beneficiarios» - asunto C-352/85, punto 16), sino a la existencia de una actividad que tiene «naturaleza económica» o de una «contrapartida económica» (asunto 109/92, punto 15).

- Una enorme *variedad de áreas y actividades*, por ejemplo, periódicos electrónicos, servicios educativos, enciclopedias en línea, servicios de venta de determinados productos como automóviles, servicios turísticos, servicios profesionales (abogados, médicos, expertos contables, etcétera), servicios de agencia inmobiliaria, supermercados virtuales, servicios de anuncios breves, tablones de anuncios electrónicos, servicios de búsqueda de empleo, motores de búsqueda, servicios de ocio, servicios de videojuegos, servicios de acceso a la World Wide Web, foros de discusión, etcétera.

Se deben abarcar el conjunto de estas actividades pues todos los servicios deben tener la posibilidad de beneficiarse del mercado interior y necesitan, en el ámbito jurídico, la garantía de poder desarrollarse sin tener en cuenta las fronteras.

- Tratar las cuestiones en un mismo instrumento

Deben tratarse los obstáculos que subsisten, en un mismo instrumento para abarcar las *diferentes fases de la actividad económica de los servicios pertinentes*: para poder ejercer dicha actividad es necesario comenzar por:

a) Establecerse
b) Iniciar una comunicación comercial
c) Formalizar el contrato con un destinatario
d) En caso de desacuerdos enfrentarse a problemas de responsabilidad
e) Y encontrar mecanismos de solución de conflictos, etcétera.

La Comisión, de acuerdo con lo anunciado en su Comunicación del 16 de abril de 1997[13], ha identificado en esta cadena económica los elementos clave que necesitan unas reglas del juego comunitarias para que las actividades pertinentes no se enfrenten a obstáculos a nivel transfronterizo.

Tratar los obstáculos en un mismo instrumento permite *garantizar la coherencia agrupando las cuestiones que son interdependientes*. Las disposiciones de la Directiva responden a problemas que deben examinarse conjuntamente, pues las soluciones propuestas son, en la mayoría de los

13 Capítulo 3, apartado 40 y siguiente.

casos, comunes a un gran número de servicios de la sociedad de la información y están vinculadas entre sí.

- No tratar los aspectos externos

Hasta que exista un marco normativo a nivel internacional, la Directiva solamente cubre la situación de los prestadores de servicios establecidos en un Estado miembro. En esta fase no cubre la situación de los servicios de la sociedad de la información procedentes de un prestador establecido en un país no perteneciente a la Comunidad[14]. En la práctica, esto significa que:

- Los prestadores de servicios que no están establecidos en la Comunidad *no pueden beneficiarse de las oportunidades del espacio sin fronteras interiores* tal como lo garantiza la Directiva que nos ocupa. Para poder beneficiarse de ella deberían establecerse en un Estado miembro.

- La presente Directiva se aplicará sin perjuicio de:
  - Los derechos y obligaciones internacionales de la Comunidad
  - El resultado de los diversos debates sobre aspectos jurídicos del E-comercio a nivel de organizaciones internacionales.

Esto se explica por el hecho de que el objetivo de la Directiva es garantizar el buen funcionamiento del mercado interior y porque la Comunidad ya participa activamente en las distintas tareas destinadas a constituir un marco global para la sociedad de la información.

- Basarse en los derechos y libertades fundamentales

Las actividades de servicios de la sociedad de la información constituyen a la vez servicios en el sentido de los artículos 59 y 60 del Tratado y medios de información que se benefician del principio de la libertad de expresión previsto

[14] Obsérvese que la ubicación geográfica de los medios tecnológicos utilizados no se debe tener en cuenta (la definición del establecimiento no utiliza criterios vinculados a la tecnología, sino relativos a la actividad económica). Así, los servicios de la sociedad de la información que utilizan medios técnicos en terceros países, por ejemplo, el alojamiento en un servidor, quedan cubiertos si el prestador de servicios está establecido en la Comunidad. Por el contrario, los prestadores de servicios establecidos en terceros países que utilicen un servidor en la Comunidad no deberán someterse a la Directiva.

en el artículo 10 del Convenio europeo para la protección de los derechos humanos.

De esta forma, estas actividades pueden invocar simultáneamente el principio de libre circulación de servicios, la libertad de establecimiento y la libertad de expresión. Esta característica básica justifica la aplicación de los principios del mercado interior, en concreto el artículo 3, que prevé que los Estados miembros *no pueden imponer limitaciones a los servicios prestados* por un prestador establecido en otro Estado miembro y que ya esté sometido al control y al régimen jurídico de este último.

- Establecer un marco ágil, evolutivo y flexible

La Directiva tiene en cuenta el hecho de que el desarrollo del E-comercio está dando sus primeros pasos, que no debe verse limitado por normas prematuras y mal adaptadas, y que las distintas partes interesadas pueden regular numerosos aspectos. Además, la Directiva se basa en el acervo constituido por el conjunto de directivas ya adoptadas para la aplicación del mercado interior. Por consiguiente, la prioridad no es elaborar toda una serie de normas nuevas, sino, por una parte, coordinar el ajuste y la modernización de las legislaciones nacionales que no están adaptadas al E-comercio y, por otra parte, garantizar la aplicación efectiva y eficaz de las normas actuales. Este objetivo explica, por ejemplo:

- El hecho de que la Directiva se concentre exclusivamente en los requisitos de fondo que los Estados miembros deben transponer *sean cuales sean* las categorías o regímenes en los cuales se incluyan.

- Las disposiciones destinadas a permitir que las partes interesadas o las autoridades nacionales se encarguen de las *modalidades de aplicación* de algunas disposiciones de la Directiva. La Directiva fomenta la *elaboración de códigos de conducta* a nivel europeo puesto que las propias partes interesadas pueden regular numerosas cuestiones relativas al E-comercio sin que sea necesaria intervención alguna a nivel legislativo.

- Que la directiva, a fin de tener en cuenta las particularidades de determinados ámbitos o actividades, prevea *excepciones a los principios del mercado interior*, justificadas por la jurisprudencia del Tribunal

- Garantizar un elevado nivel de protección de los consumidores

Teniendo en cuenta la apuesta que representa el E-comercio para el sector europeo de servicios y que su desarrollo acaba de empezar, es esencial no ponerle frenos y favorecer el crecimiento de este sector al tiempo que se garantiza el cumplimiento eficaz y efectivo de objetivos de interés general, como la protección del consumidor. De esta forma, la Directiva prevé una serie de medidas que reforzarán la protección del consumidor y aumentarán su confianza en los nuevos servicios en Europa; en particular:

- *Disminuirá los riesgos de actividades ilegales* en Internet en Europa al prever un control efectivo de las autoridades nacionales en el origen mismo de las actividades (en el Estado miembro en que esté establecida la empresa de que se trate). . Tendrá por efecto responsabilizar a las autoridades nacionales respecto a su obligación de garantizar la protección del interés general, no sólo dentro de sus fronteras sino en la totalidad de la Comunidad y en favor de los ciudadanos de los demás Estados miembros.

- Impone obligaciones de *información y transparencia* a los operadores, que son imprescindibles para que el consumidor pueda adoptar decisiones con conocimiento de causa.

- Prevé determinadas garantías nuevas en las *relaciones contractuales*, en particular la obligación de poner a disposición de los usuarios los medios que les permitan corregir errores de manipulación, la clarificación del momento en que se formaliza un contrato en línea y la necesidad de que el prestador de servicios envíe un acuse de recibo.

- Garantiza mejores *medios de recurso* a través del fomento de códigos de conducta, haciendo posible el uso en línea de mecanismos extrajudiciales de solución de litigios (conciliación, arbitraje), facilitando los recursos jurídicos eficaces y rápidos y estableciendo puntos de contacto en los Estados miembros encargados de ayudar a los consumidores.

Además, la Directiva deja a los Estados miembros la posibilidad de adoptar, por motivos de protección del consumidor y en determinadas condiciones, medidas que impongan limitaciones a la libre circulación de los servicios de la

sociedad de la información, en particular en el ámbito de los contratos con los consumidores.

Cabe observar que los criterios del Convenio de Roma sobre la ley aplicable a las obligaciones contractuales, que permiten la aplicación de un régimen de excepción en favor del consumidor, se cumplirían, por ejemplo, si la conclusión del contrato estuvo precedida en el país del consumidor por una propuesta especialmente realizada mediante el envío de un mensaje electrónico y si el consumidor realizó en su país los actos necesarios para la conclusión del contrato.

Por último, habida cuenta de la *rapidez* y *amplitud* geográfica de los perjuicios que pueden producirse a causa de las actividades ilícitas en Internet, es deseable que los Estados miembros permitan que el acto original de recurso a la justicia nacional se transmita por vías electrónicas apropiadas y esté hecho en una lengua de la Comunidad diferente de la del Estado miembro de la jurisdicción.

3 Principales aspectos jurídicos del E-comercio: una visión española

Una de las primeras y más completas visiones de los aspectos jurídicos del E-comercio ha sido sistematizada por Javier Ribas[15], cuyos trabajos y cuyo "*Manual práctico sobre E-comercio en Internet*" pueden encontrarse encontrarse en la Web[16]**.**

- Propiedad intelectual e industrial de los contenidos

La propiedad intelectual e industrial de los contenidos, uno de los aspectos más complejos, nos remite a una serie de temas como el diseño de la oferta, los contenidos de un Web y otros que veremos a continuación siguiendo al mismo autor.

- Diseño de la oferta comercial

Un *web site* tiene tres elementos susceptibles de ser protegidos mediante el derecho de autor: la información que contiene, el diseño gráfico y el código fuente que debe ser interpretado por el programa navegador o *browser*[17].

Aunque el contenido es el que genera a los usuarios de Internet la necesidad de visitar un web, el diseño gráfico es el que le da su atractivo y hace que el usuario se sienta cómodo. En muchos casos, es el diseño gráfico el que, a través de las revistas especializadas, hace que los cibernautas se sientan atraídos por esa URL.

En el comercio convencional, se intenta, a través de la publicidad, que la oferta sea atractiva para el consumidor potencial de un producto o servicio. En Internet, existe un gran empeño en que el atractivo de la oferta comercial sea incluso superior al que se daría en la vida presencial. Este fenómeno tiene su explicación en diversas causas, entre las que cabe destacar las siguientes:

1. Al no estar presentes las partes, la imagen corporativa de la empresa depende de la apariencia estética y los contenidos del web.

---

[15] **Javier Ribas.** RIBAS&RODRIGUEZ. Abogados Asociados.
[16] http://www.onnet.es/06039004.htm
[17] http://www.onnet.es/01005013.htm

2. El usuario no puede apreciar directamente la calidad de los productos, por lo que debe tomar como referencia las fotografías y las explicaciones técnicas introducidas en el web.
3. El aspecto estético, la comodidad del usuario, la capacidad de sorpresa que ofrezca la disposición de los contenidos, la accesibilidad de los menús, entre otros, son los elementos que diferenciarán un web con éxito de los demás.

Este esfuerzo invertido en el diseño estético y funcional del web debe ser protegido jurídicamente no sólo porque constituye una creación intelectual, sino también porque representa una estrategia comercial de la empresa que puede ser copiada o imitada por la competencia.

El contenido puede estar formado por obras independientes, que gozan de protección jurídica como creaciones intelectuales, pero también puede contener información o datos que no pueden ser considerados como obras protegidas, pero que al estar dispuestas y ordenadas de una manera singular, constituyen una creación intelectual reconocida en el artículo 12 de la Ley de Propiedad Intelectual.

- Obras incluidas habitualmente en un *web*

Las empresas que introducen y mantienen un *web site* en Internet son a la vez proveedores y consumidores de la llamada industria de contenidos, puesto que generan información, y la enlazan con información preexistente, que se halla en su servidor o en otros webs, al mismo tiempo que utilizan la información elaborada por otros autores.

Un web es por lo tanto, una obra compuesta formada por trabajos de nueva creación, obras preexistentes y unos menús de búsqueda, navegación y clasificación de la información. Todo ello va enlazado y sistematizado según el criterio del editor o autor de la obra principal.

Entre las obras que acostumbran a formar parte de un web figuran:

1. Vídeo
Contenido: Obras cinematográficas, reportajes científicos, documentos audiovisuales, etcéteraétera.
Formatos: AVI, MOV, MPEG, etcétera.

2. Fotografías:
Contenido: Personas, productos, animales, monumentos, situaciones, objetos, paisajes, fotografías de otras creaciones intelectuales, etcétera.
Formatos: GIF, JPEG, etcétera.

3. Texto:
Contenido: Definiciones, descripciones, obras literarias, obras científicas, artículos de prensa, poesía, etcétera.
Formatos: HTML, TXT, DOC, PDF, etcétera.

4. Animaciones:
Contenido: Descripciones animadas, funcionamiento de aparatos, esquemas animados, mapas animados, etcétera.
Formatos: GIF ANIMADOS, JAVA, ACTIVE X, MMM, ANI, etcétera.

5. Sonido:
Contenido: Música, voz, efectos especiales, etcétera.
Formatos: WAVE, REAL AUDIO, MIDI, etcétera.

6. Gráficos y dibujos:
Contenido: Esquemas, mapas, diagramas, gráficos estadísticos, etcétera.
Formatos: GIF, JPG, etcétera.

3.1 Formas de obtención de las obras

Las diversas formas de obtención de las obras desde una perspectiva jurídica son las que siguen:

a. Licencia del titular de una obra preexistente:

La licencia de una obra que va a ser introducida en un web debe otorgarse por escrito y contener una descripción de las actividades autorizadas, en la que se incluyan expresamente:

- La comunicación pública a través de redes de telecomunicación (Internet)
- La transmisión telemática o por cualquier otro medio

- El almacenamiento en un centro servidor
- La posibilidad de efectuar un *download* por parte de terceros

La negociación y formalización de la licencia puede tener lugar directamente con el titular de los derechos o a través de una entidad de gestión.

En cualquier caso, los editores de webs intentan crear sus propios fondos documentales de imágenes, sonidos, animaciones, etcétera., debido al elevado coste que supondría el pago de royalties por todas ellas. Debe tenerse en cuenta que un web puede contener decenas de fotografías escaneadas, textos, diseños, etcétera. y que cada vez que un usuario los visualiza en la pantalla de su ordenador, se produce una reproducción temporal de la obra, que puede llegar a ser definitiva si la graba en el disco duro de su ordenador.

b. Obra de nueva creación

Los medios empleados habitualmente para crear nuevas obras son los siguientes:

- *Obra individual*: los derechos corresponden al autor.
- *Obra colectiva*: los derechos corresponden a la persona física o jurídica que ha tenido la iniciativa de crear la obra, ha coordinado el proyecto y ha publicado la obra bajo su nombre.
- *Obra creada por encargo*: los derechos corresponden a la persona que se designe en el contrato y en caso de silencio, al autor.
- *Obra asalariada*: salvo pacto en contrario, los derechos de explotación pertenecen a la empresa.
- *Obra en colaboración*: salvo pacto en contrario, los derechos pertenecen a los partícipes por igual.

En cualquier caso, debemos repetir la importancia de especificar el ámbito de la cesión de los derechos. Un ejemplo de las consecuencias de no prever la existencia de nuevos soportes de información y nuevas formas de edición, lo constituye el conflicto surgido en 1993 entre el New York Times y un grupo de periodistas *freelance*. Éstos interpusieron una demanda contra el periódico por haber publicado sus artículos en formato CD Rom. Los demandantes entendían que el contrato de arrendamiento de servicios sólo autorizaba al New York Times a publicar los artículos de dichos periodistas en formato papel.

c. Dominio público

Existen numerosos ficheros de imágenes, gráficos, sonido etcétera. que han sido cedidos al dominio público. Estos ficheros pueden obtenerse fácilmente a través de Internet y de BBS.

d. Recopilaciones

Son también obras protegidas las colecciones de obras ajenas y las de otros elementos o datos que por la selección o disposición de las materias constituyan creaciones intelectuales, sin perjuicio, en su caso, de los autores de las obras originales. (Artículo 12 LPI).

3.2 Dispersión de obras, derechos y titulares

El problema de recopilar obras ajenas para integrarlas en un web no es sólo el coste total de las licencias que hay que pagar por las actividades de reproducción y distribución.

A ello se une el hecho de que las obras no pertenecen a un solo género, sino que pueden ser de tipo literario, artístico, audiovisual, etcétera.

Ello significa que el editor de un web deberá seleccionar y determinar las obras que le interesan, localizar a sus autores y negociar el contrato de cesión de derechos. Pero esta tarea se ve dificultada por el hecho de que las obras se hallan dispersas y los derechos no están administrados por una sola entidad de gestión.

En Estados Unidos hay una corriente que aboga por la creación de una cámara de compensación o *clearinghouse* en Internet, en la que se hallen clasificadas por categorías todas las obras disponibles. De esta manera, el propio titular o la entidad de gestión correspondiente, introduciría la obra en la base de datos, o al menos una descripción de la misma y el coste de la licencia de reproducción. Los interesados accederían a la base de datos, visualizarían las obras, elegirían y tramitarían *on line* el pago y la concesión de la licencia. La obra podría ser transmitida en ese momento al ordenador del interesado para su posterior integración en un web o en un proyecto multimedia.

- Diseño gráfico

Si el diseño gráfico del web es original, puede llegar a ser una obra artística o gráfica independiente, protegida por el derecho de autor e incluso por la propiedad industrial como dibujo industrial.

El ancho de banda actual de la red en España, la inexistencia hasta hace poco de un nodo neutro y la velocidad media de los módems de los usuarios, ha provocado cierta lentitud en la visualización de imágenes de gran volumen. Ello ha exigido un mayor esfuerzo en la optimización e indexación de las paletas de colores, con el fin de disminuir el tamaño de las imágenes. De hecho, los formatos de compresión utilizados en Internet, GIF y JPEG, han permitido hasta ahora encontrar cierto equilibrio entre la calidad y el tamaño de las imágenes.

No obstante, es evidente que cuanto más aumenta la comprensión de los ficheros gráficos, más disminuye la calidad de las imágenes y ello influye también en la fidelidad de la oferta en cuanto a su representación gráfica.

En la venta a distancia, la imagen del producto es decisiva. La única referencia que el usuario puede tener del producto que va a adquirir está configurada por las fotografías, dibujos o esquemas que puede visualizar en la página web. No es de extrañar que los autores de dichos gráficos exijan una mayor protección de sus obras en la red, ya que al esfuerzo creativo y artístico habitual, se une en este caso una habilidad técnica para conseguir la mayor calidad de visualización con el menor espacio.

Los elementos estéticos que acostumbran a adornar una página web son los siguientes:

- Texturas y colores de fondo (*backgrounds*)
- Botones de navegación, flechas y demás indicadores.
- Iconos estáticos y animados.
- Fotografías.
- Dibujos, *cliparts*, gráficos, etcétera.

Todos ellos, de manera individual o formando un conjunto estético homogéneo, junto con los demás elementos de la página web, serán objeto de protección como obras de propiedad intelectual, de acuerdo con lo

establecido en la ley española y en los convenios internacionales sobre la materia.

- Código fuente:

El código fuente del web también se halla protegido por la propiedad intelectual y puede estar constituido por:

a) Lenguaje HTML
b) *Applets* Java o Java Script (Animación)
c) Código residente en el servidor que gestiona los pedidos (CGI)
d) Código Active X

El código fuente está escrito en un lenguaje de alto nivel comprensible por el ser humano pero no por el ordenador, mientras que el código objeto está expresado en un lenguaje que puede ser comprendido por el ordenador pero no por el ser humano, ya que es el resultado de la compilación del código objeto.

En el caso de los programas de ordenador, es habitual comercializar sólo el código objeto, de manera que el usuario no accede al código fuente del programa estándar sino solamente a la versión del programa capaz de funcionar en el ordenador pero inhábil para ser modificado o adaptado a las necesidades del usuario.

En Internet las páginas web se hallan escritas en lenguaje HTML, que constituye el sistema universal utilizado por los diseñadores de webs, y que es interpretado por los *browsers* o navegadores.

Una página web es una recopilación de texto, imágenes, gráficos y enlaces hipertextuales configurados mediante una serie de instrucciones denominadas *tags* o etiquetas, que se parecen a los antiguos comandos de los primeros procesadores de textos.

Pese a la sencillez de estas instrucciones, que se limitan a dar formato al texto, a los párrafos, y a la disposición de las imágenes entre el texto, el esfuerzo creativo aumenta cuando estas instrucciones son utilizadas para crear tablas, tabulaciones, *frames* o ventanas, y demás elementos que enriquecen y aumentan el nivel estético y de comprensión de la información contenida en un web.

Por ello, debemos concluir que el código fuente de una página web en HTML, debe encontrar alojamiento en la definición de programa de ordenador que ofrece el Texto Refundido de la Ley de Propiedad Intelectual, gozando de protección plena a efectos de los derechos de autor.

Por otra parte, el hecho de que el código fuente de las páginas web tenga un formato de simple texto en código ASCII, hace que pueda ser editado y visualizado por cualquier editor o procesador de textos. De esta manera, cualquier usuario de Internet puede visualizar sin ninguna traba el código fuente de un web, y ello está produciendo una constante labor de imitación entre los diferentes autores o diseñadores de páginas web.

A diferencia de este sistema, las páginas web también pueden incorporar *applets* de Java, y programas en Active X, que salvo el caso del Java Script, van en código objeto, siendo más difícil su aprovechamiento por otros diseñadores, salvo en el caso de que sean de propósito general.

- Derechos de terceros: imágenes, gráficos, citas, links, marcas, etcétera.

- Marcas

Si se hace referencia a marcas que son propiedad de terceros, es importante mencionarlo, bien al lado de la marca o al final del documento o página.

- Imágenes y gráficos

En algunos casos, puede resultar rentable utilizar gráficos, imágenes o cualquier otro tipo de obras que pertenecen a terceros. Es importante comprobar si el autor de dichas obras ha decidido cederlas al dominio público o, si, por el contrario, ha reservado sus derechos. Como hemos dicho en capítulos anteriores, a pesar de que una obra haya sido localizada en Internet, la ley presume que los derechos no han sido objeto de renuncia y que por lo tanto se precisa autorización expresa para llevar a cabo actividades como la reproducción, adaptación, distribución ó comunicación pública de la obra.

Por ello, la primera labor a realizar consiste en la comprobación de que la obra que se desea incorporar en el web es de dominio público o se dispone de derechos que permiten la actividad de reproducción y comunicación pública.

- **Derecho de cita**

El artículo 32 del TRLPI establece la posibilidad de que se reproduzcan fragmentos reducidos de una obra a modo de cita. Los requisitos para ejercitar el derecho de cita, son los siguientes:

- La cita debe limitarse a fragmentos de la obra
- La obra citada debe haber sido divulgada con anterioridad
- La finalidad de la cita debe ser docente o de investigación
- Debe mencionarse el nombre
- Debe mencionarse el autor de la obra citada

De acuerdo con el artículo 32 del TRLPI, "*es lícita la inclusión en una obra propia de fragmentos de otras ajenas de naturaleza escrita, sonora o audiovisual, así como la de obras aisladas de carácter plástico, fotográfico figurativo o análogo, siempre que se trate de obras ya divulgadas y su inclusión se realice a título de cita o para su análisis, comentario o juicio crítico. Tal utilización sólo podrá realizarse con fines docentes o de investigación, en la medida justificada por el fin de esa incorporación e indicando la fuente y el nombre del autor de la obra utilizada. Las recopilaciones periódicas efectuadas en forma de reseñas o revistas de prensa tendrán la consideración de citas.*"

- Links

En los casos en que se introducen enlaces hipertextuales con webs de terceros, no es obligatorio seguir los requisitos del derecho de cita, ya que, aunque se está enviando al lector a consultar una obra ajena, no se reproduce parte de esa obra en el web propio. Además, en el web de destino el usuario encontrará la completa identificación del autor.

No obstante, debe entenderse que el uso de links que remiten a otros webs no puede llevarse al extremo de utilizarlos como menú remoto de una obra. Ello se produciría cuando se incluyese en una página el índice de contenidos de otro web, de manera que el usuario llegase a una confusión sobre la autoría de la obra al comprobar que cada enlace hipertextual remite a una sección de texto en la que no se identifica al autor y globalmente el texto de referencia aparece como un contenido del web inicial

3.3 Requisitos de la oferta

- Descripción del producto o servicio: prevención de errores de interpretación del usuario

Es importante que la descripción del producto sea clara, con el fin de evitar dificultades en la interpretación de sus cualidades o características técnicas por parte del usuario.

Los productos o servicios ofrecidos deben quedar ampliamente descritos de forma que no pueda producirse confusión en el momento del pedido. En cualquier caso, puede incluirse la recomendación, en el caso de productos complejos, de que se solicite asesoramiento al servicio de atención al cliente, y que no se adquiera el producto hasta que se hayan despejado todas las dudas sobre su funcionamiento, compatibilidad, adecuación a las necesidades del usuario, etcétera.

Con los mismos fines que el párrafo anterior el Gobierno podrá, reglamentariamente, extender la prohibición prevista en el presente número a bebidas con graduación alcohólica inferior a 20 grados centesimales.

3.4 Formulario de pedido

- Requisitos establecidos en la LORTAD

Cuando un usuario cumplimenta un formulario en papel puede tener ciertas dudas sobre el tratamiento informático posterior de sus datos personales, pero cuando se cumplimenta un formulario a través de Internet, no cabe ninguna duda respecto a su tratamiento automatizado, ya que el usuario tiene la certeza de que él mismo está introduciendo sus datos personales en un sistema informático. Tanto la programación en CGI como la más reciente programación en Java permiten el enlace directo de los formularios de WWW con las bases de datos instaladas en el servidor. De esta manera, puede obtenerse una integración completa entre la recogida de datos que se produce en el entorno gráfico que sirve de *interface* con el usuario y la gestión en tiempo real de dicha información en la base de datos.

Pese a ello, la mayoría de los formularios de recogida de datos que podemos encontrar en Internet, adolecen de una ausencia total de referencias a la

LORTAD en forma de cláusulas de consentimiento por parte del usuario respecto al tratamiento automatizado de los datos personales introducidos, así como de una información sobre la posibilidad de modificar o incluso cancelar los registros referentes a su persona.

Por ello, es recomendable introducir en todos los formularios de Internet las cláusulas que exige la LORTAD, comunicando a la Agencia de Protección de Datos la creación de dichas bases de datos personales.

La firma original del afectado será necesaria en el caso de recogida de datos referentes a la salud. Por ejemplo, la contratación a través de Internet de seguros de vida o enfermedad, la solicitud de ingreso en mutuas médicas, y demás servicios relacionados con la salud, exigirá el posterior envío del documento original en papel, con la firma del usuario.

3.5 Normativa sobre venta a distancia

La venta a través de Internet puede ser interpretada de diferentes modos:

1. *Venta celebrada en el domicilio del suministrador*

Se aplica la Ley General para la Defensa de los Consumidores y Usuarios y el Código Civil.

Es el sistema más ventajoso para el suministrador, ya que no establece otras obligaciones que las propias de un comerciante que vende sus productos a través de una tienda abierta al público.

Tiene el riesgo de que más adelante, cuando se generalice la modalidad del E-comercio, empiecen a formularse denuncias por considerar que se trata de una venta a distancia.

2. *Venta a distancia*

Se aplica la Ley de Ordenación del Comercio Minorista, de 15 de enero de 1996. Algunas Comunidades Autónomas disponen de su propia ley sobre la materia, pero no son aplicables a los medios de difusión que abarquen varias CCAA, como es el caso de Internet.

La empresa suministradora debe solicitar autorización al Ministerio de Turismo y Comercio e inscribirse en el Registro correspondiente. Exige que se conceda un plazo de 7 días al usuario para desistir de la operación y devolver el material adquirido.

Se exceptúan de la posibilidad de devolución todos los bienes que puedan ser copiados o reproducidos con carácter inmediato (como el *software*).

Sobre la calificación de las transacciones de comercio minorista en Internet como ventas a distancia, entendemos que caben perfectamente en la definición que da la Ley:

> *"Se consideran ventas a distancia las celebradas sin la presencia física simultánea del comprador y del vendedor, transmitiéndose la propuesta de contratación del vendedor y la aceptación del comprador por un medio de comunicación a distancia de cualquier naturaleza".*

Podría defenderse la tesis de que la propuesta de contratación del vendedor no se transmite, sino que permanece estática en un servidor a la espera de que los clientes potenciales la consulten, pero en cualquier caso, es evidente que la venta minorista a través de Internet está más cerca de la figura legal de la venta a distancia que de la venta tradicional en una tienda.

3. *Venta celebrada fuera del establecimiento del suministrador*

Se aplica la Ley 26/1991, de 21 de noviembre, sobre contratos celebrados fuera del establecimiento mercantil. Exige que se conceda un plazo de 7 días al usuario para revocar el pedido y devolver el material adquirido, sin necesidad de expresar justa causa. El contrato debe ir acompañado de un documento de revocación.

También exige la firma de un contrato específico firmado por el usuario con "su puño y letra". No es aplicable a las operaciones de cuantía inferior a las 8.000 pesetas.

Conclusiones: aunque lo ideal sería mantener la idea de que una transacción minorista a través de Internet no debería diferenciarse de una venta convencional en un establecimiento abierto al público, debemos advertir que

tanto la Ley española como la propuesta de Directiva comunitaria sobre la materia establecen que se trata de una venta a distancia.

3.6 Normativa sobre facturación telemática[18]

En la Orden del Ministerio de Economía y Hacienda de 22 de marzo de 1996 se dictan las normas de aplicación del sistema de facturación telemática que ya había sido previsto en el artículo 88 de la Ley del Impuesto sobre el Valor Añadido y en el artículo 9 bis del Real Decreto 2402/1985.

La referida Orden define la factura electrónica como un conjunto de registros lógicos, almacenados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos, que documentan las operaciones empresariales o profesionales, con los requisitos exigidos para las facturas convencionales.

Los interesados en promover la implantación de un sistema de intercambio de facturación por medios telemáticos deberán solicitarlo al Departamento de Inspección Financiera y Tributaria de la Agencia Estatal de Administración Tributaria, que resolverá de forma expresa en el plazo de seis meses.

Los empresarios o profesionales que deseen operar como usuarios de un sistema de intercambio de facturación por medios telemáticos deberán solicitarlo al mismo organismo, que resolverá en el plazo de un mes. En este caso, el silencio administrativo se interpretará de forma positiva.

Los usuarios que utilicen el sistema de facturación telemática estarán obligados a conservar en soporte magnético u óptico y en el mismo orden de transmisión o recepción, e íntegramente, los ficheros de facturas transmitidos y recibidos. Asimismo deberán adoptar las medidas de seguridad necesarias para su conservación, y guardar un listado secuencial de las operaciones diarias efectuadas.

De acuerdo con la información facilitada por AECOC, durante los tres meses siguientes a la entrada en vigor de la Orden de 22 de marzo de 1996 sobre facturación telemática, más de 800 empresas solicitaron a la Agencia Tributaria adherirse a este sistema.

---

[18] Javier Ribas http://www.onnet.es/c05.htm

- Resolución de conflictos[19]

Dado que en Internet pueden producirse operaciones comerciales con personas físicas o jurídicas de otros países, será fundamental incorporar una cláusula en la que señale que la legislación aplicable a dicho contrato será la española.

- Ventajas del arbitraje

Las principales ventajas del arbitraje son las que siguen:

a) Rapidez. Frente a la actual saturación de la Administración de Justicia, el arbitraje proporciona una agilidad enorme, pudiendo las partes establecer el plazo máximo dentro del cual el laudo debe ser dictado.

b) Especialización en la materia. Las partes pueden escoger a árbitros que conozcan a fondo, por razón de su profesión o del cargo que ocupan, la materia en la que se ha originado la controversia. Por ejemplo, en caso de divergencias surgidas en la contratación de tecnología, o de servicios informáticos, las pruebas presentadas, pueden ser analizadas directamente por los árbitros, mientras que en la vía judicial, el juez debe confiar en los dictámenes de los peritos.

c) Ausencia de publicidad. El arbitraje permite la solución de las diferencias surgidas entre las partes de forma privada, sin que conozcan su existencia los demás consumidores y usuarios del producto o servicio, los proveedores, las instituciones financieras y el público en general.

d) Eficacia. En caso de incumplimiento, el laudo arbitral firme puede ser objeto de ejecución forzosa, al igual que las sentencias judiciales.

e) Reducción de la sobrecarga de trabajo de los Tribunales. El Comité de Ministros del Consejo de Europa, en su Recomendación 12/1986, con el fin de reducir la sobrecarga de trabajo de los Tribunales, propone que los Gobiernos de los Estados Miembros adopten las disposiciones adecuadas para que en los casos que se presten a ello, el arbitraje pueda constituir una alternativa más accesible y eficaz a la acción judicial.

---

[19] Javier Ribas http://www.onnet.es/c13.htm

- Concepto de arbitraje

Mediante el Arbitraje, las personas naturales o jurídicas pueden someter, previo convenio, a la decisión de uno o varios árbitros, las cuestiones litigiosas, surgidas o que puedan surgir, en materias de su libre disposición conforme a derecho.

- Materias excluidas del arbitraje

No podrán ser objeto de arbitraje:

a) Las cuestiones sobre las que haya recaído resolución judicial firme y definitiva, salvo los aspectos derivados de su ejecución.
b) Las materias inseparablemente unidas a otras sobre las que las partes no tengan poder de disposición.
c) Las cuestiones en que, con arreglo a las Leyes, deba intervenir el Ministerio Fiscal en representación y defensa de quienes, por carecer de capacidad de obrar o de representación legal, no pueden actuar por sí mismos.
d) Las materias sometidas a arbitraje laboral.

- Tipos de arbitraje

La elección del tipo de arbitraje corresponderá a las partes, y en caso de que no hayan manifestado su voluntad en este aspecto, el arbitraje será del primero de los dos tipos que se indican:

a) Arbitraje de equidad. Los árbitros deciden la cuestión litigiosa según su saber y entender. En este caso puede ser árbitro cualquier persona natural que se halle, desde su aceptación, en el pleno ejercicio de sus derechos civiles.

b) Arbitraje jurídico. Los árbitros deciden la cuestión litigiosa con sujeción a derecho. En este caso los árbitros habrán de ser abogados en ejercicio.

- El convenio arbitral

a) Concepto. Es el acuerdo mediante el cual las partes expresan su voluntad inequívoca de someter la solución de todas las cuestiones litigiosas o de

algunas de estas cuestiones, surgidas o que puedan surgir de relaciones jurídicas determinadas, sean o no contractuales, a la decisión de uno o más árbitros, así como expresar la obligación de cumplir tal decisión.

b) Modelo de cláusula arbitral. *"Para cualquier divergencia surgida del presente contrato, ambas partes se someten expresamente, y con renuncia a su fuero propio, a la decisión del asunto o litigio planteado, mediante el arbitraje institucional de ARBITEC, Asociación Española de Arbitraje Tecnológico, a la cual encomiendan la administración del arbitraje y la designación de los árbitros. El arbitraje se realizará conforme al procedimiento establecido en el Reglamento Arbitral de ARBITEC y en la Ley de Arbitraje, de 5 de diciembre de 1988. El laudo arbitral deberá dictarse durante los noventa días siguientes a la aceptación del cargo por parte de los árbitros designados, obligándose ambas partes a aceptar y cumplir la decisión contenida en él.*

Para el caso de que el arbitraje no llegara a realizarse por mutuo acuerdo o fuese declarado nulo, ambas partes se someten a los Juzgados y Tribunales de la Ciudad de ..... con renuncia a su propio fuero, si éste fuese otro".

3.7 Prueba de la aceptación: entidades certificadoras

La emisión de certificados y la creación de claves privadas para firmas digitales acostumbra a depender de una pluralidad de entidades que están jerarquizadas de una manera que las de nivel inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Finalmente, en la cúspide de la pirámide suele hallarse una autoridad certificadora, que puede pertenecer al Estado, y que en el proyecto alemán coincide con el organismo que controla las telecomunicaciones.

Las autoridades certificadoras tienen la función de emitir, suspender y revocar certificados, así como dar a conocer la situación actual de un certificado y crear claves privadas. Los certificados indican la autoridad certificadora que lo ha emitido, identifican al firmante del mensaje o transacción, contienen la clave pública del firmante, y contienen a su vez la firma digital de la autoridad certificadora que lo ha emitido.

De esta manera, las partes que intervienen en una transacción aportan como credencial los certificados de su correspondiente entidad certificadora. Por

ejemplo, la entidad certificadora A da fe de la identidad del usuario A1 cuando éste adquiere un bien al usuario B1, que es a su vez identificado por la entidad certificadora B.

Para llegar a ser una entidad certificadora deberá mediar una solicitud a una autoridad certificadora de nivel superior, que podrá denegar la licencia si el solicitante no ofrece la fiabilidad o los conocimientos necesarios, ni cumple los requisitos establecidos en la ley.

3.8 La firma digital: primeras experiencias legislativas

Existe una opinión generalizada de que, si ya es complicado, en la vida presencial, demostrar la existencia de una deuda que no se ha formalizado en un título ejecutivo, la dificultad probatoria será mayor en una plataforma contractual en la que el consentimiento se transmite en forma de bits.

Es evidente que los que basan sus compromisos comerciales en el célebre apretón de manos, tendrán que recurrir a la realidad virtual para poder sellar así sus acuerdos a través de Internet. Pero los que tienen por norma documentar sus transacciones con contratos escritos podrán comprobar en poco tiempo, que la firma digital aporta una eficacia probatoria igual, o incluso superior a la que aporta la firma original en papel.

La firma digital, según Javier Ribas, que ha resumido los esquemas planteados[20], es el instrumento que permitirá, entre otras cosas, determinar de forma fiable si las partes que intervienen en una transacción son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente.

La primera ley que ha regulado los aspectos jurídicos de la firma digital como instrumento probatorio se aprobó el año pasado en Utah. Posteriormente surgieron proyectos legislativos en Georgia, California y Washington. En Europa, el primer país que ha elaborado una Ley sobre la materia ha sido Alemania.

Es evidente que la eficacia de estas leyes radica en su uniformidad, ya que si su contenido difiere en cada estado, será difícil su aplicación a un entorno

[20] Javier Ribas http://www.onnet.es/06041008.htm

global como Internet. Por ello, el esfuerzo a realizar a partir de ahora deberá centrarse en la consecución de un modelo supraestatal, que pueda ser implantado de manera uniforme en las leyes nacionales. Tal tarea puede encomendarse a organismos internacionales como UNCITRAL, que ya dispone de experiencia en iniciativas similares en materia de EDI.

- Definiciones establecidas en las leyes sobre firma digital

Firma digital: Transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posea el mensaje inicial y la clave pública del firmante, pueda determinar de forma fiable si dicha transformación se hizo utilizando la clave privada correspondiente a la clave pública del firmante, y si el mensaje ha sido alterado desde el momento en que se hizo la transformación (Utah). Es un sello integrado en datos digitales, creado con una clave privada, que permite identificar al propietario de la firma y comprobar que los datos no han sido falsificados (Alemania)

Certificado: Documento digital que identifica a la autoridad certificadora que lo ha emitido y al firmante del mensaje o transacción, contiene la clave pública del firmante, y contiene a su vez la firma digital de la autoridad certificadora que lo ha emitido.

Autoridad certificadora: Entidad que da testimonio de la pertenencia o atribución de una determinada firma digital a un usuario o a otro certificador de nivel jerárquico inferior.

- Contenido de la norma española

El Consejo de Ministros español aprobó el 17 de septiembre de 1999 el Real Decreto Ley sobre Firma Electrónica[21], en el que se reconoce la eficacia jurídica de la misma y las condiciones para prestar servicios de certificación en España. Antes, el Ministerio de Fomento había elaborado un proyecto de ley para regular la firma electrónica, que había pasado ya todos los trámites pertinentes, pero la proximidad de las elecciones generales impedía que el Parlamento tuviera tiempo para discutirla. Había urgencia para regular la figura de los certificadores de firmas electrónicas nacionales antes de que se impusieran multinacionales. España se anticipó así a la mayoría de los países de la Unión Europea, pues sólo Alemania tenía en esa fecha una ley.

[21] http://noticias.juridicas.com/lec/Admin/rdl14-1999.html

Esta firma electrónica española no sólo pretende favorecer las transacciones electrónicas de los ciudadanos, sino facilitará sus trámites con la Administración, con la posibilidad de solicitar el DNI, certificados de nacimiento, certificados de penales, presentar recursos administrativos, etcétera a través de Internet. Para ello, la firma electrónica avanzada recogerá un conjunto de datos que permitirán la identificación del usuario y tendrá el mismo valor jurídico que la firma manuscrita, siendo admisible como prueba en un juicio.

- Certificación

Para que tenga la máxima eficacia jurídica, la firma electrónica tendrá que ser avalada por un "certificado reconocido", que permite verificar la identidad del usuario y que será expedido por un prestador de servicios de certificación. Cualquier persona física o jurídica, pública o privada, puede convertirse en prestador de servicios de certificación sin necesidad de autorización previa. Sin embargo, para poder expedir "certificados reconocidos", que den la máxima eficacia a la firma electrónica, los prestadores tendrán que solicitar su inscripción en el Registro de Prestadores de Servicios de Certificación, creado para este fin en el Ministerio de Justicia.

La Fábrica Nacional de Moneda y Timbre ya lograba con esta Ley el reconocimiento para erigirse como entidad de certificación, estatus que también habían solicitado VISA, Telefónica, la Cámara de Comercio y los Corredores de Comercio..

- Responsabilidad ante el usuario

Entre las obligaciones, garantías y condiciones exigibles a los prestadores de servicios de certificación establecidos en España, destaca la necesidad de disponer de recursos económicos suficientes para afrontar "el riesgo de la responsabilidad por daños y perjuicios", tanto a los usuarios de sus servicios como a terceros afectados por éstos. La garantía mínima habrá de cubrir el cuatro por ciento de la suma de los importes de las transacciones en que puedan emplearse el conjunto de los certificados que emita el prestador de este servicio.

Asimismo, el anteproyecto recogía una clasificación de las infracciones y sus respectivas sanciones. Una infracción muy grave puede dar lugar a multas de hasta 100 millones de pesetas y en caso de que se repitan pueden dar lugar a que se le prohibirá continuar con su actividad. Una infracción grave se multará

con multas de hasta 50 millones de pesetas y las leves con sanciones de hasta 5 millones de pesetas.

Para urgir al Gobierno esta medida, considerada un gran empuje para la consolidación del E-comercio en España, el PP expusieron en el Congreso informes realizados por empresas de consultoría y servicios informáticos como Cap Gemini, Sun o Netscape, en los cuales se expone que el 72% de las empresas españolas disponen de página en la red, pero solo el se ha recorrido "el 32% del camino hacia el comercio electrónico". La propuesta del PP mostraba también un estudio de VISA, según el cual más del 90,5% de los usuarios que han realizado compras a través de Internet notan la ausencia de más sitios preparados para este tipo de transacciones. Pero el PSOE se opuso a la convalidación del Decreto Ley, aunque a los votos del PP se sumaron los de CiU, PNV y Coalición Canaria.

Unos días después, el 27 de octubre de 1999, el Parlamento Europeo aprobó la directiva (ley comunitaria) que establece un marco común para la firma electrónica, consensuado por los ministros de Telecomunicaciones de la Unión Europea en abril anterior. Pero tanto en este como en el caso anterior se siguen las pautas de la ley alemana.

3.9 Ley alemana sobre firma digital

- La ley alemana está divida en dos partes, un texto principal y un reglamento que desarrolla aspectos concretos de la ley, como el procedimiento de concesión, transferencia y revocación de una licencia de entidad certificadora, así como los deberes de los certificadores, el periodo de validez de los certificados, los métodos de control de los mismos, los requisitos de los componentes técnicos y el procedimiento de examen de los mismos.

- Un certificado deberá contener obligatoriamente: el nombre del propietario de la firma digital, que deberá estar identificado de forma inequívoca, la clave pública atribuida, el nombre de los algoritmos utilizados, el número del certificado, la fecha de inicio y final de la validez del certificado, el nombre de la entidad certificadora, información sobre las limitaciones que se hayan establecido para su utilización e información relativa a certificados asociados.

- Una entidad certificadora deberá bloquear un certificado en el momento en que compruebe que está basado en información falsa, cuando la entidad cese en su actividad sin que otra entidad la suceda, o cuando reciba la orden de bloqueo de la autoridad certificadora de nivel superior.

- La entidad certificadora podrá recabar datos personales del afectado, pero sólo directamente del mismo, y con la única finalidad de emitir un certificado. Si el propietario de la firma digital utiliza un seudónimo, la entidad certificadora sólo podrá transmitir datos relativos a su identidad a requerimiento de la autoridad judicial y en los casos establecidos por la ley.

- También establece un sistema de auditoría que permitirá a la autoridad certificadora inspeccionar los equipos de la entidad, con el fin de comprobar el cumplimiento de los requisitos técnicos y el plan de seguridad exigidos para el desarrollo de dicha actividad. Dichos requisitos se refieren a los procedimientos de creación, almacenamiento y comprobación de firmas digitales, que deberán permitir la detección inmediata de cualquier uso no autorizado de una firma digital y la alteración del contenido de los datos, mensajes o transacciones que se hayan efectuado con dicha firma.

3.10 Prevención de responsabilidad civil[22]

Antes de examinar la prevención de delitos en general, veremos la responsabilidad civil por links. Aunque es verdaderamente difícil que un usuario presente una demanda por los daños sufridos al seguir un enlace hipertextual introducido en un web, debe tenerse en cuenta que existen precedentes sobre la materia en Estados Unidos. Los casos aparecidos en este país se basan en una ausencia de advertencias sobre el riesgo que corre el usuario siguiendo la recomendación del propietario del web de visitar otros destinos en Internet, sugeridos a través de la fórmula del link.

Es decir, el usuario reclamante entiende que la introducción de un link en una página web equivale a una invitación, recomendación o sugerencia para el visitante, que le induce a entrar en otro servidor y visualizar una información

[22] Javier Ribas http://www.onnet.es/07.htm

que puede herir su sensibilidad, provocarle un daño o incluso convertirlo en víctima de un delito.

El camino seguido para una eventual reclamación en este sentido, sería el del artículo 1902 del Código Civil, siendo aplicable el régimen de responsabilidad civil extracontractual descrito en otros apartados de este informe.

- Revisión de la cobertura del seguro de RC, correspondiente a la actividad de la empresa.

La actividad principal de una compañía acostumbra a tener cobertura en materia de responsabilidad civil a través de una póliza de seguros que, probablemente, no ha previsto las modernas modalidades de E-comercio que la empresa puede utilizar para distribuir sus productos o prestar sus servicios.

Ello obliga a revisar el texto de dicha póliza con el fin de comprobar si la cobertura dispensada por la compañía de seguros es la adecuada y si realmente se ha previsto la posibilidad de compensar las pérdidas sufridas por una operación realizada a través de medios telemáticos.

- Prevención de delitos[23]

Sobre las pautas de Javier Ribas, presentamos el siguiente resumen de prevención de delitos informáticos que afectan al E-comercio:

a) Infracción de los derechos de autor

Respecto a los delitos contra la propiedad intelectual, no se introducen cambios significativos. Con la proliferación de las 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, etcétera. que incorporan las webs y las bases de datos accesibles a través de Internet.

El art. 270 del nuevo CP establece la pena de prisión de 6 meses a 2 años e incluye en la categoría de los delitos contra la propiedad intelectual la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la

[23] Javier Ribas http://www.onnet.es/c10.htm

neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

b) 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.

El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina.

El art. 248 y ss. establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

c) Daños informáticos.

La antigua redacción del código penal no tuvo en cuenta el enorme valor de la información como bien jurídico a tutelar. Por ello, el delito de daños debía referirse a bienes materiales, quedando excluida cualquier modalidad de destrucción de bienes materiales.

El apartado 2 de artículo 264 del nuevo Código Penal integra el concepto de información como bien jurídico protegido por el hecho penal, de manera que la acción de destrucción o alteración de datos, programas o cualquier otro tipo de información digital albergada en un sistema informático, será considerada un delito de daños.

El legislador ha sido consciente de la tremenda importancia de la información en su formato digital. La contabilidad, las bases de datos, la facturación de una empresa, su listado de clientes, el estado de cuentas de una entidad financiera... todo ello configura un nuevo activo patrimonial que debe ser protegido por la Ley.

Evidentemente, la protección ante este tipo de delitos, implica diversas medidas de seguridad informática, entre las quede cabe destacar, la prevención contra virus informáticos, tanto de tipo puramente informático, es decir, asociados a un fichero ejecutable o a un soporte magnético, como los

que tienen su origen en una transmisión telemática, entre los que se pueden citar los macros de procesadores de texto, los *applets* de Java y los programas Active X generados con la finalidad de obtener resultados negativos para un sistema informático.

d) Interceptación de telecomunicaciones

En el apartado correspondiente a los delitos contra la intimidad se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia.

El artículo 197 extiende el ámbito de aplicación de este delito a las siguientes conductas:

- apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.
- interceptación de las telecomunicaciones, en las mismas condiciones
- utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos.

Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad.

La pena que se establece es de prisión, de uno a cuatro años y multa de doce a veinticuatro meses (Con el nuevo concepto de días-multa, un día equivale a un mínimo de 200 pesetas y un máximo de 50.000 pesetas).

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 acceder y descubrir sus secretos.

e) Uso no autorizado de terminales

El artículo 256 castiga con multa de tres a doce meses el uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas. En caso de perjuicios inferiores la infracción constituiría una falta.

f) Revelación de secretos

El art. 278 establece una pena de 2 a 4 años para el que, con el fin de descubrir un secreto, se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo.

Si los secretos descubiertos se revelasen, difundieren o cedieren a terceros, la pena llegará a los 5 años de prisión.

g) Falsedades documentales

Los artículos 390 y siguientes castigan con la pena de prisión de hasta seis años las alteraciones, simulaciones y demás falsedades cometidas en documentos públicos.

Los artículos 395 y 396 se refieren a las falsedades cometidas en documentos privados, pudiendo alcanzar la pena de prisión hasta dos años. También se castiga la utilización de un documento falso para perjudicar a un tercero.

El artículo 26 define como documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Entendemos que quedaría incluido en el concepto documento los mensajes estáticos, compuestos por información almacenada en un sistema informático después de haber sido remitida o recibida a través de la red, pero surgen dudas sobre la naturaleza documental del mensaje que está circulando.

Finalmente, el artículo 400 introduce el delito consistente en la fabricación o tenencia de útiles, materiales, instrumentos, programas de ordenador o aparatos destinados específicamente a la comisión de estos delitos, que se castigará con las penas señaladas para los autores. Entrarían dentro de este tipo los programas copiadores, las utilidades empleadas por los hackers y cualquier otro dispositivo similar.

h) Publicidad engañosa en Internet

El uso del www con fines publicitarios hace que se trasladen a Internet los eslóganes y mensajes publicitarios que se difunden en la vida real. Ello hace

posible la aplicación de la ley a las infracciones que se produzcan en el ciberespacio y que puedan causar un perjuicio grave a los consumidores.

En este sentido el art. 282 castiga con la pena de prisión de seis meses a un año a los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos.

4 La seguridad en Internet: el Protocolo SET

Una de las principales preocupaciones que suscita el E-comercio es la seguridad, fundamentalmente en lo que se refiere a la forma de pago. Vamos a explicar cómo y por qué se pueden realizar compras de bienes y servicios a través de redes abiertas, mediante tarjeta de crédito, bajo las máximas garantías de seguridad para todas las partes.

El método desarrollado para garantizar este tipo de operaciones es el protocolo SET (*Secure Electronic Transaction*), explicado entre otros por la Agencia Española de Certificación Electrónica[24], y el certificado digital

4.1 El pago de bienes y servicios en Internet

En el E-comercio se aplica el proceso de compra / venta de productos y servicios a través de redes de información. En este proceso se pueden distinguir las siguientes etapas:

1. El consumidor accede a la Red a través de su ordenador personal conectado a un módem. Mediante el uso de su navegador, va introduciéndose en diferentes sitios web donde los comercios exponen sus productos o servicios.

2. El consumidor encuentra un producto / servicio que desea comprar, iniciando el proceso de compra del mismo el cual vendrá determinado por la operativa que haya establecido el "comercio virtual" así como por el sistema de pago que el cliente elija. En este sentido existen dos alternativas básicas:

    2.1 Realizar el pedido de forma electrónica, rellenando el formulario que presenta el comercio. El consumidor ha de indicar la modalidad de pago mediante la cual abonará el importe de la compra. En caso de tratarse de tarjeta de crédito, enviará los datos correspondientes junto con el formulario de pedido. En el resto de los casos(cheque, efectivo, contra reembolso, etcétera), la realización del pago deberá llevarse a cabo por los métodos tradicionales fuera de la Red.

[24] http://www.ace.es/faq_b.htm

2.2 Realizar el pedido por los medios tradicionales (teléfono, fax, etcétera) de manera que el resto de la operación se realiza fuera de la Red.

3. El comercio recibe la petición de pedido y procede a la entrega del producto / servicio que el cliente haya solicitado.

4. El comercio realiza la gestión del cobro al cliente en función del sistema de pago que éste haya seleccionado.

Desde sus inicios, el E-comercio, ha sufrido una evolución progresiva encaminada a facilitar la realización de todo el proceso de compra/venta a través de la propia Red mediante transacciones electrónicas. Obviamente, la entrega física del producto adquirido es un aspecto que podría ser o no incorporado dependiendo de la naturaleza del mismo.

El primer paso consistió en la propia presentación y publicitación de los productos y servicios en la Red, de manera que el cliente potencial pudiera realizar la selección de los mismos mediante la búsqueda y acceso al *Web site* del comercio o empresa suministradora.

Inmediatamente se incorpora la posibilidad de realizar el pedido a través de un formulario electrónico presentado por el comercio / empresa a petición del cliente.

Sin embargo, la gestión del pago se tenía que realizar a través de los canales tradicionales como el teléfono, fax o contra-reembolso dado que enviar datos como el número de tarjeta de crédito del cliente planteaba problemas de confidencialidad e integridad (riesgo de acceso y/o modificación de dicha información por terceros) y de autenticidad (incertidumbre tanto del cliente como del comercio sobre la identidad de cada uno y la validez de la información intercambiada: garantía de productos adquiridos al comercio y autenticidad del mismo / validez de los datos de pago comunicados por el cliente).

Así surge el protocolo SSL que, incorporado en los servidores de los comercios, permite encriptar la información sobre el cliente (garantizando la confidencialidad de la misma), autentificar el servidor (incrementando la confiabilidad del cliente), asegurando la integridad de los datos durante la transmisión entre las dos partes. No obstante, el comercio debía realizar la

gestión del cobro a través de los canales tradicionales. En estos momentos, el desarrollo del E-comercio se encuentra en un momento crítico debido a que:

- El consumidor demanda servicios de acceso seguro para realizar sus operaciones de E-comercio.

- Los comercios necesitan métodos simples y de bajo coste para lanzarse a este nuevo entorno de mercado.

- Las entidades financieras requieren un sistema estándar que permita la gestión de la operación económica derivada de la compra a través de la Red, bajo las máximas garantías de seguridad.

- Los operadores de tarjetas de crédito deben ser capaces de implementar transacciones de E-comercio sin que ello suponga un gran impacto en sus actuales infraestructuras.

- Los proveedores de hardware y *software* necesitan incorporar los elementos necesarios en sus sistemas y poder ofrecer sus productos de E-comercio que incorporen el elemento seguridad, a precios competitivos.

El desarrollo del Protocolo SET llevado a cabo por Visa y Mastercard principalmente, da respuesta a todas estas necesidades planteadas y facilita la realización del pago/cobro mediante tarjeta de crédito de forma electrónica con todas las garantías de seguridad.

4.2 La especificación SET

SECURE ELECTRONIC TRANSACTION (SET), en español Transacción electrónica segura, es una especificación diseñada con el propósito de asegurar y autenticar la identidad de los participantes en las compras abonadas con tarjetas de crédito/débito en cualquier tipo de red en línea, incluyendo Internet/InfoVía.

SET ha desarrollada por Visa y MasterCard, con la participación de Microsoft, IBM, Netscape, SAIC, GTE, RSA, Terisa Systems, VeriSign y otras empresas líderes en tecnología.

Los objetivos que cumple SET son:

- Confidencialidad de la información transmitida.
- Autenticación de los titulares y comercios.
- Integridad de la información transmitida.
- No repudio de las operaciones realizadas.
- Interoperabilidad entre las distintas plataformas de hardware y *software* que utilizan los diferentes participantes en las transacciones electrónicas.

Antes de entrar más a fondo en la descripción del protocolo convendría analizar cuáles son las distintas partes que intervienen en una transacción comercial a través de tarjetas de crédito:

- Titular / Cardholder**:**

El titular de una tarjeta de crédito/débito es la persona a nombre de la cual se ha emitido la tarjeta. En este ámbito es el cliente / comprador del producto.

- Emisor:

El emisor es la entidad financiera emisora de la tarjeta de crédito/débito del titular y con el cual éste mantiene una cuenta bancaria.

- Comercio / Merchant:

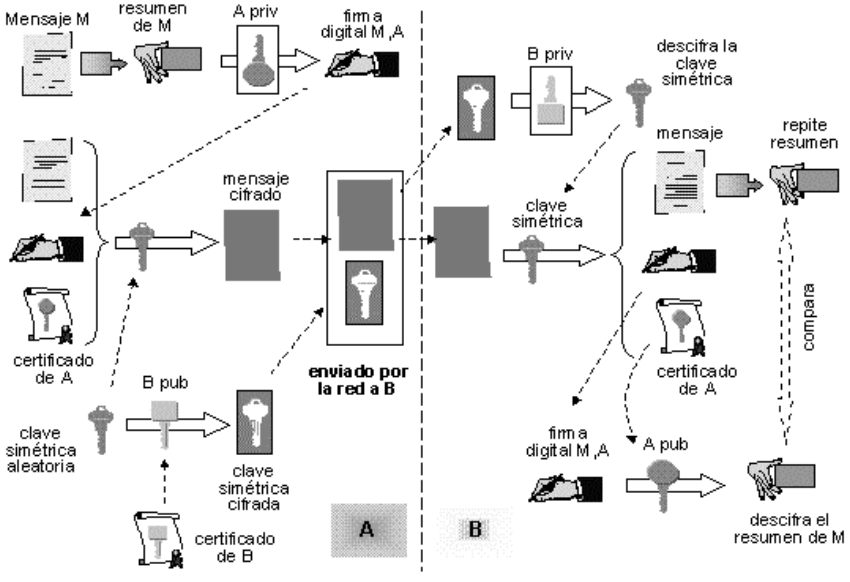
El merchant es el comercio que ofrece productos y servicios en su Web a cambio de un pago. El merchant que acepta pagos a través de tarjeta debe establecer una relación con una entidad financiera (Adquirente), el cual se encarga de gestionar el cobro de las ventas realizadas.

- Adquirente:

El adquirente es una entidad financiera que establece una cuenta bancaria con el comercio y procesa las autorizaciones de pago por tarjeta de crédito y los propios pagos realizados por dicho comercio.

- Pasarela de pagos:

Una pasarela de pagos es el mecanismo mediante el cual se procesan y autorizan las transacciones del merchant. La pasarela puede pertenecer a una entidad financiera (Adquirente) o a un operador de medio de pago, el cual procesa todas las transacciones de un conjunto de entidades. En este escenario, los diferentes medios de pago realizan el cruce e intercambio de las operaciones para las distintas entidades que representan.



Apub, Apriv: claves pública y privada de A; Bpub, Bpriv: claves pública y privada de B

4.3 Características de la especificación SET

Para facilitar y fomentar el uso de tarjetas de crédito/débito en el E-comercio la información debe viajar a través de la Red de forma segura, de modo que los datos que contienen las instrucciones de pago (número de tarjeta o su fecha de caducidad) no puedan ser interceptados.

- Confidencialidad de la Información:

La especificación SET encripta los mensajes de tal forma que la confidencialidad de la información está asegurada.

- Encriptación:

Encriptación es la transformación de la información a un formato ilegible para cualquiera que no posee una clave de desencriptación. Los procesos de encriptación y desencriptación requieren una fórmula matemática denominada algoritmo y unas claves que son utilizadas para resolver dicho algoritmo. Su funcionalidad es la de asegurar la privacidad manteniendo la información oculta de aquellas personas a las que no va destinada, incluidos aquellos que pueden ver los datos encriptados.

En un entorno multi-usuario, la encriptación ayuda a dar seguridad a las comunicaciones en un canal por si mismo inseguro. Por ejemplo, Juan quiere enviar un mensaje a María de tal forma que sólo ella sea capaz de leerlo. Juan encripta el mensaje, denominado *plaintext*, con una clave de encriptación. El mensaje encriptado, denominado *ciphertext*, es enviado a María. María descifra el ciphertext con una clave de desencriptación y lo lee. Alguien puede intentar obtener la clave secreta o recuperar el plaintext sin utilizar la clave secreta. En un entorno seguro, el plaintext no puede ser obtenido del ciphertext sin utilizar la clave de desencriptación.

La criptografía tradicional está basada en que el emisor y el receptor conocen y comparten la misma clave secreta. Este método es conocido como **criptografía de clave simétrica**. El principal problema es conseguir que el emisor y el receptor se pongan de acuerdo sobre la clave y su transporte, desde el punto de origen al punto de destino, sin que nadie tenga conocimiento de ello. En el caso de que estuviesen separados físicamente deberían confiar en un correo, utilizar el teléfono u otro medio de transmisión. Este es el tipo de criptografía utilizado por las entidades financieras para encriptar los PINs (números de identificación personal). La criptografía de clave secreta no es práctica en el ámbito de la especificación SET, ya que un comercio, para realizar transacciones con miles de clientes, necesitaría una clave diferente para cada uno de ellos y que la transmisión se realizase en canales seguros separados.

La **criptografía de clave asimétrica** (conocida también como **criptografía de clave pública**) incorpora un par de claves para cada una de las partes que intervienen en el proceso denominadas clave pública y clave privada.

El par de claves (pública y privada) se generan en el entorno del usuario. La clave pública de cada usuario suele estar almacenada en un directorio, mientras que la clave privada es mantenida como tal y nunca sale del entorno del usuario. La necesidad de compartir información secreta entre el emisor y el receptor es eliminada. Todas las comunicaciones implican sólo a las claves públicas y las claves privadas nunca son transmitidas o compartidas. Todo el mundo puede mandar mensajes confidenciales usando información pública, pero éstos sólo pueden ser descifrados con la clave privada que únicamente está en posesión del receptor. La criptografía de clave pública puede ser utilizada tanto para autentificación (firmas digitales) como para encriptación (confidencialidad).

La especificación SET utiliza criptografía de clave pública ya que permite al comercio generar su par de claves y publicar la clave pública, de tal forma que cualquier posible cliente pueda enviar mensajes seguros al comercio utilizando dicha clave.

- Autentificación de las partes que intervienen en una transacción

Los comercios necesitan verificar que el titular es usuario legítimo de una tarjeta válida. Un mecanismo que sirva para asociar a un titular con un número específico de tarjeta de crédito/débito reducirá posibles fraudes y, por lo tanto, el coste total del proceso de pago.

Los titulares deben poder confirmar que un determinado comercio tiene una relación con una entidad financiera que le permita aceptar tarjetas de crédito/débito. A su vez también deben poder confirmar la identidad de los comercios con quien van a realizar transacciones comerciales.

La especificación SET utiliza las firmas digitales y los certificados electrónicos para autentificar a todas las partes intervinientes en una transacción económica a través de Internet.

- Autenticación

Autenticación en un entorno electrónico es un proceso en el que el receptor de un mensaje puede estar seguro de la identidad del emisor y/o del mensaje. Los protocolos de autenticación pueden estar basados en sistemas de clave secreta (DES) o en sistemas de clave pública (RSA). La autenticación en sistemas de clave pública se basan en firmas digitales.

Una firma digital es una cadena de datos que asegura que la firma incorporada en el mensaje corresponde a la persona que lo escribió. El receptor puede verificar que: (1) el mensaje fue originado en la persona cuya firma se adjunta con el mensaje; (2) que el mensaje no a sido alterado desde que se firmó.

Por lo tanto, una firma digital consta de dos partes: un método para firmar mensajes con el fin de que no sea posible su falsificación y un método para verificar que la firma fue generada por la persona que realmente representa. Además, las firmas digitales no pueden ser repudiadas, de tal forma que el firmante no pueda alegar que el mensaje haya sido modificado.

- Integridad de la Información

La especificación debe garantizar que el contenido del mensaje no es alterado durante la transacción entre el titular y el comercio.

La especificación SET incorpora firmas digitales (descritas en el apartado anterior) que aseguran la integridad de la información contenida en la transacción, como se ha descrito en la sección anterior.

- Interoperabilidad

La especificación SET utiliza protocolos y formatos de mensaje específicos que posibilitan su utilización en diferentes plataformas de *software* y hardware. Cualquier titular podrá operar con cualquier comercio que cumplan con el estándar SET.

- Certificados SET

Los certificados son el soporte electrónico mediante el cual se genera la firma digital y el cifrado de la información de acuerdo con el protocolo SET. Cada uno de los participantes en la transacción comercial electrónica debe disponer de su certificado SET.

- Certificados SET de Titular (*Cardholde*r)

Los certificados de titular actúan como una representación electrónica de una tarjeta de crédito. Estos sólo pueden ser emitidos a propuesta de una entidad financiera de modo que no pueden ser alterados por una tercera parte. En el certificado los datos relativos al número de tarjeta y fecha de caducidad están codificados utilizando un algoritmo y no pueden ser derivados visualizando el certificado. El titular proporciona dicha información a la Pasarela de Pagos donde se verifica el certificado.

Sólo puede emitirse un certificado a un titular cuando su entidad financiera lo aprueba. Mediante la solicitud de un certificado, un titular está indicando su intención de llevar a cabo operaciones de E-comercio. El certificado es transmitido a los comercios con la orden de compra y las instrucciones de pago encriptadas. Con la recepción del certificado de titular, en comercio puede estar seguro, como mínimo de que el número de tarjeta ha sido validado por una entidad financiera emisora.

Un titular puede solicitar tantos certificados como tarjetas de crédito/débito disponga, quedando asociado cada uno a la tarjeta correspondiente.

El *software* utilizado por el titular para almacenar sus certificados y comunicarse con el comercio se denomina "**Electronic Wallet"** o **cartera electrónica**. Este *software*, integrado en el navegador de Internet que utilice el titular, le permitirá además almacenar la información sobre las transacciones efectuadas a lo largo del tiempo.

- Certificados SET de Comercio (*Merchant*):

Los certificados de *merchant* o comercio son un sustitutivo de los logotipos de las marcas de tarjetas de crédito que se muestran en las cristaleras de los comercios. Estos logotipos indican que el comercio posee una relación con una entidad financiera que le permite aceptar pagos a través de tarjetas de crédito.

Dichos certificados son aprobados por la entidad financiera adquirente y aseguran que existe un acuerdo válido entre ambas partes. Un comercio debe disponer de un certificado para cada Brand o marca de tarjeta que acepte (Visa, MasterCard, ...).

El comercio necesita instalar en su servidor un ***software* gestor o *software de Merchant*** de transacciones comerciales a través de redes abiertas y que será compatible con cualquier red de proceso de pagos que soporte la especificación SET independientemente del proveedor. Dicho *software* gestionará los certificados del comercio y todos los procesos de encriptación, direccionamiento, desencriptación, manejo de claves públicas y privadas y comunicaciones con la pasarela de pagos de una forma automática.

- Certificados SET de Pasarela de Pagos (*Payment Gateway*)

Los certificados de pasarela de pagos son emitidos a los adquirentes o sus procesadores de transacciones (operador de medio de pago) y se aplican a los sistemas que procesan las autorizaciones y capturan los mensajes. La clave de encriptación de la pasarela, recogida en el certificado de titular, es utilizada para proteger la información sobre la tarjeta del mismo.

La validez y garantías de los certificados SET reside en la **jerarquía de confianza** que los soporta. Cada certificado esta relacionado con la entidad que los firmó digitalmente. Mediante el seguimiento del árbol de confianza hasta una tercera parte confiable (TTP) conocida, se puede estar seguro de que el certificado es válido. Por ejemplo, un certificado de titular está relacionado con el certificado del emisor el cual a su vez está relacionado con la Brand o Marca a la que pertenece la tarjeta del titular (Visa, MasterCard, ...). La clave pública raíz o clave pública de "Brand" es conocido por todos los *software* SET y podrá ser utilizado para verificar todos los certificados que se encuentran por debajo de él. La clave raíz es distribuida a través de un certificado autofirmado. Esta clave va incluida en el *software* distribuido por los proveedores de *software* SET.

Dicho *software* puede confirmar que posee una clave raíz válida mediante una consulta a la Autoridad de Certificación que posee el *hash* de la clave raíz. Cuando se genera una clave raíz, también se genera una clave de reemplazo. Esta clave de reemplazo se guarda de forma segura hasta que sea necesitada.

El certificado raíz autofirmado y el *hash* de la clave de reemplazo son distribuidos conjuntamente. El *software* SET es notificado del cambio de clave mediante el envío de un mensaje que contenga un certificado autofirmado con la clave de reemplazo y el *hash* de la clave de reemplazo siguiente.

El *software* SET valida la clave de reemplazo mediante el cálculo de su *hash* y comparándolo con el *hash* de esta clave recibido anteriormente.

- La Agencia de Certificación Electrónica

La Agencia de Certificación Electrónica (ACE), creada en 1997 e integrada en un 40% por el Grupo Telefónica (otros socios son SERMEPA, la CECA y Sistema 4B, con un 20% cada uno) es la Autoridad de Certificación encargada del procesamiento de las solicitudes de emisión de certificados de titular, comercio y pasarela de pagos realizadas por las entidades financieras y de la emisión de los mismos.

La ACE[25] facilita la infraestructura necesaria para la emisión de los certificados. Los certificados tendrán una vigencia de un año tras el cual ACE se encargará del proceso de renovación. Además la Agencia de Certificación Electrónica se hará cargo de la gestión de revocaciones de certificados y de las listas negras.

- Requisitos de *software*:

Como se ha indicado anteriormente, una transacción SET utiliza tres componentes de *software*:

Electronic Wallet: la aplicación de cartera electrónica está integrada en el navegador y proporciona al titular un lugar donde almacenar y gestionar sus tarjetas y certificados con el fin de comprar electrónicamente. Al mismo tiempo responde a los mensajes SET que recibe del comercio instándole a seleccionar una tarjeta de crédito para realizar la compra.

Software* de comercio/*merchant: el *software* de comercio es una aplicación que procesa las transacciones de los titulares y comunica con el banco adquirente o la pasarela de pagos solicitando autorización de pago y recibiendo el número de autorización o denegación correspondiente.

***Software* de Pasarela de Pagos:** *software* instalado en la pasarela de pagos para la recepción y procesamiento de transacciones SET.

[25] http://www.ace.es/servicios_f.htm

- Descripción de la operativa SET de E-comercio

En general, en las operaciones de E-comercio se distinguen las siguientes fases:

1. El titular, mediante su *browser* o navegador, conecta con el *web site* del comercio. El contacto inicial puede haberse realizado no sólo a través de los catálogos *on-line* que se muestran en los "escaparates electrónicos" sino, además:
   - Ojeando un catálogo suministrado por el comercio en CD-ROM.
   - Ojeando un catálogo en papel.

2. El titular selecciona un producto que desea comprar.

3. El titular visualiza una solicitud de comprar que contiene una lista de productos, precios, impuestos, gastos de envío, etcétera. Esta solicitud podrá haber sido enviada desde el servidor del comercio o generada por el propio *software* de compra del titular.

4. El titular selecciona el medio de pago (tarjeta, contra-reembolso...) que le ofrece el comercio. En el caso de que seleccione el pago a través tarjeta de crédito utilizando SET abrirá su *wallet* o cartera electrónica. El titular selecciona en su *walle*t el certificado SET ligado a la tarjeta con la que quiere realizar el pago.

5. Se establece una comunicación bajo el protocolo SET entre el *browser* y el comercio utilizando los certificados SET de titular y comercio.

6. El titular, mediante su *wallet,* envía dos sobres con información de su certificado: el pedido de compra firmado (mensaje abierto) y una orden de pago firmada (encriptada).

7. El comercio recibe la transacción electrónica del titular y verifica, mediante su *software* gestor, la validez del certificado del titular y el pedido de compra (firmado por el titular).

8. El comercio envía a la Pasarela de Pagos los datos de la transacción y el sobre encriptado con los datos de la tarjeta del titular.

9. La Pasarela de Pagos recibe la transacción electrónica del comercio, verifica los certificados las firmas del comercio y del titular, y descifra la petición de autorización enviada por el comercio y los datos de la tarjeta enviados por el titular con el fin de solicitar la autorización económica al Medio de Pago correspondiente.

10. La Pasarela de Pagos procesa la petición de autorización económica al Medio de Pago.

11. El Medio de Pago autoriza el pago y envía un mensaje con el número de autorización de la transacción SET a la Pasarela de Pagos.

12. La Pasarela de Pagos envía el número de autorización SET al comercio.

13. El comercio envía los productos o presta los servicios requeridos.

14. El Medio de pago realiza la liquidación a la Entidad Emisora (cargo) y a la Entidad Adquirente (abono).

4.4 Componentes de seguridad

Las soluciones técnicas deben incluir soluciones tanto para los componentes básicos de seguridad y pago electrónico, como para las arquitecturas integradas propuestas por diversos organismos y consorcios industriales, así como para los procedentes de la investigación realizada en los proyectos de I+D europeos sobre E-comercio[26].

Las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:

1. Confidencialidad: evita que un tercero pueda acceder a la información enviada.
2. Integridad: evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.

[26] Secretaria General de Comunicaciones, Estudio de Comunicaciones, "Estudio de situación del comercio electrónico en España", mayo 1999, http://www.sgc.mfom.es/sat/ce/sec2/par211.html

3. Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.
4. No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.

La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra). La Tabla 1 resume brevemente los aspectos técnicos básicos de estos métodos de cifrado. Una descripción más extensa puede encontrarse en multitud de textos y artículos, por ejemplo en [35] o en las referencias citadas al final de la tabla.

Los métodos de cifrado simétrico, por ejemplo el sistema DES, usan una misma clave para cifrar y descifrar. Suponiendo que dos interlocutores comparten una clave secreta y de longitud suficientemente grande, el cifrado simétrico permite garantizar la confidencialidad de la comunicación entre ellos. Este esquema es poco adecuado cuando una parte establece comunicaciones ocasionales con muchas otras con las que no tenía una relación previa, como ocurre frecuentemente en el E-comercio, ya que antes de poder establecer cada comunicación sería necesario intercambiar previamente por algún procedimiento seguro la clave que se va a utilizar para cifrar y descifrar en esa comunicación. Por ejemplo, un consumidor que quisiera comprar a través de Internet necesitaría intercambiar una clave secreta diferente con cada uno de los vendedores a los que quisiera acceder.

Cifrado/descifrado simétrico

Los métodos de cifrado asimétrico, por ejemplo el sistema RSA, usan parejas de claves con la propiedad de que lo que se cifra con una cualquiera de las claves de una pareja sólo se puede descifrar con la otra clave de la pareja. En el caso mas simple, con este sistema un interlocutor sólo necesita tener una pareja de claves que puede utilizar para comunicarse de forma segura con cualquier otro interlocutor que disponga a su vez de otra pareja de claves. Cada interlocutor hace pública una de sus claves (será su clave pública) y mantiene en secreto la otra (su clave privada). Por ello, el cifrado asimétrico se denomina también cifrado de clave pública. La clave privada (o las claves privadas si el usuario utiliza varias parejas de claves para diferentes propósitos) puede guardarse en el ordenador del usuario o en una tarjeta inteligente.

Por la propiedad de las parejas de claves citada antes, para enviar un mensaje de forma confidencial a un destinatario basta cifrarlo con la clave pública de ese destinatario. Así sólo el podrá descifrarlo mediante la clave privada que mantiene en secreto. No es necesario que el remitente y el destinatario intercambien previamente ninguna clave secreta. El remitente sólo necesita averiguar la clave pública del destinatario. Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

Cifrado asimétrico con consulta de clave publica a autoridad de certificación y descifrado con clave privada del destinatario

Los sistemas de clave pública permiten además cumplir los requisitos de integridad del mensaje, autenticación y no repudio del remitente utilizando firmas digitales. El procedimiento de firma digital de un mensaje consiste en extraer un "resumen" (o *hash* en inglés) del mensaje, cifrar este resumen con la clave privada del remitente y añadir el resumen cifrado al final del mensaje. A continuación, el mensaje más la firma (el resumen cifrado) se envían como antes cifrados con la clave pública del destinatario. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un resumen diferente (la firma digital de un usuario no es siempre la misma secuencia de bits, sino que depende del mensaje firmado).

Generación de la firma digital de un mensaje

Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma. Para ello, hace dos operaciones: por un lado averigua la clave pública del remitente y descifra con ella el resumen que calculó y cifró el remitente. Por otro lado, el destinatario calcula el resumen del mensaje recibido repitiendo el procedimiento que usó el remitente. Si los dos resúmenes (el del remitente descifrado y el calculado ahora por el destinatario) coinciden la firma se considera válida y el destinatario puede estar seguro de la integridad del mensaje: si el mensaje hubiera sido alterado a su paso por la red, el resumen calculado por el destinatario no coincidiría con el original calculado por el remitente.

Además, el hecho de que el resumen original se ha descifrado con la clave pública del remitente prueba que sólo él pudo cifrarlo con su clave privada. Así el destinatario está seguro de la procedencia del mensaje (autenticación del origen) y, llegado el caso, el remitente no podría negar haberlo enviado (no repudio) ya que sólo él conoce su clave secreta. Los inconvenientes de este sistema son la lentitud de los algoritmos de clave asimétrica (típicamente varia veces más lentos que los de clave simétrica) y la necesidad de las autoridades de certificación ya mencionadas. Un certificado digital emitido por una de estas autoridades contiene la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el periodo de validez del certificado), todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. Pueden existir varios tipos de certificados, válidos para diferentes usos, según la información y garantías que la autoridad de certificación (directamente o a través de una autoridad de registro) pide al usuario antes de emitir el certificado. Unos de los formatos de certificado más extendidos es el definido en la recomendación X.509 v3 del ITU-T [36].

Comprobación de una firma digital

Como en la práctica no es viable que todos los usuarios estén certificados por la misma autoridad, surge la necesidad de que unas autoridades de

certificación certifique a su vez a otras, bien de forma jerárquica (las autoridades de un nivel jerárquico son certificadas por otras de nivel superior hasta llegar a una autoridad raíz) o mediante certificaciones cruzadas entre autoridades del mismo nivel (de forma que cada una acepta como fiables los certificados emitidos por la otra). La infraestructura necesaria para el uso de los sistemas de clave pública, incluyendo las autoridades de certificación, se llama Infraestructura de Clave Pública (PKI: *Public Key Infrastructure*).

Hay muchos detalles no incluidos en este resumen, por ejemplo el uso de varias parejas de claves, diferentes tipos de certificados, la combinación de algoritmos de clave simétrica y asimétrica (ver Figura 5), los estándares existentes para cifrado, firmas, certificados, etcétera[27].

4.5 Arquitecturas de E-comercio

Diversos organismos han definido arquitecturas para el E-comercio con pretensiones de seguridad, entre ellos la Asociación CommerceNet, varios consorcios industriales y diversos proyectos financiados por la Comisión Europea[28].

- CommerceNet

CommerceNet, representada en España, entre otros proyectos piloto de investigación tecnológica (prototipos y demostraciones) realizados con sus importantes socios, ha lanzado la arquitectura eCo. El grupo de trabajo eCo, que incluye expertos de compañías como Hewlett-Packard, IBM, Intel, Sun

[27] Para más información, el estudio oficial remite a las siguientes referencias técnicas sobre seguridad: Guías del Open Information Interchange (OII) sobre Seguridad de la Información [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx37], Estándares de Seguridad [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx] y Servicios de Terceras Partes Fiables [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx], Sección de estándares de firma digital de [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx], Revista Novática, número sobre Criptología [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx], Página sobre seguridad del W3C [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx] y Proyectos europeos sobre seguridad [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx

[28] Otras arquitecturas pueden consultarse en La Guía de E-comercio [http://www.sgc.mfom.es/sat/ce/parrefs.html#xx] del *Open Information Interchange* (OII).

Microsystems, RosettaNet y VeoSystems, tiene como objetivo desarrollar un entorno común que permita la interoperabilidad de diversas especificaciones de entornos de E-comercio tales como EDI, OBI, OTP y otras. La arquitectura eCo está basada en el lenguaje XML. Las interfaces de servicio se definen en términos de documentos comerciales, por ejemplo una oferta de precios, un pedido, etcétera y de los procedimientos asociados a cada uno de ellos (*Business Interface Definition* o BID).
CommerceNet, al igual que otros consorcios como el W3C, define una especificación y ofrece un *software* genérico que la cumple. El disponer de *software* asequible ayuda a crear una norma "de facto", mientras que la existencia de una especificación da una vía evolutiva para sustituir este *software* por otro de mejor calidad si es necesario.

Las directrices del Memorándum de Acuerdo sobre libre acceso de las PYMEs europeas al E-comercio con el respaldo de la Comisión Europea recomiendan el uso del sistema eCo como punto de partida para el desarrollo de una arquitectura de E-comercio interoperable. Es una plataforma neutral en el sentido de que se beneficia de la aportación de la mayoría de las principales empresas implicadas en el E-comercio en Estados Unidos Las mismas directrices del Memorándum de Acuerdo recomiendan el establecimiento de un pequeño número de puntos focales europeos; por ejemplo ECE, CommerceNet, W3C, CEN/ISSS o ICC para promover el desarrollo de bloques constitutivos de *software* interoperables, tomando como punto de partida la arquitectura eCo.

- Open Buying on the Internet (OBI)

Esta es una especificación para E-comercio entre empresas que compren numerosos productos de bajo precio unitario. El consorcio OBI, desde junio de 1998, está gestionado también por CommerceNet. Su arquitectura incluye cuatro entidades: la persona que hace un pedido, la empresa vendedora, la compradora y la autoridad de pago. Omitiendo algunas interacciones complementarias u opcionales, las entidades citadas interactúan en cuatro pasos:

La versión 1.1 de OBI especifica los procedimientos de acceso a los catálogos, el formato de los mensajes intercambiados entre las entidades

anteriores (basado en el estándar EDI ANSI X12, aunque en el futuro pueden incluirse EDIFACT y XML), los procedimientos de transmisión de estos mensajes a través de Internet (HTTP) y los mecanismos de seguridad necesarios para la autenticación de las partes, confidencialidad y no repudio de los mensajes (uso de SSL, mensajes formato PKCS 7 y certificados digitales X.509 versión 3). La inclusión del lenguaje XML es una de las mejoras previstas.

- Open Trading Protocol (OTP)

OTP pretende reproducir en un escenario electrónico la secuencia de interacciones que tienen lugar en las transacciones tradicionales, incluyendo los documentos que ahora nos son familiares: recibos, facturas, etcétera. Los roles definidos por OTP son el comprador, el vendedor, el receptor del pago (que actúa en representación del vendedor), la entidad que entrega el producto y la entidad que se encarga de la atención al cliente y la resolución de posibles conflictos. OTP especifica el formato y contenido de los mensajes intercambiados entre entidades, así como las posibles formas de transmitir los mensajes de una entidad a otra. Hace uso del estándar XML Los pasos de una transacción encapsulan procedimientos básicos como por ejemplo: oferta, acuerdo de compra , pago (usando alguno de los mecanismos de pago existentes), entrega, recibo de compra y resolución de problemas en la transacción. El uso de firmas digitales es opcional y no se requieren certificados de cliente. La primera versión de la especificación se publicó en 1998.

- Building Blocks for Electronic Commerce

El proyecto fue patrocinado por la Comisión Europea DGIII/B2. Los componentes (*building blocks*) de E-comercio se definen a partir del análisis de los procesos comerciales de interés, clasificándolos en tres grupos: componentes del comprador, del vendedor y de terceras partes. El modelo identifica los siguientes componentes:

1. De marketing:
   Creación / consulta de catálogos
   Publicación de información / análisis de información
   Ofertar un precio / pedir una oferta de precio
   Reservar un producto para un comprador / añadir un producto a la cesta de la compra

2. De contratación:
   Confirmar un pedido / hacer un pedido
   Reponer existencias de un producto / registrar la confirmación de un pedido
   Aceptar la cancelación / cancelar un pedido

3. De logística:
   Recibir / generar una notificación de entrega
   Recibir /entregar un producto

4. De cierre de una operación:
   Confirmar / seleccionar un método de pago
   Procesar / entregar una tarjeta de crédito o monedero electrónico
   Efectuar el pago

5. De interfaz con la Administración
   Declaración de impuestos
   Notificaciones de exportación

4.6 Arquitectura SEMPER

Abreviatura de *Secure Electronic Market Place for Europe*, es un proyecto también financiado por la Unión Europea que se planteó como objetivos estudiar los requisitos e implicaciones técnicos, legales, comerciales y sociales del E-comercio, definir una arquitectura de E-comercio abierta e independiente de plataformas hardware/*software* o arquitecturas de red específicas y, por último, implementar y evaluar un prototipo. Soporta transacciones seguras entre comprador y vendedor, así como con terceras partes como autoridades de certificación, *brokers*, notarios, etc. SEMPER ofrece dos grupos de servicios de seguridad:

- 1.Básicos: autenticación, integridad, firma digital, pago y confidencialidad

- 2.Avanzados, por ejemplo anonimidad, resolución de conflictos, sellos de tiempo y firma de contratos por varias partes**.**

5. Bibliografía

- BALLESTEROS A. “La logística como opción estratégica”, Código 84, enero-febrero, Barcelona 1998

- CASARES Y REBOLLO. “Distribución Comercial” Ed. Civitas. Madrid 1996

- Forrester Research, Inc. “Informe sobre E-comercio”. . http;//www.forrester.com

- Javier Ribas http://www.onnet.es “*Manual práctico sobre E-comercio en Internet”***.** RIBAS&RODRIGUEZ. Abogados Asociados

- Resolución del consejo de 19 de enero de 1999, sobre la dimensión relativa a los consumidores en la sociedad de la información. *Diario Oficial n° C 023 de 28/01/1999 P. 0001 – 0003*

- SET Secure Electronic Transaction LLC, http://www.setcéteraéterao.org/

- Secretaria General de Comunicaciones, “Estudio de situación del E-comercio en España”, mayo 1999, http://www.sgc.mfom.es/sat/ce/sec2/par211.html

- TAMCRA, “E-comercio e Internet”, .fudesco.es/publicab/b-188-189/informe1.html, 1997

- The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda. OCDE. Octubre 1998. http://www.oecd.org/subject/e_commerce/summary.htm

- Ensuring security and trust in electronic communication: Towards a European Framework for Digital Signatures and Encryption. Comunicación de la Comisión Europea COM(97) 503 final. Octubre 1997. http://www.ispo.cec.be/eif/policy/97503toc.html

- A common framework for electronic signatures. Propuesta de directiva del Parlamento Europeo y el Consejo. COM(98) 297 final. Mayo 1998. http://www.ispo.cec.be/eif/policy/com98297.html

- Taking up, pursuit and prudential supervision of the business of electronic money institutions. Propuesta de directiva del Parlamento Europeo y el Consejo. 1998. http://europa.eu.int/comm/dg15/en/finances/general/727.htm

- Commission Recommendation concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder. 97/489/EC. Julio 1997.
http://www.ispo.cec.be/ecommerce/recpay.zip

- Taxation Principles and Electronic Commerce. OCDE. 1998.
http://www.oecd.org/subject/e_commerce/ebooks/ecomm2_1.pdf

- Comunicación de la Comisión Europea sobre E-comercio y fiscalidad indirecta. COM(98) 374 final; junio 1998.
http://www.ispo.cec.be/ecommerce/docs/Es.zip

- Commission green paper on copyright and related rights in the information society. COM (95) 382 final. Julio 1995.
http://www.ispo.cec.be/infosoc/legreg/com95382.doc

- Copyright and related rights in the information society. Comunicación de la Comisión Europea COM (96) 586 final, Noviembre 1996.
http://www.ispo.cec.be/infosoc/legreg/docs/com96586.html

- Problemas jurídicos del E-comercio. Fernando Ramos. Revista Electrónica de Derecho Informático R.E.D.I. Número 2. Septiembre de 1998.
http://www.derecho.org/redi/numero2/ramos2.shtml

- E-comercio en Internet. Aspectos jurídicos. Xavier Ribas. (Extracto de la obra del mismo autor: Manual práctico sobre E-comercio en Internet.) Revista Electrónica de Derecho Informático R.E.D.I. Número 2. Septiembre de 1998.
http://www.derecho.org/redi/numero2/ribas2.shtml

- Autoridades de certificación. Fernando Ramos. Anguiano y Asociados.
http://www.arrakis.es/~anguiano/artautcert.html

- Digital Signature: Inventory of International Regulatory, Standardisation, and Commercial Activities. Editado por A. Servida, Comisión Europea DGIII F/4. Abril 1998.
http://www.ispo.cec.be/ecommerce/digisign.htm

- Novática: Número 134, Julio-Agosto 1998. Criptología.
http://www.ati.es/PUBLICACIONES/novatica/1998/134/nv134sum.html

- W3C Security Resources. http://www.w3.org/Security/

- Electronic commerce security related projects supported by the EC. Febrero 1997. (Documento previo a la convocatoria temática sobre E-comercio de ESPRIT de marzo de 1997). http://www.ispo.cec.be/ecommerce/securit1.htm

- Recomendaciones sobre E-comercio. ACTS guideline SII G9. Julio 1998.
http://www.infowin.org/ACTS/ANALYSYS/CONCERTATION/glindex.htm

- Accelerating Electronic Commerce in Europe. Comisión Europea. Junio 1998. http://www.ispo.cec.be/Ecommerce/ecbook.html

- Memorándum de acuerdo sobre libre acceso de las PYMEs europeas al E-comercio - Directrices. Abril 1998.
http://www.ispo.cec.be/Ecommerce/MoU/default.htm (acuerdo)
http://www.ispo.cec.be/Ecommerce/MoU/S1300.htm (directrices)

- Iniciativa Europea de E-comercio. Comunicación al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones. COM (97) 157. Abril 1997.
http://www.ispo.cec.be/Ecommerce/initiat.htm

- Legal Framework for the Development of Electronic Commerce. Propuesta de directiva del Parlamento Europeo y el Consejo. COM(98) 586 final. Noviembre 1998. http://www.ispo.cec.be/ecommerce/legal.htm#legal
http://www.ispo.cec.be/ecommerce/docs/legal.pdf (nota de prensa)
http://europa.eu.int/comm/dg15/en/media/eleccomm/999.htm (resumen)

- A Framework for Global Electronic Commerce. (Política de E-comercio del gobierno federal de Estados Unidos). Julio 1997.
http://www.ecommerce.gov/framewrk.htm

- Globalisation and the Information Society: The Need for Strengthened International Coordination. Comunicación de la Comisión Europea. COM (98) 50. Febrero 1998.
http://www.ispo.cec.be/eif/policy/com9850en.html

- "A Borderless World - Realising the Potential of Global Electronic Commerce." . Documentos de la conferencia ministerial de la OCDE celebrada en Ottawa, 7-9 octubre 1998.
http://www.oecd.org/subject/e_commerce/

- "Dismantling the Barriers to Global Electronic Commerce". Informe final de la conferencia ministerial de la OCDE celebrada en Turku, Finlandia, 19-21 noviembre 1997.
http://www.oecd.org/dsti/sti/it/ec/prod/turkufin.pdf

- Electronic Commerce: Opportunities and Challenges for Government (Sacher Report). OCDE. Junio 1997.
http://www.oecd.org/dsti/sti/it/ec/act/sacher.htm

- Measuring Electronic Commerce. OCDE/GD(97)185. 1997.
http://www.oecd.org/dsti/sti/it/ec/prod/e_97-185.htm

- Guidelines for Cryptography Policy. OCDE. 1997.
http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm

- Código ético de protección de datos en Internet. AECE. 1998.
http://www.aece.org/corporativo/codigoetico.doc

- Informe final del proyecto AEQUITAS.
http://aequitas.encomix.es/finalpro.htm

- Propuesta para un proyecto de ley de firma electrónica español. Comité de legislación de la Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE). Borrador. Julio 1998.
https://ca.feste.com/981001pl.htm

- Análisis de la propuesta de directiva europea por la que se establece un marco común para la firma electrónica (COM(98) 297, ver referencia [3]). FESTE, septiembre 1998.
https://ca.feste.com/posidire.htm

- Audiencia en Internet - resultados de la 2ª encuesta sobre Internet. AIMC. Abril - Mayo 1998.
http://www.aimc.es/aimc/html/inter/net.html

- Estudio sobre E-comercio entre empresa y consumidor, en Internet y en España, AECE. Noviembre 1998.
http://www.aece.org/info/documento/estudio.htm

- El E-comercio entre empresas. Francisco J. Ruiz. Novática. Número 135, Septiembre-Octubre 1998.
http://www.ati.es/PUBLICACIONES/novatica/1998/135/nv135sum.html