La Firma Digital y Entidades de Certificación

JOSÉ CUERVO ÁLVAREZ

Doctor en Derecho

INTRODUCCIÓN

La incorporación de las nuevas tecnologías de la información hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades. El avance de su implantación en todas nuestras actividades ha provocado cambios de tal magnitud que podemos afirmar que la sociedad actual está inmersa en la era de la revolución informática. Este avance no es sólo cuantitativo, sino de algo más importante, que podemos acceder a todo tipo de información y obtener con ello el beneficio correspondiente.

La información ha sido calificada como un auténtico poder de las sociedades avanzadas, ya tenía su importancia en la antigüedad, pero con el desarrollo de la telemática su valor ha crecido de forma tal que se dirige a un futuro prometedor para unos e incierto para otros.

El comercio, como dice DEL PESO NAVARRO [1], pionero en innovaciones jurídicas introducidas en el pasado por medio de la costumbre, una vez más toma la delantera e innumerables transacciones económicas se vienen realizando a través de los medios electrónicos, sin más soporte legal que el pacto entre las partes.

La contratación electrónica en su más puro sentido, poco a poco se viene abriendo paso y crece de forma espectacular. Una vez más los hechos caminan delante del Derecho, entendiendo éste como Derecho positivo.

Muchas veces sucede que cuando tratamos de reconducir estos nuevos hechos a las figuras jurídicas existentes nos encontramos con dificultades. Las viejas instituciones jurídicas que, a través de los siglos han ido incorporando nuevas realidades sociales, cuando tienen que hacerlo respecto a estas nuevas tecnologías, en cierto modo chirrían y las admiten con reservas. Así ocurre cuando tratamos de adaptar el concepto de firma, tal como antiguamente se concebía, al nuevo campo de las transferencias electrónicas.

El objetivo que se pretende con el presente trabajo es introducirnos dentro del tema del documento informático, en el de la firma y su autenticación y su importancia a efectos probatorios del documento en sí, haciendo un breve repaso de su aceptación nacional e internacional y de las futuras autoridades de certificación de las firmas digitales.

1. FIRMA ANALÓGICA (MANUSCRITA)

Siguiendo a CARRASCOSA LÓPEZ[2], podemos indicar que en Roma, los documentos no eran firmados. Existía una ceremonia llamada

[1] Emilio del PESO NAVARRO . "Resoluciones de Conflictos en el intercambio electrónico de documentos", en Ámbito jurídico de las tecnologías de la información. Cuadernos de Derecho Judicial. Escuela Judicial/Consejo General del Poder Judicial. Madrid. 1996, pág. 196.

[2] Valentín CARRASCOSA LÓPEZ. "Valor probatorio del documento electrónico". Revista Informática y Derecho 8, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 133 y ss.

manufirmatio, por la cual, luego de la lectura del documento por su autor o el *notarius*, era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir esta ceremonia se estampaba el nombre del autor.

En el Sistema Jurídico Visigótico existía la confirmación del documento por los testigos que lo tocaban (*chartam tangere*), signaban o suscribían (*firmatio, roboratio, stipulatio*). La firma del que da el documento o librador es corriente, pero no imprescindible. Los documentos privados son, en ocasiones, confirmados por documentos reales. Desde la época euriciana las leyes visigodas prestaron atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escrituras. La "*subscriptio*", representaba la indicación del nombre del signante y la fecha, y el "*signum*", un rasgo que la sustituye si no sabe o no puede escribir. La "*subcriptio*" daba pleno valor probatorio al documento y el "*signun*" debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, éste es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido.

En la Edad Media, la documentación regia viene garantizada en su autenticidad por la implantación del sello real. Sello que posteriormente pasó a las clases nobles y privilegiadas.

La firma es definida en la doctrina como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto.

Valentín CARRASCOSA LÓPEZ, Marcelo BAUZA REILLY y Audilio GONZÁLEZ AGUILAR. "El derecho de la prueba y la informática. Problemática y perspectivas". Revista Informática y Derecho 2, UNED, Centro Regional de Extremadura, Mérida, 1991, págs. 49 y ss.

Valentín CARRASCOSA LÓPEZ, Mª A. POZO ARRANZ y E. P.. RODRÍGUEZ DE CASTRO. "La contratación informática: El nuevo horizonte contractual. Los contratos electrónicos e informáticos". Editorial Comares S.L., Granada, 1997, págs. 55 y 56.

La Real Academia de la Lengua define la firma como: "nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice".

En el Vocabulario Jurídico de COUTOURE se define como :"Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice.

1.1. CARACTERÍSTICAS DE LA FIRMA

De las anteriores definiciones se desprenden las siguientes características:

identificatíva: Sirve para identificar quién es el autor del documento.

declarativa: Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

probatoria: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

1.2. ELEMENTOS DE LA FIRMA

Hemos de distinguir entre:

Elementos formales

Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la firma.

- La firma como signo personal

La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma

manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

- El *animus signandi*

Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar, como señala el profesor LARRIEU[3].

Elementos funcionales

Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

- Identificadora

La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado.

La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones.

La firma manuscrita expresa la identidad, aceptación y autoría del firmante. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido -falsificado- y en el caso de que no exista la firma autógrafa parece que ya no exista otro modo de autenticación[4]. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.

[3] J. LARRIEU. "Les nouveaux moyens de preuve: pour ou contre l'identification des documents informatiques à des escrits sous seing privé". Cahiers Lamy du droit de l'informatique, novembre 1988.

[4] Miguel Ángel DAVARA RODRÍGUEZ. "De las Autopistas de la Información a la Sociedad Virtual", Aranzadi, 1996.

- Autenticación

El autor del acto expresa su consentimiento y hace propio el mensaje. Destacando:

- Operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado.

- Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo.

1.3. ASPECTOS LEGALES

La firma acredita la autoría del documento subscrito normalmente al pie del mismo y representa la formalización del consentimiento y la aceptación de lo expuesto, y es por tanto origen de derechos y obligaciones.

La firma será válida siempre que no sea falsificada o se haya obtenido con engaño, coacciones o de cualquier otro ilícito proceder.

Algunos artículos del Código Civil se refieren a la firma:

Artículo 688 sobre el testamento ológrafo.
Artículo 695 al hablar del testamento abierto.
Artículo 706 y 707 referidos al testamento cerrado.
Artículo 709 sobre testamento de personas que no se pueden expresar verbalmente.
Artículo 1.223 sobre escritura defectuosa por falta en la forma.
Artículo 1.225 al hablar de documento privado.
Artículo 1.226 sobre oposición en juicio de obligación firmada.
Artículo 1.229 referido a nota escrita o firmada por el acreedor.

2. FIRMA DIGITAL (ELECTRÓNICA)

Desde el punto de vista técnico, como alternativa a la firma manuscrita sobre papel se ofrecen las firmas electrónicas y/o digitales.

En el comercio electrónico el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas, que pueden ser remplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica, dentro del que tiene cabida, como categoría particular, el de firma digital.[5]

Las firmas digitales basadas sobre la criptografía asimétrica podemos encuadrarlas en un concepto más general de firma electrónica, que no presupone necesariamente la utilización de las tecnologías de cifrado asimétrico. Aunque, generalmente, varios autores hablan indistintamente de firma electrónica o de firma digital.

Tiene los mismos cometidos que la firma manuscrita, pero expresa, además de la identidad y la autoría, la autentificación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL, PGP, DSA, LUC, etc.), técnicas de sellamiento electrónico y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe (no es constante), pero que la hace absolutamente inimitable como no se tenga la clave privada con la que está encriptada, verdadera atribución de la identidad y autoría[6].

- [5] Apolonia MARTÍNEZ NADAL. "Aproximación al borrador de propuesta de directiva para un marco común en materia de firma electrónica y proveedores de servicios relacionados", Actualidad Informática Aranzadi nº 29, octubre de 1.998

- [6] Carlos BARRIUSO RUIZ. "La contratación electrónica", Madrid, Dykinson, 1998, pág. 50

Para Y. POULLET[7] la firma electrónica supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.

Para DEL PESO NAVARRO[8] es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina fedatario electrónico o telemático que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, sino también jurídica.

Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. En este concepto amplio y tecnológicamente indefinido de firma, tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (p. ej. la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje. Por ello de forma adecuada, el art. 2.1 de la propuesta de Directiva sobre firma digital, define la firma electrónica como aquella firma en forma digital puesta sobre unos datos, o añadida o asociada lógicamente a los mismos, y utilizada por el firmante para indicar la aprobación por parte del firmante del contenido de estos datos y cumpliendo ciertos requisitos.[9]

Las firmas electrónicas o digitales consisten básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la

- [7] Citado por Valentín CARRASCOSA LÓPEZ. "La contratación informática:..." , obra ya citada, pág. 70.
- [8] Emilio del PESO NAVARRO, obra ya citada, pág. 224.
- [9] Apolonia MARTÍNEZ NADAL, obra ya citada

identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la confidencialidad.

La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no violación del secreto.

Los criptosistemas de clave pública, son los más idóneos como firma digital, están basados en el uso de un par de claves asociadas: una clave privada, que se mantiene en secreto, y una clave pública, libremente accesible por cualquier persona. Este par de claves esta matemáticamente relacionado de tal forma que sólo con la clave pública correspondiente a la clave privada utilizada para firmar puede verificarse el mensaje firmado; además técnicamente son muy resistentes, se calcula en miles de siglos la duración media que tardaría el ordenador más potente para poder romper la clave. Su mecanismo de seguridad se basa sobre todo en el absoluto secreto de las claves privadas, tanto al generarse como al guardarse y en la certificación de la clave pública por la autoridad certificadora.

Entre los objetivos de la firma electrónica está el conseguir una universalización de un estándar de firma electrónica.

2.1. CARACTERÍSTICAS DE LA FIRMA ELECTRÓNICA

De las anteriores definiciones podemos destacar las siguientes características:

- Debe permitir la identificación del signatario. Entramos en el concepto de "autoría electrónica" como la forma de determinar que una persona es quien dice ser.

- No puede ser generada más que por el emisor del documento, infalsificable e inimitable.

- Las informaciones que se generen a partir de la signatura electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.

- La posible intervención del Notario Electrónico mejora la seguridad del sistema.

- La aposición de una signatura debe ser significativa y va unida indisociablemente al documento a que se refiere.

- No debe existir dilación de tiempo ni de lugar entre aceptación por el signatario y la aposición de la signatura.

El artículo 2.1 de la propuesta de Directiva sobre firma electrónica, además de definir el concepto de firma electrónica, indica que se deben cumplir los siguientes requisitos:

- está vinculada únicamente al firmante

- es capaz de identificar al firmante

- está creada de un modo o utilizando un medio que está únicamente bajo el control del firmante

- está vinculada a los datos a los que se refiere de tal forma que si los datos son alterados la firma electrónica es invalidada

2.2. ASPECTOS LEGALES

2.2.1. En Estados Unidos

A finales de la década de los setenta, el gobierno de los Estados Unidos publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles pero no clasificados. El 16 de abril de 1993, el gobierno de los EE.UU. anunció una nueva iniciativa criptográfica encaminada a proporcionar a los civiles un alto nivel de seguridad en las comunicaciones: proyecto Clipper. Esta iniciativa está basada en dos elementos fundamentales:

-Un chip cifrador a prueba de cualquier tipo de análisis o manipulación (el Clipper chip o EES (Escrowed Encryption Standard) y

-Un sistema para compartir las claves secretas (KES -Key Escrow System) que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.[10]

En EE.UU. es donde más avanzada está la legislación sobre firma electrónica, aunque el proyecto de estandarización del NIST (The National Institute of Science and Technology) no lo consiga. El NIST ha introducido dentro del proyecto Capstone, el DSS (Digital Signature Standard) como estándar de firma, si bien todavía el gobierno americano no ha asumido como estándar su utilización. El NIST se ha pronunciado a favor de la equiparación de la firma manuscrita y la digital.[11]

La ley de referencia de la firma digital, para los legisladores de los Estados Unidos, es la ABA (American Bar Association), **Digital Signature Guidelines**, de 1 de agosto de 1996.

El valor probatorio de la firma ha sido ya admitido en Utah, primer estado en dotarse de una Ley de firma digital. La firma digital de Utah (**Digital Signature Act Utah** de 27 de febrero de 1995, modificado en 1996) se basa en un "Criptosistema Asimétrico" definido como un algoritmo que proporciona una pareja de claves segura.

Sus objetivos son, facilitar el comercio por medio de mensajes electrónicos fiables, minimizar la incidencias de la falsificación de firmas digitales y el fraude en el comercio electrónico.

▪ [10] Jorge DÁVILA MURO, José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ. "Control gubernamental en la protección de datos: proyecto Clipper", X años de encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1997, págs 25 a 50.

▪ [11] Jorge DÁVILA MURO, José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ, obra ya citada, pág. 39.

La firma digital es una transformación de un mensaje utilizando un criptosistema asimétrico, de tal forma que una persona que tenga el mensaje cifrado y la clave pública de quien lo firmó, puede determinar con precisión el mensaje en claro y si se cifró usando la clave privada que corresponde a la pública del firmante.

Esta ley establece la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen ciertas existencias; una de las exigencias es que la firma digital sea verificada por referencia a una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia.

El Estado de Utah ha redactado un proyecto de ley (**The Act on Electronic Notarization**) en 1997.

California define la firma digital como la creación por ordenador de un identificador electrónico que incluye todas las características de una firma válida, aceptable, como :

- única
- capaz de comprobarse
- bajo un solo control
- enlazándose con los datos de tal manera que si se cambian los datos se invalide la firma
- adoptada al menos como un standard por dos de las organizaciones siguientes:

- The International Telecommunication Unión.
- The American National Standards Institute.
- The Internet Activities Board.
- The National Institute of Science and Technology.
- The International Standards Organization.

Podemos hacer referencia a:

ABA, Resolution concerning the CyberNotary: an International computer-transaction specialist, de 2 de agosto de 1994.

The Electronic Signature Act Florida ,de mayo de 1.996 que reconoce la equivalencia probatoria de la firma digital con la firma manual. En esta ley se usa el término de *"international notary"* en vez del *"cybernotary"* utilizado en otras leyes de EE.UU.

The Electronic Commerce Act, de 30 de mayo de 1997, que hace referencia al *cybernotary.*

The Massachusetts Electronic Records and Signatures Act, de 1996, que acoge todo mecanismo capaz de proporcionar las funciones de las firma manuscrita sin ceñirse a un tipo concreto de tecnología.

2.2.2. En Europa

La Comisión Europea está abocada a armonizar los reglamentos sobre Criptografía de todos sus estados miembros. Hasta el momento, sólo algunos países disponen de leyes sobre firma digital y/o cifrado:

En España

La legislación actual y la jurisprudencia, son suficientemente amplias para acoger bajo el concepto de firma y de escrito a la firma digital y a cualquier otro tipo de firma. Cierto es que por razones de seguridad y para ofrecer mayor confianza en los usuarios y jueces que a la postre deben juzgar sobre la firma digital, una reforma de ley cuyo objetivo fuera equiparar la firma manuscrita a cualquier otro medio de firma que cumpliera las mismas finalidades, sería una medida positiva[12]

[12] Rosa JULIÁ BARCELÓ. "Firma digital y Trusted Third Parties: Iniciativas reguladoras a nivel internacional", Encuentros sobre Informática y Derecho 1997-1998,

El artículo 3 del RD. 2402/1985, de 18 de diciembre, al regular los requisitos mínimos de las facturas, no exige que se firmen. Bien es verdad que nuestro Código de Comercio no exige, por regla general, para una eficacia del contrato o de la factura, la firma ni ningún otro signo de validez, si bien muchos ordenamientos jurídicos requieren que los documentos estén firmados en forma manuscrita -de puño y letra- en orden a solemnizar la transacción o a efectos de su consideración como un documento privado. Creemos no existe inconveniente alguno en admitir la posibilidad de una firma electrónica.[13]

La Circular del Banco de España 8/88 de 14 de Junio creando el reglamento del Sistema Nacional de compensación electrónica, se convirtió en pionera y marcó un hito para la protección y seguridad necesaria en la identificación para el acceso a la información, al indicar que la información se cifrará, para que las entidades introduzcan un dato de autentificación con la información de cada comunicación, a lo que se le reconoce a este método el **mismo valor** que el que posee un **escrito firmado** por personas con poder bastante.[14]

El artículo 45 de la Ley 30/1992 de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común incorporó el empleo y aplicación de los medios electrónicos en la actuación administrativa, de cara a los ciudadanos. Para su regulación, el Real Decreto 263/1996 de 16 de febrero, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación legal de la "firma electrónica"..

Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, pág. 225.

- [13] Mª del Pilar PERALES VISCASILLAS. "La factura electrónica". Actualidad Informática Aranzadi nº 24, julio de 1997.

- [14] Carlos BARRIUSO RUIZ, obra citada, pág. 253

En Alemania

La ley de firma digital regula los certificados de las claves y la autoridad certificadora. Permite el seudónimo, pero prevé su identificación real por orden judicial. A la firma electrónica se la define como sello digital, con una clave privada asociada a la clave pública certificada por un certificador.

La Ley de 19 de septiembre de 1.996 es el primer proyecto de ley de firma digital en Europa. (Entra en vigor el 1 de noviembre de 1997).

En Francia

La nueva Ley de Telecomunicaciones y disposiciones sobre uso interior de cifrado

En Italia

La Ley de 15 de marzo de 1997 número 59, es la primera norma del ordenamiento jurídico italiano que recoge el principio de la plena validez de los documentos informáticos.

El reglamento aprobado por el Consejo de Ministros el 31 de octubre de 1997, si bien para el efectivo reconocimiento del valor jurídico de la documentación informática y de las firmas digitales será necesario esperar a que sea operativo en virtud de la emanación de los posteriores e indispensables reglamentos técnicos de actuación.

Se define la firma digital como el resultado del proceso informático (validación) basado en un sistema de claves asimétricas o dobles, una pública y una privada, que permite al suscriptor transmitir la clave privada y al destinatario transmitir la clave pública, respectivamente, para verificar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos (artículo 1° apartado b). En el reglamento la

firma digital está basada exclusivamente en el empleo de sistemas de cifrado llamados asimétricos.

El art. 2 del Reglamento italiano establece que los documentos informáticos serán válidos y eficaces a todos los efectos legales si son acordes a las exigencias del Reglamento; en concreto, el art. 10.2 equipara la firma digital sobre un documento informático a la firma escrita en soporte papel; y el art. 11.1 establece que los contratos realizados por medios telemáticos o informáticos mediante el uso de la firma digital según las disposiciones del reglamento serán válidos y eficaces a todos los efectos legales; pero téngase en cuenta que el art. 8 establece que cualquiera que pretenda utilizar la criptografía asimétrica con los efectos del art. 2 debe conseguir un par de claves adecuado y hacer pública una de ellas a través del procedimiento de certificación efectuada por un certificador.[15]

Regulan la Ley y el Reglamento entre otras cosas: La validez del documento informático; el documento informático sin firma digital; el documento informático con firma digital; los certificadores; los certificados; autentificación de la firma digital; el *"cybernotary"*; los actos públicos notariales; la validación temporal; la caducidad, revocación y suspensión de las claves; la firma digital falsa; la duplicidad, copia y extractos del documento; y la transmisión del documento.

Esta basada esta normativa en soluciones extranjeras y supranacionales.

En Reino Unido

Hay un vivo debate sobre la posible reglamentación de los Terceros de Confianza -TC . Existe un proyecto de ley sobre firma digital y Terceros de Confianza.

[15] Apolonia MARTÍNEZ NADAL, obra ya citada.

En los Países Bajos

Se ha creado un organismo interministerial encargado del estudio de la firma digital.

En Dinamarca , Suiza y Bélgica

Preparan proyectos de ley sobre firma digital.

En Suecia

Organizó una audiencia pública sobre la firma digital en 1997.

En la Comunidad Europea

El artículo 6 del Acuerdo EDI de la Comisión de la Comunidades Europeas, que determina la necesidad de garantía de origen del documento electrónico, no regula la firma electrónica.

No obstante PERALES VISCASILLAS[16] cree que no existe inconveniente alguno en admitir la posibilidad de una firma electrónica apoyada en las siguientes circunstancias:

1. La fiabilidad de la firma electrónica es superior a la de la firma manuscrita.

2. La equiparación en el ámbito comercial internacional de la firma electrónica y la firma manuscrita

3. En el contexto de las transacciones EDI es habitual la utilización de la conocida como "firma digital" que se basa en "algoritmos simétricos" en los que ambas partes conocen la misma clave o en "algoritmos asimétricos" en los que, por el contrario, cada contratante tiene una clave diferente.

[16] Mª del Pilar PERALES VISCASILLAS, obra ya citada.

En el mismo sentido Isabel HERNANDO[17] refiriéndose a los contratos-tipo en EDI indica que si los mensajes EDI se transmiten mediante procedimientos de autentificación como una firma digital, estos mensajes tendrán entre las partes contratantes el mismo valor probatorio que el acordado a un documento escrito firmado.

La Comisión Europea ha financiado numerosos proyectos (INFOSEC, SPRI, etc.) cuyo objetivo es la investigación de los aspectos técnicos, legales y económicos de la firma digital.

La Comisión Europea hizo pública en octubre de 1.997 una Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones titulada "Iniciativa Europea de Comercio Electrónico", con un subtítulo de "Hacia un Marco Europeo para la Firma Digital y el Cifrado".[18]

En el segundo trimestre del 1.998 se deberán encauzar las propuestas para nuevas medidas, una de las cuales podría ser la elaboración de una Directiva de firma digital.

Lo que pretende la Comisión Europea es encontrar un reconocimiento legal común en Europa de la firma digital, con el objeto de armonizar las diferentes legislaciones antes del año 2000, para que ésta tenga carta de naturaleza legal ante tribunales en materia penal, civil y mercantil, a efectos de prueba, apercibimiento y autenticidad. A efectos de dar cumplimiento a esta previsión, ha salido a finales de 1.998 un borrador de propuesta de directiva sobre firma electrónica y servicios relacionados. Pese a la seguridad ofrecida por la firma digital, el borrador de propuesta de directiva regula la firma electrónica en general, y no sólo la firma digital en particular, en un intento de abarcar otras firmas electrónicas, basadas en

- [17] Isabel HERNANDO. "La transmisión electrónica de datos (EDI) en Europa (Perspectiva jurídica)". Derecho Informático Novática nº 108, marzo-abril 1994,, pág. 74.

- [18] European Commission, Ensuring Security and Trust in Electronic Communication-Towards a European Framework for Digital Signatures and Encryption ,de 8 de octubre de 1997, COM (97) 503.

técnicas distintas de la criptografía asimétrica. Esta tendencia a la neutralidad tecnológica se ha acentuado a medida que se han ido sucediendo las distintas versiones del borrador de directiva, como pone de manifiesto el hecho de que la versión actual defina única y exclusivamente la firma electrónica (art. 2.1), mientras que en el primer borrador existía también una definición de firma digital, en el art. 2.2.; y del par de claves, pública y privada, en los art. 2.4 y 2.5. únicamente al establecer el concepto de elemento de creación de firma (definido, en el art. 2.3, como aquel dato único, como códigos o claves critpográficas privadas, o un elemento físico configurado de forma única, el cual es usado por el firmante para crear una firma electrónica) y elemento de verificación de firma (definido, en el art. 2.4, como aquel dato único, como códigos o claves criptográficas públicas, o un elemento físico configurado de forma única, el cual es usado para verificar una firma electrónica) existe una referencia a la criptografía asimétrica. Esta neutralidad es seguramente conveniente, para dejar abiertas las puertas a desarrollos tecnológicos futuros. Pero, por otra parte, llevada a ese extremo, deja sin resolver, porque no son siquiera abordados, muchos de los problemas planteados actualmente por las firmas digitales, únicas firmas electrónicas seguras hoy día.[19]

Para conseguir una coherencia europea se deberá, sin duda, pasar por el establecimiento de una política europea de control armónica con otras potencias económicas como EE.UU., Canadá y Japón.

2.2.3. A nivel internacional.

En Naciones Unidas

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL) en su 24° periodo de sesiones celebrado en el año 1991 encargó al Grupo de Trabajo denominado sobre Pagos internacionales el estudio de los problemas jurídicos del intercambio electrónico de datos (EDI: Electronic Data Interchange) .

[19] Apolonia MARTÍNEZ NADAL, obra ya citada.

El Grupo de Trabajo dedicó su 24° periodo de sesiones, celebrado en Viena del 27 de enero al 7 de febrero de 1992, a éste tema y elaboró un informe que fue elevado a la Comisión.

Se examinó la definición de "firma" y otros medios de autenticación que se han dado en algunos convenios internacionales. Se tuvo presente la definición amplia de "firma" que se contiene en la Convención de las Naciones Unidas sobre Letra de Cambio Internacionales y Pagarés Internacionales, que dice: *"El término firma designa la firma manuscrita, su facsímil o una autenticación equivalente efectuada por otros medios"*. Por el contrario, la Ley Modelo sobre Transferencias Internacionales de Crédito utiliza el concepto de "autenticación" o de "autenticación comercialmente razonable", prescindiendo de la noción de "firma", a fin de evitar las dificultades que ésta pueda ocasionar, tanto en la acepción tradicional de este término como en su acepción ampliada.

En su 25° período de sesiones celebrado en 1992, la Comisión examinó el informe del Grupo de Trabajo y encomendó la preparación de la reglamentación jurídica del EDI al Grupo de Trabajo, ahora denominado sobre Intercambio Electrónico de Datos.

El Grupo de Trabajo sobre Intercambio Electrónico de Datos , celebró su 25° periodo de sesiones en Nueva York del 4 al 15 de enero de 1993 en el que se trató de la autenticación de los mensajes EDI, con miras a establecer un equivalente funcional con la "firma".[20]

El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL), el 14 de Junio de 1996 en su 29° periodo de sesiones celebrado en Nueva York, examinó y aprobó el proyecto de Ley Modelo sobre aspectos jurídicos de EDI bajo la denominación de Ley Modelo sobre el comercio electrónico. (Resolución General de la Asamblea 51/162 de 16 de diciembre de 1996). El artículo 7 de la Ley Modelo recoge el concepto de firma.

▪ [20] Agustín MADRID PARRA. "EDI (Electronic Data Interchange): Estado de la cuestión en UNCITRAL, Revista de Derecho Mercantil n° 207, enero-marzo 1993.

La Comisión encomendó al Grupo de Trabajo, ahora denominado "sobre Comercio Electrónico" que se ocupara de examinar las cuestiones jurídicas relativas a las firmas digitales y a las autoridades de certificación.

La Comisión pidió a la Secretaría que preparara un estudio de antecedentes sobre cuestiones relativas a las firmas digitales. El estudio de la Secretaría quedó recogido en el documento A/CN.9/WG.IV/WP.71 de 31 de diciembre de 1996.

El Grupo de Trabajo sobre Comercio Electrónico celebró su 31° periodo de sesiones en Nueva York del 18 al 28 de febrero de 1997 que trató de fijar las directrices sobre firmas digitales publicadas por la American Bar Association.

El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, que celebró su 30° periodo de sesiones en Viena del 12 al 30 de mayo de 1997, examinó el informe del Grupo de Trabajo, hizo suyas las conclusiones y le encomendó la preparación de un régimen uniforme sobre las cuestiones jurídicas de la firma numérica y de las entidades certificadoras.[21]

El artículo 7 de la Ley Modelo sobre Comercio Electrónico (LMCE) regula el equivalente funcional de firma, estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos, que nos da un concepto amplio de firma electrónica, indicando "*cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) si ese método es tan fiable como sea apropiado para los fines para los que se creó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acto pertinente*".

[21] Agustín MADRID PARRA. "Firmas digitales y entidades de certificación a examen en la CNUDMI/UNCITRAL". Actualidad Informática Aranzadi n° 24, julio de 1997.

El apartado 3 del proyecto de artículo A del WP.71 indica que "una firma digital adherida a un mensaje de datos se considera autorizada si se puede verificar de conformidad con los procedimientos establecidos por una autoridad certificadora".

En la O.C.D.E.

La Recomendación de la OCDE (Organización para la Cooperación y Desarrollo Económico) sobre la utilización de criptografía (Guidelines for Cryptography Policy) fue aprobada el 27 de marzo de 1997. Esta recomendación no tiene fuerza vinculante y señala una serie de reglas que los gobiernos debieran tener en cuenta al adoptar legislación sobre firma digital y terceros de confianza, con el fin de impedir la adopción de diferentes reglas nacionales que podrían dificultar el comercio electrónico y la sociedad de la información en general.

En la Organización Internacional de Normas ISO

La norma ISO/IEC 7498-2 (Arquitectura de Seguridad de OSI) sobre la que descansan todos los desarrollos normativos posteriores, regula los servicios de seguridad sobre confidencialidad, integridad, autenticidad, control de accesos y no repudio.

A través de su subcomité 27, SC 27, trabaja en una norma de firma digital.

2.3. LEGALIDAD DE LOS DOCUMENTOS CON FIRMA DIGITAL

Se plantea el problema de que algunas legislaciones imponen requisitos de escrito y de firma manuscrita como condición de validez o como condición de pruebas de ciertos contratos y actos jurídicos. En consecuencia, para que desde un punto de vista legal estos contratos sean plausibles, o bien la jurisprudencia debe interpretar el término firma y escrito de forma suficientemente amplia para acoger la firma digital, o bien

debe modificarse la ley tratando de asimilar la firma digital a la firma manuscrita.

Todavía no se ha probado la validez legal de la firma digital en ninguna vista ante los tribunales de justicia, no existiendo por ello las garantías jurídicas plenas para su uso. No obstante, en entornos criptográficos se considera la firma digital con capacidad superior a la manuscrita, ya que no sólo comporta la autenticidad del documento firmado, sino su integridad; o lo que es lo mismo, la certidumbre de que no ha sido alterado en ninguna de sus partes. Actualmente no existe problema legal para el uso de la firma digital por un grupo de usuarios, siempre que éstos firmen "manualmente" un acuerdo previo acerca de su uso en sus transacciones comerciales, así como el método de firma y los tamaños (y valores) de las claves públicas a emplear.[22]

El borrador de directiva comunitaria, igual que algunas de las iniciativas legislativas existentes sobre firma digital, realizan un reconocimiento de los efectos de la misma, equiparándola, con más o menos exigencias, a la firma manuscrita. En efecto, el art. 5.2 establece que los Estados miembros asegurarán que las firmas electrónicas basadas en certificados cualificados emitidos por un proveedor de servicios de certificación, que cumpla los requisitos establecidos en el anexo II:

a) satisfacen las exigencias legales de firma manuscrita.

b) son admisibles como medio de prueba en procedimientos legales de la misma forma que las firmas manuscritas.[23]

- [22] Jorge DÁVILA MURO, José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ, obra ya citada, pág. 40.
- [23] Apolonia MARTÍNEZ NADAL, obra ya citada.

3. AUTORIDAD O ENTIDAD DE CERTIFICACIÓN DE LAS CLAVES

La creciente interconexión de los sistemas de información, posibilitada por la general aceptación de los sistemas abiertos, y las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas principalmente de la digitalización, están potenciando formas de intercambio de información impensables hace pocos años. A su vez, ello está conduciendo a una avalancha de nuevos servicios y aplicaciones telemáticas, con un enorme poder de penetración en las emergentes sociedades de la información. Así, el teletrabajo, la teleadministración, el comercio electrónico, etc., están modificando revolucionariamente las relaciones económicas, administrativas, laborales de tal forma que en pocos años serán radicalmente distintas de como son ahora.

Todos estos nuevos servicios y aplicaciones no podrán desarrollarse en plenitud a no ser que se les dote de unos servicios y mecanismos de seguridad fiables.

Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento a seguir.

Existen diferentes tipos de protocolos en los que intervienen terceras partes confiables (*Trusted Third Party, TTP,* en la terminología inglesa):

Los **protocolos arbitrados.** En ellos una TPC o Autoridad de Certificación participa en las transacción para asegurar que ambos lados actúan según las pautas marcadas por el protocolo.

Los **protocolos notariales.** En este caso la TPC , además de garantizar la correcta operación, también permite juzgar si ambas partes actuarán por derecho según la evidencia presentada a través de los documentos aportados por los participantes e incluidos dentro del protocolo

notarial. En estos casos, se añade la firma (digital) del notario a la transacción, pudiendo éste testificar, posteriormente, en caso de disputa.

Los **protocolos autoverificables.** En estos protocolos cada una de las partes puede darse cuenta si la otra actúa deshonestamente, durante el transcurso de la operación.

La firma digital en sí, es un elemento básico de los protocolos autoverificables, ya que no precisa de la intervención de una Autoridad de Certificación para determinar la validez de una firma.[24]

La Autoridad o Entidad de Certificación debe reunir los requisitos que determine la ley, conocimientos técnicos y experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad. Se debería prever el caso de desaparición del organismo certificador y crear algún registro general de certificación tanto nacional como internacional, que a su vez auditase a las entidades encargadas, y fuese garante en su funcionamiento. Pues aun se carece de normas que regulen la autoridad o entidad de certificación. Para una certificación de naturaleza pública, el Notario, en el momento de suscribir los acuerdos de intercambio y de validación de prueba, puede generar y entregar con absoluta confidencialidad la clave privada.[25]

El documento WP.71 de 31 de diciembre de 1.996 de la Secretaría de las Naciones Unidas indica en su párrafo 44 que las entidades certificadoras deben seguir unos criterios :

- independencia
- recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida

▪ [24] Jorge DÁVILA MURO, José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ. "Autoridades de certificación y confianza digital". Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, pág. 165.

▪ [25] Carlos BARRIUSO RUIZ, obra citada, pág. 131

- experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados
- longevidad
- aprobación del equipo y los programas
- mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente
- existencia de un plan para casos de emergencia (programas de recuperación en casos de desastres o depósitos de claves).
- selección y administración del personal
- disposiciones para proteger su propia clave privada
- seguridad interna
- disposiciones para suspender las operaciones, incluida la notificación a los usuarios
- garantías y representaciones (otorgadas o excluidas)
- limitación de la responsabilidad
- seguros
- capacidad para intercambiar datos con otras autoridades certificadoras
- procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado expuesta).[26]

Las autoridades de Certificación pueden emitir diferentes tipos de certificados:

- Los certificados de Identidad, que son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.
- Los certificados de Autorización o potestad que son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad.
- Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero.

[26] Agustín MADRID PARRA, obra ya citada.

- Los Certificados de Tiempo o estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo.[27]

El Sector de autoridades de certificación, hasta la fecha, está dominado por entidades privadas americanas, aunque ya existen iniciativas propias de la Unión Europea que se circunscriben a las fronteras de sus países de origen, es decir, sin salir a otros Estados miembros.

El término TTP (Tercera Parte Confiable) al que antes nos referíamos nos indican aquellas asociaciones que suministran un amplio margen de servicios, frecuentemente asociados con el acceso legal a claves criptográficas. Aunque no se descarta que las TTP actúen como Autoridades de Certificación (AC), las funciones de ambas se van considerando progresivamente diferentes; decantándose la expresión AC para las organizaciones que garantizan la asociación de una clave pública a una cierta entidad, lo que por motivos obvios debería excluir el conocimiento por parte de dicha Autoridad de la clave privada; que es justamente lo que se supone debería conocer una TTP.[28]

La Comisión Europea distingue entre:

- Autoridades de certificación (AC)

El cometido esencial es "autenticar la propiedad y las características de una clave pública, de manera que resulte digna de confianza, y expedir certificados".

▪ [27] Jorge DÁVILA MUÑOZ, José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ, obra ya citada, "Autoridades de certificación... ", pág. 165.

▪ [28] Arturo RIBAGORDA GARNACHO. "Las Autoridades de Certificación en los nuevos servicios y aplicaciones telemáticas". Jornadas sobre Seguridad en Entornos Informáticos, Instituto Universitario "General Gutiérrez Mellado", Madrid 12 de marzo de 1998.

-Terceros de confianza (TC)

Ofrecen diversos servicios, pudiendo gozar de acceso legitimo a claves de cifrado. Una TC podría actuar como una AC.

Lo que la Comisión pretende es que las legislaciones sobre firma digital y AC/TC de los distintos países miembros:

- se basen en criterios comunitarios.
-delimiten las tareas -certificación o administración de claves- y servicios.
-puedan establecerse prescripciones técnicas comunes para los productos de firma digital, en caso de que las disposiciones nacionales no se reconozcan mutuamente y ello merme el buen funcionamiento del Mercado Interior.
-normas claras en materia de responsabilidades (usuarios frente a AC)
-errores, etc.[29]

3.1. FUNCIONES DE LAS AUTORIDADES DE CERTIFICACIÓN

Las funciones de una Autoridad de Certificación deben ser, entre otras, las siguientes [30]:

- Generación y Registro de claves.
- Identificación de Peticionarios de Certificados.
- Emisión de certificado.
- Almacenamiento en la AC de su clave privada.
- Mantenimiento de las claves vigentes y revocadas.

▪ [29] José de la PEÑA MUÑOZ. "Hacia un marco europeo para la firma digital y el cifrado". Revista SIC, Seguridad en informática y comunicaciones nº 28, febrero 1998.

▪ [30] Jorge DÁVILA MURO, José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ, obra ya citada, "Autoridades de certificación....", págs. 171 a 176.

- Servicios de directorio.

3.2. AUTORIDADES PÚBLICAS DE CERTIFICACIÓN

La estructura y el cuadro de funcionamiento de las autoridades de certificación (*public key infrastructure"* prevén generalmente una estructura jerarquizada a dos niveles: El nivel superior suele estar ocupado por la autoridades públicas , que es la que certifica a la autoridad subordinada, normalmente privada.

En España

Está el Proyecto CERES, en el que participan el MAP, el Consejo Superior de Informática, el Ministerio de Economía y Hacienda y Correos y Telégrafos y contempla el papel de la Fábrica Nacional de Moneda y Timbre como entidad encargada de prestar servicios que garanticen la seguridad y validez de la emisión y recepción de comunicaciones y documentos por medios electrónicos, informáticos y telemáticos.

Se pretende garantizar la seguridad y la validez en la emisión y recepción de comunicaciones y documentos por medios electrónicos, informáticos y telemáticos en las relaciones entre órganos de la Administración General del Estado y otras Administraciones, y entre éstos y los ciudadanos, siguiendo directrices de legislación previa (Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, de 1.992, y Real Decreto 263/1996.

El objetivo de esta autoridad de certificación, con la que otras entidades comerciales de certificación deberán interoperar, requiere el reconocimiento a todos los efectos legales del certificado digital, algo que aún no se contempla en nuestra legislación.

Los servicios que está previsto ofrecer son:

-Primarios.- Emisión de certificados, archivo de certificados, generación de claves, archivo de claves, registro de hechos auditables.

-Interactivos.- Registro de usuarios y entidades, revocación de certificados, publicación de políticas y estándares, publicación de certificados, publicación de listas de revocación y directorio seguro de certificados.

-De certificación de mensajes y transacciones.- Certificación temporal, certificación de contenido, mecanismos de no-repudio: confirmación de envío y confirmación de recepción).

-De confidencialidad.- Soporte de mecanismos de confidencialidad, agente de recuperación de claves y recuperación de datos protegidos.

Los Notarios y Corredores de comercio, a través de sus colegios respectivos, en un intento de acomodar estatus a los nuevos tiempos virtuales han tomado parte activa en lo relativo a su condición de fedatarios públicos.

En Italia

Parece ser que la autoridad nacional de certificación será la AIPA (*Autorità per l'Informatica nella Pubblica Amministrazione).*

3.3. AUTORIDADES PRIVADAS DE CERTIFICACIÓN

En España

Existen focos privados de actividad, vinculados con la confiabilidad. El más significativo es el denominado ACE (Agencia de Certificación Electrónica) que está formado por CECA, SERMEPA, Sistemas 4B y Telefónica, y es una Autoridad de Certificación corporativa del sistema financiero español.

También existe como Terceros de confianza el Banesto

En Bélgica

Existe el Tercero Certificador llamado Systèeme Isabel, que ofrece servicios certificadores a socios financieros y comerciales.

La Cámara de Comercio unida a la empresa Belsign ha formado un Trusted Third Party en el cual la Cámara de Comercio hace las funciones de Registro y Belsign hace las funciones notariales.

En Estados Unidos

Utah Digital Signature Trust, One So. Main, Salt Lake City, Utah ARCANVS, S.A. Sanders Lane, Kaysville, Utah

En Internet

Existen ciertos servidores en Internet conocidos como "servidores de claves" que recopilan las claves de miles de usuarios. Todos los servidores de claves existentes en el mundo comparten esta información, por lo que basta publicar la clave en uno de ellos para que en pocas horas esté disponible en todos ellos.

En la Comunidad Europea

El borrador de propuesta de directiva encomienda la función de tercera parte de confianza encargada de dar seguridad a las firmas electrónicas, estableciendo un vínculo entre el elemento de verificación y una persona determinada a unas entidades que denomina proveedores de servicios de certificación (opción terminológica comunitaria que pone de manifiesto una voluntad de evitar siquiera la apariencia de atribución de naturaleza pública que sí podrían sugerir otras denominaciones como, por ejemplo, autoridad de certificación). El art. 2.6 del borrador define al proveedor de servicios de certificación como la persona o entidad que emite certificados o proporciona al público otros servicios relativos a la firmas electrónicas; tales servicios pueden ser inherentes al propio certificado y

necesarios (revocación y suspensión en caso de pérdida de la clave privada u otro elemento de firma), otros más bien discutibles (generación de las claves, que el anexo II permite al proveedor, el cual puede también almacenarlas), así como otros complementarios pero igualmente necesarios para la seguridad del sistema de certificados en particular o del comercio electrónico en general.[31]

CONCLUSIONES

En el trabajo se ha tratado de dar una idea de los cambios tan importantes que ha experimentado la firma desde sus orígenes hasta nuestros días y como debemos tratar de adaptar estos cambios a la realidad social y dejar la puerta abierta a otros futuros cambios y otras nuevas tecnologías que sin duda vendrán.

Las nuevas tecnologías de la información y las comunicaciones, unidas a otras técnicas dan fiabilidad al documento electrónico y tratan de lograr una mayor seguridad mediante el desarrollo y extensión de remedios técnicos y procedimientos de control basados en la criptografía. Esta mayor seguridad que se pretende con una adecuación normativa nos conducirán hacia la autenticación electrónica. El miedo que existe a estas nuevas tecnologías de la información no está en la electrónica, ni en las comunicaciones sino a su mala utilización debido a la no formación y adecuación de las personas y medios a la realidad social.

La creación de los fedatarios públicos electrónicos nos llevará a unas garantías superiores en la autenticación de los documentos que circulen a través de las líneas de comunicación, así como la creación de un fichero público de control con mayores garantías de las actuales.

Una única Entidad de Certificación de ámbito universal es inviable, por tanto deberán existir una o varias redes de autoridades nacionales o sectoriales, interrelacionadas entre sí y que a su vez den servicio a los usuarios de sus ámbitos respectivos.

[31] Apolonia MARTÍNEZ NADAL, obra ya citada.

La firma digital, con las garantías[32] exigidas por una cada vez más necesaria seguridad jurídica, puede abrir un prometedor camino que deje en entredicho la eficacia real de la fe pública tradicional. Entre los objetivos de la firma digital está el conseguir una universalización de un estándar de firma electrónica, que podría verse favorecido con la elaboración de una Directiva Comunitaria.

[32] Sóbre garantías de la firma electrónica ver el trabajo sobre el particular de José Luis MORANT RAMÓN y Justo SANCHO RODRÍGUEZ . "Garantías de la firma electrónica de contratos y autenticación de las partes", Encuentros sobre Informática y Derecho 1992-1993, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontifica de Comillas (ICADE), Aranzadi, 1993.

BIBLIOGRAFÍA

ALCOVER GARAU, Guillermo, "*La firma electrónica como medio de prueba (Valoración jurídica de los criptosistemas de claves asimétricas)*", Cuadernos de Derecho y Comercio nº 13, abril 1994, Consejo General de los Colegios Oficiales de Corredores de Comercio, Madrid. págs. 11 a 41.

ALVAREZ-CIENFUEGOS SUÁREZ, José María, "*Las obligaciones concertadas por medios informáticos y la documentación electrónica de los actos jurídicos*", Informática y Derecho nº 5, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994, págs. 1273 a 1298.

ALVAREZ-CIENFUEGOS SUÁREZ, José María, "*Documento electrónico*", Marco legal y deontológico de la Informática, Mérida 19 de septiembre de 1997.

ASÍS ROIG, Agustín de, "*Documento electrónico en las Administración Pública*", en "Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 137 a 189.

BARRIUSO RUIZ, Carlos, "*Interacción del Derecho y la Informática*", Dykinson, Madrid, 1996.

BARRIUSO RUIZ, Carlos, "*Contratación Electrónica*", Marco legal y deontológico de la Informática, UNED Mérida, 17 de septiembre de 1997.

BARRIUSO RUIZ, Carlos, "*La contratación electrónica*", Dykinson, Madrid, 1998.

CAMPS LLUFRIÚ, Mateo; JOYANES AGUILAR, Luis; SANTAELLA LÓPEZ, Manuel "*Aspectos sociojurídicos de la contratación electrónica*", XII Encuentro sobre Informática y Derecho, Instituto de Informática Jurídica

Facultad de Derecho de la Universidad Pontificia Comillas (ICADE), Madrid, 12 de mayo de 1998.

CARRASCOSA LÓPEZ, Valentín; BAUZA REILLY, Marcelo; GONZÁLEZ AGUILAR, Audilio, "*El derecho de la prueba y la informática. Problemática y perspectivas*", Informática y Derecho nº 2, UNED, Centro Regional de Extremadura, Mérida, 1991.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRÍGUEZ DE CASTRO, Eduardo Pedro, "*Valor probatorio del documento electrónico*", Informática y Derecho nº 8, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 133 a 173.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRÍGUEZ DE CASTRO, Eduardo Pedro, "*El consentimiento y sus vicios en los contratos perfeccionados a través de medios electrónicos*", Informática y Derecho nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 1021 a 1037.

CARRASCOSA LÓPEZ, Valentín, "*El documento electrónico o informático*", Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 43 a 46.

CARRASCOSA LÓPEZ, Valentín, "*El documento electrónico como medio de prueba*", en Dogmática penal, política criminal y criminología en evolución de Carlos María Romeo Casabona (ed.), Editorial Comares S.L., Centro de Estudios Criminológicos, Universidad de la Laguna, 1997, págs. 187 a 201.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRÍGUEZ DE CASTRO, Eduardo Pedro, "*La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*", Editorial Comares S.L, Granada, 1997.

CASTAÑO SUAREZ, Raquel, "*El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y*

telemáticas por la Administración General del Estado", X años de encuentros sobre informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1997, págs. 413 a 419.

CAVANILLAS MÚGICA, Santiago, *"Introducción al tratamiento jurídico de la contratación por medios electrónicos (EDI)"*, Actualidad Informática Aranzadi nº 10, enero de 1994.

CAVANILLAS MÚGICA, Santiago, *"Régimen jurídico del intercambio electrónico de datos"*, Encuentros sobre Informática y Derecho 1995-1996, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1996, págs. 103 a 106.

DAVARA RODRÍGUEZ, Miguel Ángel, *"Las telecomunicaciones y las Tecnologías de la Información en la Empresa: Implicaciones Socio-Jurídicas"*, Informática y Derecho nº 1, UNED, Centro Regional de Extremadura, Mérida, 1992, págs. 27 a 39.

DAVARA RODRÍGUEZ, Miguel Ángel, *"El Intercambio Telemático de datos en las transacciones comerciales. Su validez jurídica"*, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 58 a 60. Actualidad Informática Aranzadi nº 14, enero de 1995.

DAVARA RODRÍGUEZ, Miguel Ángel, *"De las Autopistas de la Información a la Sociedad Virtual"*, Aranzadi, 1996.

DAVARA RODRÍGUEZ, Miguel Ángel, *"Manual de Derecho Informático"*, Aranzadi, Pamplona, 1997.

DAVARA RODRÍGUEZ, Miguel Ángel, *"El documento electrónico, informática y telemático y la firma electrónica"*, Actualidad Informática Aranzadi nº 24, Julio de 1997.

DAVARA RODRÍGUEZ, Miguel Ángel, *"La sociedad de la información y el tratamiento de datos de carácter personal"*, Encuentros sobre Informática y

Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, págs. 19 a 32.

DÁVILA MURO, José; MORANT RAMÓN, José Luis ;SANCHO RODRÍGUEZ, Justo, "*Control gubernamental en la protección de datos: proyecto Clipper*", X años de encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1997, págs. 25 a 50.

DÁVILA MURO, José; MORANT RAMÓN, José Luis; SANCHO RODRÍGUEZ, Justo, *"Autoridades de certificación y confianza digital"*, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, págs. 159 a 184.

DOMÍNGUEZ, Agustín, "*Transferencia electrónica de fondos y de datos. Protección jurídica de los datos personales emitidos en una operación de pago electrónico*", Encuentros sobre Informática y Derecho 1992-1993, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1993, págs. 117 a 132.

GALLARDO ORTIZ, Miguel Ángel, "*Criptología; Seguridad Informática y Derecho. Leyes del Ciberespacio*", Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994, págs. 473 a 480.

GALLARDO ORTIZ, Miguel Ángel, "*Firmas electrónicas mediante criptología asimétrica*", Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 19 a 23.

GALLARDO ORTIZ, Miguel Ángel, "*Informatoscopia y tecnología forense*", en "Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 21 a 61.

GÓMEZ, José Manuel, *"PGP 5"*, y World, Año II, número 2, febrero 1998.

GONZÁLEZ AGUILAR, Audilio, *"EDI (Echange Data Informatics): Desafío de una nueva práctica"*, Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994, págs. 555 a 568.

HERNANDO, Isabel, *"La transmisión electrónica de datos (EDI) en Europa (Perspectiva jurídica)"*, Actualidad Informática Aranzadi nº 10, enero de 1994.

HEREDERO HIGUERAS, Manuel, " *Valor probatorio del documento electrónico*", Encuentros sobre Informática y Derecho 1990-1991, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia Comillas (ICADE), Aranzadi, 1991.

JULIÁ BARCELÓ, Rosa, *"Firma digital y Trusted Third Parties: Iniciativas reguladoras a nivel internacional"*, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, págs. 217 a 226.

LARRIEU, J. *"Les nouveaux moyens de preuve: pour ou contre l'identification des documents informatiques à des escrits sous seing privé"*, Cahiers Lamy du Droit de l'Informatique, noviembre 1988, Pantin.

LÓPEZ ALONSO, Miguel Ángel, *"El Servicio EDI y su contratación"*, Informática y Derecho nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 1039 a 1053.

MADRID PARRA, Agustín, *"EDI (Electronic Data Interchange): Estado de la cuestión en UNCITRAL"*, Revista de Derecho Mercantil nº 207 enero-marzo 1993. Madrid, págs. 115 a 149.

MADRID PARRA, Agustín, *"Firmas digitales y entidades de certificación a examen en la CNUDMI/UNCITRAL"*, Actualidad Informática Aranzadi nº 24, julio de 1997.

MARTÍNEZ NOVAL, Apolonia, *"Comentarios y reflexiones críticas. Aproximación al borrador de propuesta de directiva para un marco comùn en materia de firma electrónica y proveedores de servicios relacionados"*, Actualidad Informática Aranzadi nº 29, octubre de 1.998

MELTZER CAMINO, David, "*Comunicado sobre la experiencia obtenida por el Departamento de Ingeniería y Arquitecturas telemáticas de la UPM en el desarrollo de un EDI seguro dentro del proyecto EDISE*", Encuentros sobre Informática y Derecho 1995-1996, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1996, págs. 147 a 152.

MORANT RAMÓN, José Luis y SANCHO RODRÍGUEZ, Justo, "*Garantías de la firma electrónica de contratos y autenticación de las partes*", Encuentros sobre Informática y Derecho 1992-1993, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad de Comillas (ICADE), Aranzadi, Pamplona, 1993, págs. 107 a 115.

MORANT RAMÓN, José Luis; DÁVILA MURO, Jorge; SANCHO RODRÍGUEZ, Justo, "*Registros públicos digitales: el tiempo y su veracidad*", XII Encuentro sobre Informática y Derecho, Instituto de Informática Jurídica Facultad de Derecho de la Universidad Pontificia de Comillas (ICADE), Madrid, 11 de mayo de 1998.

NO-LOUIS Y CABALLERO, Eduardo de, *"Internet, germen de la sociedad de la información"*, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad de Comillas (ICADE), Aranzadi, 1998, págs. 227 a 242.

PEÑA MUÑOZ, José de la, "*Hacia un marco Europeo para la firma digital y el cifrado*", Revista SIC (Seguridad en Informática y Comunicaciones) nº 28, febrero 1998, págs. 28 a 32.

PERALES VISCASILLAS, Mª del Pilar, "*La factura electrónica*", Actualidad Informática Aranzadi nº 24, Julio de 1997.

PÉREZ LUÑO, Antonio-Enrique, "*Manual de informática y derecho*", Ariel Derecho, Barcelona, 1996.

PÉREZ LUÑO, Antonio-Enrique, "*Ensayos de Informática Jurídica*", Biblioteca de Ética, Filosofía del Derecho y Política nº 46, México, 1996.

PESO NAVARRO, Emilio del, "*Resolución de conflictos en el intercambio electrónico de documentos*", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 191 a 245.

POZO ARRANZ, Mª Asunción y RODRÍGUEZ DE CASTRO, Eduardo Pedro, "*Nueva Perspectiva de la contratación ante las modernas tecnologías*", Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 11 y 12.

RIBAGORDA GARNACHO, Arturo, "*Las Autoridades de Certificación en los nuevos servicios y aplicaciones telemáticas*". Ponencia en las Jornadas sobre Seguridad en Entornos Informáticos. Instituto Universitario "General Gutiérrez Mellado", Madrid 9-12 de marzo de 1998.

ROUANET MOSCARDÓ, Jaime, "*Valor Probatorio Procesal del Documento Electrónico*" , Informática y Derecho nº 1, UNED, Centro Regional de Extremadura, Mérida, 1992, págs. 163 a 175.

ZAGAMI, Raimondo, "*La firma digitale tra soggetti privati nel regolamento concernente. Atti, documenti e contratti in forma elettronica*", Il Diritto dell'informazione e dell'informatica. Anno XIII nº 6 novembre-dicembre 1997, Editore A. Giuffré, Milano, págs. 903 a 926.

http://dev.abanet.org/scitech/ec/isc/dsgfree.html. The American Bar Association Section of Science and Technology.

http://www.Banesto.es. Ofrece los servicios de Tercero de Confianza a sus usuarios.

http://www.cohasset.com/elec_filing/pag10.html.

http://www.ilpf.org./digsig/intl.htm. Digital Signature Legislation.

http://www.ispo.cec.be/Ecommerce. *"A European Initiative in Electronic Commerce"*

http://www.itd.umich.edu/ITDigest/0797/news05.html. Digital Signature Laws.

http://www.kriptopolis.com. Criptografía, PGP y seguridad en Internet.

http://www.map.es/csi. Comité Técnico del Consejo Superior de Informática.

http://www.state.ut.us/web/commerce/digsig/dsmain.htm. Utah Digital Signature Program.