Firma Electrónica y Fe Pública extrajudicial

JOSE MARÍA MOLINA MATEOS

Dotor en Derecho. Criptólogo.

1.- EL COMERCIO ELECTRÓNICO Y LA NECESIDAD DE CONFIANZA.

Para la Comisión Europea, en su documento sobre la Iniciativa de Comercio electrónico, en el contexto actual, la utilización de las nuevas tecnologías de la comunicación, y, especialmente, de Internet, como instrumentos de desarrollo del comercio electrónico, permite grandes y nuevas oportunidades de negocio, mayor competitividad, reducción de costes, y mayor rapidez en el desarrollo de las relaciones comerciales. Todos ellos principios que deben presidir la organización y desarrollo de cualquier actividad empresarial.

E1 comercio electrónico favorece también a los consumidores, que gozan de mayor capacidad de elección y se pueden beneficiar de una bajada de precios a medida que disminuyan los costes generales.

Pero junto a las evidentes ventajas, la utilización de estas nuevas tecnologías, y los cambios que suponen, pueden generar riesgos e

incertidumbres en los operadores económicos sobre cuestiones jurídicas tan esenciales como la validez y eficacia de las transacciones electrónicas, problemas derivados del perfeccionamiento del contrato celebrado a través de estos medios, la prueba, la delimitación de responsabilidades, la ley aplicable o jurisdicción competente, entre otras. En definitiva, los múltiples problemas derivados de la dificultad de aplicar conceptos y categorías jurídicas tradicionales a contratos realizados por medios totalmente distintos a los utilizados en el momento de ser concebidos estos conceptos y categorías.

Además existen también riesgos derivados de los problemas propios de los sistemas electrónicos a través de los que se desarrolla este nuevo comercio, los cuales son susceptibles de usos, abusos y errores que pueden provocar graves consecuencias a los participantes.

Los riesgos aumentan cuando este comercio se desarrolla en redes abiertas, como Internet, donde la suplantación de la autoría, la alteracion del mensaje, el repudio o la vulneración de la confidencialidad, que desde el punto de vista jurídico plantea serias dudas sobre la validez y eficacia de las transacciones electrónicas.

Por ello, el primer objetivo que ha de conseguirse para poder desarrollar el comercio electrónico es generar confianza: es preciso que los consumidores como las empresas tengan confianza en que sus transacciones no serán interceptadas ni modificadas, el comprador y el vendedor son los que dicen que son, y los mecanismos utilizados en la transacción son accesibles, legales y seguros. Sin embargo, está muy extendida la inquietud respecto a la identidad y solvencia de los suministradores, su localización ffsica, la integridad de la información, la intimidad, el cumplimiento de contratos a distancia, las garantías de pago, los recursos en caso de error o estafa, y los posibles abusos de posiciones dominantes, todas estas inquietudes, aumentan exponencialmente cuando las transacciones se hacen a través de las fronteras.

En esta transición de un sistema comercial basado en el soporte papel hacia un sistema con base en soportes magnéticos, y medios electrónicos, es

necesario que la sustitución tanto del papel como de la firma manuscrita, que tanta confianza ha generado durante siglos, logren encontrar sus equivalentes electrónicos capaces de generar, al menos, la misma confianza, y ofrecer seguridad jurídica a los operadores económicos.

Se necesita eliminar estos riesgos e incertidumbres actualmente inherentes a los medios electrónicos y pasar a hablar de un comercio electrónico seguro. Pero en el nuevo entorno tecnológico en el que se desarrolla el comercio electrónico, las soluciones jurídicas están ligadas a soluciones técnicas que las posibiliten de forma eficaz, a través de la integridad, disponibilidad, autenticación, no repudio y confidencialidad, presupuestos básicos de la seguridad técnica, en cuya base opera de forma determinante la criptología.

Sin embargo, mientras las tecnologías seguras están operativas y disponibles para su uso comercial, no se ha logrado, todavía, completar el marco regulador, jurídico e institucional, necesario para el logro de un comercio electrónico seguro.

a) **Firma electrónica, criptografía y tercero de confianza.**

La firma electrónica se podría entender como el método, signo o símbolo de naturaleza electrónica incorporado por su titular a un documento preparado para ser tratado por medios telemáticos, con cualquiera de las finalidades previstas para la firma manual.

Los elementos que la constituyan han de estar dispuestos de modo que proporcionen, de forma técnicamente segura y verificable: Certeza sobre la identidad de su autor, garantía de integridad sobre el contenido del documento al que se asocia, control exclusivo por su titular, garantías de "no rechazo" por autor y destinatario, y confidencialidad, en los casos que la firma electrónica se utilice también para evitar que el contenido del documento pueda ser conocido por terceros.

La firma electrónica está constituida por el conjunto de elementos técnicos, matemáticos, organizativos, procedimentales, o de cualquier otra naturaleza, utilizados para la creación y verificación de la misma.

Los elementos básicos, constitutivos de la firma electrónica, se podrían agrupar en: mecanismos de emisión, mecanismos de comprobación, herramientas y certificados.

También son elementos constitutivos de la firma electrónica, los proveedores de servicios de certificación y la entidad que los acredite como tales, en su caso.

El auge y desarrollo de la criptografia, especialmente, la asimétrica, basada en un par de claves asociadas: una clave privada, conocida solo por su titular, que debe mantenerla en secreto, y una clave pública relacionada matemáticamente con ella y que puede ser accesible para cualquiera, es un instrumento esencial en la firma electrónica. Las dos claves están matemáticamente relacionadas entre sí, con un diseño y ejecución de forma segura de modo que es virtualmente imposible que quien conozca la clave pública pueda derivar de ella la clave privada.

Este sistema, además de garantizar la confidencialidad a través de canales inseguros, como Internet, sin necesidad de comunicación previa de una clave secreta compartida, permite realizar firmas digitales, que proporcionan autenticidad, integridad y no repudio, y pueden ser tanto o más válidas, eficaces y seguras que la firma manuscrita.

En el estado actual de la tecnología, la criptografia asimétrica y la firma digital, son un paso decisivo hacia el comercio electrónico seguro, -aunque eventualmente podrían surgir otros procedimientos- pero por sí solas no son suficientes. En comunidades amplias son necesarias, por razones prácticas, una forma de distribución segura de claves públicas que garanticen su correcta asociación con una persona privada, y se necesitaría una tercera parte de confianza, la cual actuará para asegurar el vínculo entre la clave pública y el titular de la clave privada, además de realizar funciones como autenticar fechas y horas de las transacciones, publicar electrónicamente las

claves revocadas o suspendidas, responsabilidades en la negación de la transacción, funciones de emisión de certificados de clave pública, servicios de registro, sellado temporal de datos, y otros servicios basados en firmas digitales.

Para la distribución fiable de claves públicas, se ofrecen diversas vías: Registro de claves públicas, Web-of-trusty Terceras partes de confianza.

La que parece ser la solución más adecuada y posible, Terceras partes de confianza (Trusted third party o TTP) consiste en la intervención de una o más terceras partes de confianza que emiten certificados que, a la vez que sirven para distribuir la clave pública, sirven, fundamentalmente, para asociar, de forma segura, la identidad de una persona concreta a una clave pública determinada.

Tercera parte de confianza es cualquier entidad de confianza de las partes intervinientes en una transacción para proporcionar servicios de seguridad. La específica tercera parte de confianza que desempeña esencialmente la función de emisión de certificados se suele denominar entidad de certificación, proveedor de servicios de certificación o certificador.

La criptografia permite la creación de dos claves para la creación de una firma digital, pero esta, per se, no tiene una asociación intrínseca con nadie. Por ello necesita de una tercera parte de confianza para las dos primeras partes que usan las claves que pueda certificar la persona realmente asociada a ese par de claves. Estas terceras partes necesitan de una regulación y determinación de responsabilidad.

Dentro de las firmas digitales pueden existir distintos niveles o firmas de distinta naturaleza y diferente valor, en definitiva, firmas de distinta calidad, que pueden ser igualmente válidas, pero que pueden tener distinta eficacia jurídica, e incluso legal, en la medida que se establezcan determinados efectos legales para firmas electrónicas de mayor calidad, beneficiándola con determinadas presunciones a efectos probatorios.

UNCITRAL establece una clasificación de categorías de firmas en orden creciente en función de su mayor seguridad: firmas electrónicas, firmas digitales, firmas digitales verificadas por referencia a un certificado emitido por una entidad de certificación, firmas digitales verificadas por referencia a un certificado emitido por una autoridad con licencia.

Y cabría añadir, también, firmas digitales verificadas por referencia a un certificado emitido por una autoridad de certificación especialmente cualificada como podría ser un Notario o un Corredor de Comercio, y firmas digitales autenticadas ante Notario.

Dentro de estas categorías generales cabría distinguir subolases en función del nível y calidad de los servicios pactados y prestados por la autoridad de certificación.

b) Entidades de certificación.

La intervención de una entidad de certificación debe añadir confianza a la firma digital. La fiabilidad de cada firma digital creada por una clave privada dependerá en buena medida de la fiabilidad de la asociación de aquella clave con una persona determinada realizada por una entidad de certifcación, que puede ir desde una simple entidad independiente, creada libremente, hasta llegar a ser una entidad que actúe como fedataria pública.

En todo caso, el papel central de la entidad de certificación, al emitir un certificado, es vincular de forma segura una clave pública, e indirectamente, una clave privada, a una persona determinada. Por ello, la entidad de certificación es responsable de adoptar las medidas necesarias para determinar la identidad de la persona para la que emite un certificado.

Las necesidades generales del mercado parecen evolucionar hacia certificados de distintos niveles. Desde los certificados en los que la entidad de certificación se limita a comprobar determinados datos proporcionados por el solicitante on-line; o certificados con otras medidas como presencia física, presentación de documentos identificativos y verificación de capacidad.

La existencia de distintos tipos de certificados, y diversas clases de firmas digitales, con distintos niveles de seguridad, supone, desde el punto de vista jurídico, el reconocimiento de efectos diferentes, y la existencia de variados niveles de responsabilidad en función de la clase de firma y certificado.

La acomodación de efectos jurídicos y prácticas comerciales no ha de llegar hasta el extremo de considerar "certificados", aquellos que, aún siendolo en el sentido literal del término, no reunen con las exigencias básicas de la distribución de las claves públicas, como podría ser el caso de de los certificados basados en un proceso de solicitud y registro puramente on-line, sin comprobación alguna de identidad.

La función principal de la entidad de certificación es la comprobación de la identidad del titular de la clave pública. Para asegurar tanto la autenticidad del mensaje como la identidad de la persona que ha expedido el certificado, la entidad de certificación lo firma digitalmente con la doble finalidad de proteger la integridad del certificado y permitir que la firma digital de la entidad de certificación sea verificada.

De esta forma se resuelve el problema de una asociación segura de una clave a una persona determinada, pero no el de quien certifica a la entidad de certificación para lo cual existen procedimientos inspirados en líneas jerárquicas o verticales y horizontales o de reconocimiento recíproco entre entidades de certificación. En todo este proceso, la confianza resulta determinante.

Los proveedores de servicios de certificación son "terceros" de "confianza" con una función que tiene trascendencia pública por su cometido de comprobar identidades, certificar cifras o guarismos y la pertenencia de estas a personas concretas con sus características y prestar otros servicios de seguridad, que incluyen aspectos técnicos, jurídicos y administrativos .

La "confianza" es fundamental para la existencia del Comercio Electrónico, los proveedores de estos servicios serán un catalizador en el

desarrollo de una sociedad de la información que incluirá la mayoría de organizaciones y naciones del mundo.

Estos "terceros", "suministradores de confianza", necesitan trabajar juntos para dar respuesta a la demanda creciente, compleja, múltiple y diversa de transacciones y relaciones requeridas, frecuentemente sin fronteras. Ha de tenerse en cuenta que estos "terceros de confianza"tienen una función de transcendencia pública por su contenido de comprobar identidades, certificar dígitos pertenecientes a personas concretas con sus características, y prestar otros servicios de seguridad que incluyen aspectos técnicos, jurídicos v administrativos.

Para ello se necesita crear políticas y standares, construidos y elaborados desde una perspectiva de cooperación que facilite el comercio global a nivel internacional y nacional.

En este contexto es conveniente la articulación de los "entes" prestadores de estos servicios, mediante la formación de asociaciones para satisfacer los requerimientos nacionales o de industrias específicas, pero basados en una cooperación de base global.

La iniciativa EMERITUS de la Unión Europea pretende establecer un sistema de políticas voluntario, articulado a través de asociaciones de servicios de confianza en cada nación (Trust Servise Association, TSA) y una federación global (Global Trust Servises Union, GTSU) de las asociaciones de servicios de confianza nacionales, de forma que permitan a los proveedores de servicios de confianza la libre competencia, en el marco de unos determinados principios.

2.- EL FEDATARIO PÚBLICO EXTRAJUDICIAL COMO TERCERO DE CONFIANZA EN LA SOCIEDAD DE LA INFORMACIÓN: ESPECIAL REFERENCIA AL NOTARIADO.

a) Antecedentes históricos del notariado.

Los sectores doctrinales más numerosos se inclinan por afirmar que el Notariado es una Institución que aparece con caracteres perfilados en el Bajo Imperio Romano, ya que es el derecho bizantino el que da lugar a un primer grado de evolución de la institución, al unificar tabularios y tabeliones.

Los precedentes notariales estarían ya recogidos en los libros sagrados y los más antiguos códigos de los que se tienen vestigios y no hacen otra cosa que poner de manifiesto la necesidad de la función notarial en las sociedades políticas con un grado superior de desarrollo.

Las escuelas de Derecho romano y de Derecho canónico, de la Universidad de Bolonia, crearon la base científica de la función notarial profesional durante el siglo XII. Los notarios realizaban las funciones de escribanos y de funcionarios de actuaciones en los tribunales eclesiásticos de la Edad Media y en las cancillerías de los soberanos laicos o de los municipios.

En el ámbito latino, la práctica de los tribunales el documento notarial obtuvo desde el primer momento la significación de un argumento que no tenía necesidad de prueba alguna, recibiendo los notarios la cualidad de funcionarios cuyos documentos gozan de fe pública.

Salvando las distancias entre el escriba hebreo y el Notario de hoy, como igualmente tenemos que salvar las distancias entre las sociedades de entonces y las actuales, las funciones de estas dos personas, aunque históricamente lejanas, tienen un gran parecido. Ambas redactan actos o sucesos jurídicos y les dan la notoriedad oficial que la organización jurídica en la que viven les permite.

Entre los hebreos había varias clases de Scribae, los Escribas del Rey, Escribas de la Ley, Escribas del pueblo y Escribas del Estado, los cuales ejercían funciones similares a la fe pública, en su sentido moderno y daban autoridad a los actos que suscribían. En unos casos daban fe por la delegación que recibían, en otros eran meros amanuenses, en otros tenían funciones autentificadoras, etc.

Existen referencias históricas suficientes como para apreciar la similitud de instituciones tanto en el derecho romano, como en el heleno y el egipcio.

El profesor Seidi llega a afirmar que "La diplomacia de los egipoios arranca del documento en papiro, y está, por tanto, ya por el material, más cerca del documento en papiro del período helénico-romano posterior y de nuestro documento actual, en papel, que el ladrillo de los babilonios o la tabla encerada de los romanos. Egipto nos muestra, lo más antiguo de la historia de nuestra forma de documentos. En la época más antigua, entre los negocios de derecho privado vemos un documento garantizado por un sello oficial de cierre; en época posterior encontramos un documento sin sellar, pero garantizado frente a añadiduras o falseamientos posteriores por la observación de un rígido formulario y la firma del notario y de los testigos, y en los últimos siglos, por lo menos, los archivos y los registros constituían otra protección más contra aquellas alteraciones"

b) Los sistemas notariales.

Según se entienda la natura de la función y su alcance, así como el modo de realizarla, la intervención del Estado o los efectos del documento notarial, se pueden establecer diversas clasificaciones del notariado en el derecho comparado.

Doctrinalmente se distinguen cinco clases distintas de organizaciones o sistemas notariales, aunque se observan coincidencias fundamentales que permiten reducir sustancialmente este número, llegándose a dos divisiones

fundamentales el notariado latino al también denominado público y el notariado sajón denominado privado.

Los sistemas notariales de tipo latino, cuya denominación procede de su implantación en los países de este área cultural, tienen como características básicas que el notario actúa como funcionario y a la vez como profesional del Derecho, que el documento publico intervenido por el notario tiene una triple finalidad: construye, solemniza y autentifica, su competencia se extiende a toda la esfera extrajudicial, comprendiendo las actuaciones de la llamada jurisdicción voluntaria y, organizativamente, aunque apoyada en una base corporativa está sometida a la autoridad del Estado, a través de órganos administrativos.

El notario sajón surge en el ámbito del derecho inglés, en el que, su especial formación, su origen consuetudinario, la excepcional duración en el tiempo de sus leyes, la eficacia normativa de la Jurisprudencia y al original sistema de contratación basado, no es un criterio formal, sino causalista, ha dado lugar a un especial tipo de notariado totalmente distinto del latino.

El notario sajón no tiene carácter de funcionario, aunque el Estado señale las condiciones para el desempeño de la función, es colaborador técnico en la redacción del contrato, pero su intervención no solemniza, ni siquiera autentifica el contrato. Esta autenticidad o veracidad se refiere solamente a las firmas del documento y no al contenido del mismo.

Su competencia no es exclusiva, pues los actos en los que interviene, pueden también ser intervenidos por abogados, procuradores, o escribanos.

En los países sajones la forma instrumental no tiene la ritualidad que en los latinos. el valor formal de un acuerdo jurídico se obtiene o como consecuencia de un proceso judicial o de una actuación del Juez o por la intervención del Notario, limitada al solo efecto de garantizar la autenticidad de las firmas

c) El Notario como entidad de certificación

Existen diversos intentos de estudio y creación de cibernotarios o notarios electrónicos, aunque los conceptos que expresan tienen distinto sentido y alcance desde la perspectiva técnica y la jurídica.

Desde el punto de vista técnico, de forma genérica, por notario electrónico se suele entender la tercera parte de confianza que puede desempenar funciones de entidad de certificación. Algunos documentos técnicos definen "notarización" como el registro de datos por parte de un tercero de confianza que permite asegurar posteriormente la exactitud de características tales como su contenido, origen, tiempo y entrega; y definen el "notario" como una tercera parte de confianza que proporciona seguridad sobre las propiedades de los datos comunicados entre dos o más entidades como la integridad, el origen, el tiempo o el destino de los datos.

Desde el punto de vista jurídico, se pretende que un cibernotario o notario electrónico pueda desempeñar funciones similares a las de los notarios tradicionales, pretensión que tropieza con la dificultad de la distinta naturaleza de la función notarial en los países latinos y los anglosajones, aparte de la dificultad inherente a la actividad desarrollada por los notarios en cuanto a exámen de capacidad, asesoramiento legal, intervención en contratos bilaterales, etc.

La Comisión de Asuntos Jurídicos y Derechos de los Ciudadanos sobre la situación y la organización del notariado en los Estados miembros de la Comunidad, publicado en Documentos de Sesión del Parlamento Europeo, 9 de diciembre de 1.993, recoge la situación y organización del notariado en los existentes -entonces doce- países de la Comunidad.

De las distintas reflexiones que se contienen en el documento, deduce los requisitos comunes de los sistemas de notariado en los países miembros de la Comunidad: "El notario es siempre un jurista al servicio de relaciones jurídicas privadas que ha obtenido, para ejercer tal función, un fítulo universitario de licenciado en Derecho. Pero al mismo tiempo es un

funcionario público que recibe una delegación de la autoridad pública para redactar escrituras públicas que dan fe públicamente y, como tal, está sometido al control del Estado, que es quien le confiere el título de notario o la investidura notarial".

"El documento notarial tiene carácter de documento público y auténtico, goza de eficacia especial como medio de prueba, tiene fuerza ejecutiva, y el original siempre es conservado por el notario".

"El notario es independiente en el ejercicio de su función e imparcial en el asesoramiento que presta y en la redacción de los documento a fin de facilitar la igualdad de las partes y el equilibrio del contrato que celebran ".

"El notario insurre en su responsabilidad disciplinaria y está sujeto a responsabilidad civil y penal en el ejercicio de su profesión ".

"La fnalidad de la profesión notarial, como consecuencia de su asesoramiento imparcial, del control de la legalidad de los actos en que interviene y del carácter público y auténtico del documento del que es autor, es la de dar a los sujetos de derecho seguridad jurídica en sus relaciones privadas y, con ello, prevenir los litigios judiciales ".

La función notarial es una cuestión de seguridad jurídica, dado que el notario interviene en nombre del Estado otorgando el sello de su garantía.

Eventualmente podría intervenir en nombre de la Unión Europea, o de otros conjuntos supranacionales, incluso, globales, y, en su nombre, otorgar garantía y seguridad.

En un mercado global, con unas comunicaciones globales, el comercio, para que sea global, no solo ha de basarse en la aplicación de las nuevas tecnologías de la información y las comunicaciones, sino que necesita disponer de mecanismos de garantía y seguridad, técnica y jurídica, también globales.

En este contexto convergen el comercio, las nuevas tecnologías, la seguridad y el derecho y destilan tres conceptos contratación, fe pública y firrna digital que han de redefinirse, recíprocamente interrelacionarse y, de forma integrada, crear una RED MUNDIAL DE CONFIANZA, respaldada por las legislaciones de cada país y normas técnicas compatibles, construida sobre lo que se conoce como "entidades de certificación", en las que la concepoión notarial en el que inspira el notariado latino podría tener un papel esencial.

3.- UNA VISIÓN GLOBAL.

Los sistemas de firmas digitales y las demás funciones de las entidades que prestan servicios de confianza están razonablemente resueltas por lo que se refiere a una asociación asegura de una clave a una persona determinada, pero no está exento de debate la forma en la que se certifica a la entidad de certificación, esto es, "quien certifica al certificante".

Para ello existen procedimientos inspirados en líneas jerárquicas o verticales, mediante los que una entidad superior de confianza certifica a la inferior, y, otros inspirados en líneas horizontales o de reconocimiento recíproco entre entidades de confianza.

Adoptar una u otra puede tener sus ventajas y sus inconveniente.

La eficacia, rapidez y simplicidad de los sistemas jerárquicos o verticales chocan con la complejidad y lentitud de los sistemas horizontales o de reconocimiento recíproco.

Dado el marco global en el que se desenvuelve el proyecto EMERITUS, y por exigencia del punto 5 de los principios en los que se inspira, se debe definir y construir una TSI global "que no amenace la soberania, la seguridad o la economia de ninguna nación ", por lo que, desde el punto de vista internacional parece más adecuado un sistema de reconocimiento mutuo u horizontal, que parece que garantizaría más la no amenaza a la soberanía, la seguridad o la economías nacionales e incluso, permitiría, por lo que a servicios de confianza se refiere, situar en un plano

de igualdad a las naciones concordante con los principios del derecho internacional.

La eficacia, rapidez y simplicidad de la verticalidad o sistema jerárquico tal vez sería aconsejable para los sistemas de ámbito nacional, donde, además, existiría una autoridad u organismo público encargado por velar en este ámbito de actividad.

Con lo que estaríamos en un sistema global de reconocimiento de confianza mixto, basado en los dos principio: jerárquico en lo nacional y horizontal en lo internacional.

El sistema de reconocimiento recíproco internacional podría tener un añadido de verticalidad en la medida que el reconocimiento viniese no de un ente superior, distinto de los miembros nacionales que lo integran, sino de un ente superior integrado por todos y cada uno de los miembros que lo integran y donde funcionaria la regla de la unanimidad.

Todo ello hace determinante un diseño preciso y minucioso del G.T.S.U., T.S.As., y de sus políticas de certificación, y en las que la figura del Notario, en su concepción latina, podría ser una importante fuente inspiradora de solución.

4.- CONCLUSIÓN.

Como conclusión y sin pretender abordar las mútiples matizaciones que requeriria una red mundial de confianza, la histórica existencia del notariado ejerciendo función de tercero de confianza parece señalar el camino de por donde deben orientarse las soluciones a los problemas que plantea las entidades de certificación para la efectiva implantación de un sistema de firma electrónica.

No obstante, y como hemos señalado, las diferencias que separan los dos sistemas fundamentales de notariado, el latino y el sajón, invitan a profundizar el la búsqueda de sus concordancias, superar sus diferencias y, abordar de este modo, la construcción de un sistema notarial universal, capaz

de dar confianza en las sociedades del Tercer Milenio, en las que la firma electrónica tendrá un papel relevante.

BIBLIOGRAFÍA:

-Pirenne, "Historie des institutions et du droit rrivé de láncien Egypte. Bruselas, 1932-1935.

-Gimenez Arnau, E., "Derecho Notarial", Edit. EUNSA,

-Carrascosa López, V., y otros, "La contratación informática: el nuevo horizonte contractual", Edit. Comares, Granada, 1.997.

-Martinez Nadal, A.,"Comercio electrónico, firma digital y autoridades de certificación", Edit. CIVITAS, Madrid, 1.998.

-Ribas Alejandro, J., Edit. Aranzadi, Pamplona, 1.998.

-Barriuso Ruiz, C., "La contratación electrónica", Edit. DYKINSON, Madrid, 1.998.

-Molina Mateos, J.M., "Seguridad, información y poder", Edit. INCIPIT, 1.994.

-FESTE (Fundación para el Estudio del Seoreto en las Telecomunicaciones), fondo documental.