Firma digital y trusted third parties

Julia, Rosa

Published in:
XI Encuentro sobre Informatica y Derecho

Publication date:
1998

Document Version
le PDF de l'éditeur

Firma digital y Trusted Third Parties: Iniciativas reguladoras a nivel internacional

ROSA JULIÁ BARCELÓ
Centre de Recherches Informatique et Droit (CRID), Namur, Bélgica
Centre d'Estudis de Dret e Informàtica de les Illes Balears, Palma de Mallorca

I. INTRODUCCION

El uso de la telamática como medio de comunicación aumenta cada día. Diferentes tipos de redes de comunicación, desde redes cerradas hasta internet, son más y más utilizadas para el intercambio de todo tipo de información. Esta nueva realidad recibe diferentes nomenclaturas: en Estados Unidos se habla de la Infraestructura Global de la Información (GII), en Europa de la Sociedad de la Información[1]. Al mismo tiempo, son numerosos los recursos humanos y económicos dedicados a investigar esta nueva realidad (ver más adelante).

En sus inicios, el intercambio de mensajes por medios electrónicos se daba sobre todo en la gran industria y en sus relaciones comerciales con sus proveedores filiales. Posteriormente, con el desarrollo de internet, esta práctica se ha extendido a la pequeña y mediana industria, así como al gran público (consumidores). Hoy en día, la telemática encuentra un importante campo de aplicación en otros sectores: en la Administración Pública, en el Sanitario[2] y en la ejecución de contratos electrónicos sobre bienes sujetos a propiedad intelectual (por ejemplo, bases de datos electrónicas dirigidas al público) e información en general[3].

1. Ver para el caso de Estados Unidos «The National Information Infraestructure: Agenda for Action». En la Unión Europea, ver el llamado Rapport Bangemmann «Europa and the Global Information Society. Recommendations to the European Council.
2. El sector médico genera numerosos flujos electrónicos de datos que se llevan a cabo entre los diferentes actores del mismo: hospitales, laboratorios de análisis clínicos, farmacias, empresas aseguradoras, oficina de la seguridad social, etc. Ver: *Towards Security in Medical Telematics*, Legal and Technical Aspects, Studies in Health Technology and Informatics, N 27, IOS press, Edited by Barber et aliii, 1996, Amsterdam.
3. Dentro de lo que se entiende por comercio electrónico, se va consolidando un nuevo tipo de práctica comercial, consistente en la conclusión y ejecución de licencias de derechos de autor y derechos afines por medios electrónicos. La Unión Europea está promocionando la utilización del Modelo CITED para la elaboración de sistemas «Electronic Copyright Management Systems», los cuales sirven para proveer este servicio. Para más información sobre este tema, ver: HOEREN, T., *The answer to the Machine is in the Machine: technical devices for copyright management in the digital era*, Law, Computers & Artificial Intelligence, vol. 4, núm. 2, 1995, pgs. 175-186; BING, J., *The contribution of Technology to the Identification of Rights, Especially in Sound and Audio-Visual Works: An Overview*, International Journal of Law and Information Technology, vol. 4, núm. 3, 234-267.

El marco legal tradicional de estas actividades está pensado para un escenario «papel», el cual impone requerimientos legales, sobre todo de escrito y de firma manuscrita que ponen en duda la viabilidad legal de estas operaciones jurídicas cuando, en lugar de materializarse en soporte papel, se llevan a cabo por medios electrónicos. En consecuencia este artículo pretende plantear la cuestión de la necesidad de emprender reformas legislativas a nivel comunitario para eliminar estas trabas legales. Para ello, nos proponemos analizar los cuatro siguientes aspectos: Primero, los motivos que pueden justificar una intervención a nivel comunitario sobre la firma. Segundo, si tal iniciativa debe contemplar una técnica específica de firma, como la firma digital, o bien debe legislar en términos neutros. Tercera, mostrar y analizar los proyectos internacionales existentes que contemplan la firma digital. Cuarto, analizar cuál debe ser el contenido de las iniciativas reguladoras a nivel internacional sobre la firma digital y Terceros de confianza[4].

II. NECESIDAD DE INTERVENCION LEGISLATIVA COMUNITARIA: MOTIVOS JURIDICOS

A nivel comunitario se plantea el problema de que algunas legislaciones imponen requisitos de escrito y de firma manuscrita como condición de validez o como condición de prueba de ciertos contratos y actos jurídicos[5]. 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 deben hacerse pactos derogatorios de la ley entre las partes contratantes por medios electrónicos, o bien se hace necesario reformar la ley en aras a asimilar la firma digital a la firma manuscrita.

A su vez, se plantea un problema a nivel de prueba, dado que existen algunas legislaciones europeas (como la alemana) que otorgan mayor valor al medio de prueba documental que a los demás[6]. Por tanto es importante, en aras a someter el juicio a prueba, que el documento electrónico sea clasificado como un medio de prueba documental, en vez de presentarse a prueba a través de un reconocimiento pericial, judicial o declaración de testigos. Dado el estado de la ley, para poder calificar el documento electrónico como prueba documental, la solución una vez más, pasa por la conclusión de pactos (que en algunas legislaciones no están permitidos por considerarse ésta una materia de orden público), o bien por la interpretación judicial amplia de escrito y firma; de lo contrario se necesita una reforma legal. Además, en apoyo de la reforma legal se puede añadir el argumento de la confianza: si una ley reconoce la firma digital como «firma», ello repercutirá en la valoración por todos los actores involucrados en la comunicación electrónica (socios comerciales, consumidores, jueces y tribunales) de la firma digital como medio capaz de hacer prueba.

4. En adelante, utilizaremos de manera indistinta el término Trusted Third Parties y Terceros de confianza.
5. TEDIS-CRID– *The formation of contract by electronic data interchange*, Brussels, 1991.
Dados los límites espacio-temporales de este artículo no podemos referirnos a todas las áreas de derecho que exigen formalidades de escrito y firma. No obstante, queremos señalar que tales requisitos existen en materia contractual (sobre todo en contratos entre consumidores), en medios de pago, en Derecho Administrativo en general, etcétera.
6. LAB– *Proof value of documents held in electronic form*, Meeting of November 1992, Dossier 92/3; BLECHSCHMIDT, R., *The German Basic Electronic Data Interchange Agreement versus the European Model EDI Agreement: Some reflexions on German Law*, The EDI Law Review, núm. 3, 1996, pgs. 107-124.

La exigencia de escrito y de firma manuscrita obedece a que, tradicionalmente se ha atribuido a los mismos el cumplimiento de una serie de funciones: básicamente, la firma manuscrita puesta al final de un texto escrito hace prueba del autor y del contenido del escrito. Por tanto, cumple una función de autentificación del autor y de la integridad del mensaje.

En la Unión Europea, dadas las distorsiones qué estas diferencias legislativas de los Estados Miembros pueden producir en el mercado interior, al poner obstáculos a la libre circulación de productos y prestación de servicios y dada la enorme incidencia económica del comercio electrónico, creemos que se justifica una intervención comunitaria al respecto. En este sentido hay que destacar la reciente comunicación del Comisario Bangemmann y del Comisario Monti titulada «An European Initiative in Electronic Commerce»[7] (12 abril 1997), en la que precisamente se anticipa de manera muy general esta intervención comunitaria.

III. CONTENIDO DESEABLE DE LA LEGISLACIÓN EN MATERIA DE FIRMA

La cuestión es saber si la regulación legal de la firma debiera acoger un concepto amplio de firma, capaz de incluir como tal todo mecanismo susceptible de cumplir las finalidades de la firma manuscrita, o bien si la legislación debiera acoger una concreta tecnología, como la firma digital.

La solución de no optar por una tecnología concreta, presenta la ventaja de protegerse de la posibilidad de que la técnica evolucione de tal modo que ésta devenga obsoleta y las leyes que la regulan sean papel mojado.

De todas formas, desde nuestro punto de vista, sería aconsejable que la iniciativa comunitaria se desdoblara en dos regulaciones diferentes: 1.°) Una regulación armonizadora, que eliminara los obstáculos formales y aquéllos concernientes a la prueba a través de la adopción de un criterio de escrito y de firma suficientemente amplios para acoger la firma digital, así como cualquier otro tipo de firma que cumpla las funciones que tradicionalmente han estado atribuidas a la firma manuscrita. 2.°) Una regulación armonizadora de la firma digital y de los terceros de confianza o Trusted Third Parties, necesarios para hacer operable la firma digital.

Por tanto, puede sostenerse la posibilidad de adoptar un concepto amplio de firma, o incluso, decidir no adoptar legislación al respecto y, además, legislar sobre firma digital y terceros de confianza. Ello daría, como resultado la legalidad de utilizar cualquier tecnología y además reglamentaría la utilización de la firma digital y terceros de confianza[8].

7. El autor no ha podido hacerse con una traducción al español. Una versión en inglés puede obtenerse en la dirección siguiente: http:\\WWW. Banesto. es
8. Véase el documento preparado por la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional, titulado «Planification des Travaux a venir en matiére de commerce electronique: Signatures Numeriques, tiers authentificateurs et questions juridiques connexes», New York, 18-28 fevrier 1997, pg. 8. en el cual se justifica la elección, en el presente informe, de la firma digital en el hecho de que tal opción es mayoritaria; no obstante, la nota alienta al uso de otro tipo de firmas siempre que cumplan las funciones de la firma manuscrita.

Veamos a continuación, desde un punto de vista técnico, cómo las funciones atribuidas al escrito papel y a la firma manuscrita pueden ser cumplidas por la tecnología conocida como firma digital llevada a cabo a través de la utilización de criptosistemas de clave pública y a través de la intervención de Terceros de confianza. Posteriormente, analizaremos las diferentes proposiciones y recomendaciones legales al respecto.

IV. FIRMA DIGITAL Y TERCEROS DE CONFIANZA O TRUSTED THIRD PARTIES

Los criptosistemas de clave pública utilizan una clave privada para encriptar un mensaje a la cual le está ligada una clave pública (disponible al público), utilizada para desencriptar el mensaje. Puesto que la clave pública sólo puede utilizarse para encriptar el mensaje y como la clave privada sólo puede desencriptar el mensaje, el receptor de un mensaje criptado con la llave privada que consigue desencriptar con la clave pública del mismo y el mensaje tiene sentido, puede presumir dos cosas: 1.° Que el mensaje proviene de quien lo ha firmado; 2.° Que no ha sido alterado[9]. Cuando se utiliza el criptosistema de clave pública RSA, este proceso se realiza del siguiente modo[10]: al mensaje electrónico se le aplica una función de *hash* unidireccional, la cual resume el mensaje. A este resumen se le aplica la clave privada del emisor. A este resultado se le denomina «firma». A continuación, se envía el mensaje en claro, juntamente con la firma. El receptor procederá primero a aplicar al mensaje en claro la misma *hash function* que aplicó el emisor. A continuación, el receptor procederá a «verificar la firma», para lo cual aplicará la clave pública del emisor a la firma. El resultado deberá ser un mensaje que deberá coincidir exactamente con el resultado de aplicar la *hash function* al mensaje en claro. Si coinciden, el receptor podrá deducir: 1.°– Que el autor del mensaje es el titular de la llave (autenticidad); 2.°– Que el mensaje no fue alterado (integridad).

No obstante, para lograr tales extremos la firma digital, por sí sola, no es suficiente. En la medida en que la firma digital consiste en dos pares de llaves que no tienen ninguna relación con el concreto sujeto poseedor de las mismas (y que las utiliza para firmar), para que este sistema sea efectivo, es necesario que a los usuarios de un sistema de firma digital, antes de utilizarla, les sea públicamente reconocido que son los titulares de la clave pública, (que junto a la privada) permiten realizar y verificar la firma digital. Ello permitirá evitar que un sujeto pueda firmar con su llave privada pretendiendo ser otro sujeto distinto.

El reconocimiento de titularidad de un sujeto determinado sobre la llave pública en un sistema de redes cerrado (con un número reducido de actores), puede lograrse a través de acuerdos bilaterales[11]. El problema aparece en un sistema abierto, como internet en el que

9. TEDIS– Programme, *Service infrastructure for EDI Security*, Final Report, 1993, Manchester.
10. US Congress, Office of Technology Assessment, *Issue update on Information Security and Privacy in Network Environments*, OTA-BP-ITC-147, Washington, DC, 1995.
11. Pongamos por caso que A, B y C quieren concluir contratos por medios electrónicos y desean utilizar un sistema de firma digital. Para reconocer la clave pública de cada uno, los tres actores podrían reunirse y firmar un acto de reconocimiento de la firma de los demás. Podría incluso acudirse a un notario quien procedería a certificar la firma (o la clave pública en su caso). No obstante, nótese que esta práctica supondría una importante ralentización del comercio electrónico, el cual, precisamente responde a fines de rapidez.

cualquiera puede comunicar con cualquiera. Veremos en el siguiente apartado que la solución viene a través de los llamados Terceros de Confianza o Trusted Third Parties.

Los terceros de confianza tienen la función básica de certificar la identidad de los titulares de un par de llaves que forman la firma digital. Básicamente, esta finalidad global se puede desglosar en varias funciones: Primero, función de registro. Los terceros deben pedir documentos acreditativos de la identidad del titular de la llave. Esta función es desempeñada por la llamada Autoridad de registro. Segundo, función de certificación. Una vez comprobada la identidad, el tercero emitirá un documento electrónico cuyo contenido básico es el de declarar «Fulanito es titular de la llave pública X». Posteriormente, este documento será firmado con la clave secreta del tercero. Estos certificados deberán ser accesibles a todo sujeto receptor de mensajes electrónicos firmados, bien a través de bases de datos *on line*, bien porque cada usuario está obligado a enviarlos juntamente con sus mensajes electrónicos firmados. Esta función es desempeñada por la llamada «Autoridad de Certificación». Tal autoridad debe mantener un repertorio de todos los certificados que están en vigor. Cuando un usuario lo solicite, se debe revocar el certificado (por ejemplo, si el usuario ha perdido su llave privada o le ha sido robada).

Para llevar a cabo tales funciones es imprescindible que los terceros sean verdaderos «terceros» a las operaciones comerciales de base, y sobre todo, merecedores de confianza.

Lo que se acaba de describir hace objeto del standard técnico X509 de la CCITT (Consultative Committe on Telephony and Telegraphy). Esta norma ha sido objeto de diversas versiones, las cuales van progresivamente depurando el contenido de los certificados, haciéndolo más flexible y más apropiado para llevar a cabo las funciones legales que se espera de todo certificado.

Otras funciones importantes: (I) Generación de las llaves: Esta función puede hacerla el usuario, sin embargo, también puede ofrecerla un tercero. Es importante tener en cuenta la longitud de las llaves pues los ordenadores tienen cada vez mayor capacidad para averiguar la llave privada a partir de la pública. Si diez años atrás un ordenador tardaba 100 años para hallar tal llave, en la actualidad el ordenador lo hará en menos tiempo. Consecuentemente, las llaves deben hacerse cada vez con un número mayor de dígitos. (II) *Key Scrow:* Se trata de un mecanismo de obtención de las claves secretas de los usuarios con el fin de evitar comunicaciones secretas de interés estatal (tráfico de armas, terrorismo, etc.) (III) *Time Stamping*. Años atrás, numerosos artículos y estudios pusieron de manifiesto la necesidad de que los terceros de confianza llevaran a cabo funciones «notariales», las cuales consistían en actuar a modo de certificadores del envío y de la recepción de los mensajes, en aras de que, llegado un proceso judicial, una de las partes no pudiera negar haber recibido o enviado un mensaje. Al margen de que consideremos totalmente justificada esta función, pues la necesidad de certificación de la llegada de los mensajes es obvia (piénsese que en un escenario papel tal función es asegurada por la Oficina de Correos y Telégrafos a través de las cartas con acuse de recibo), por motivos desconocidos al autor, esta función, así como la atención de las autoridades al respecto han caído en el olvido[12].

12. Para mayor información sobre esta función ver: TEDIS project-Barents, Gasille & Mout, Trusted Third Parties and Similar Services, 1991, Brussels; TEDIS project –CRIPTOMATIC– *Security in Open environments*, 1993, Manchester; ALCOVER GARAU, G., *La firma electrónica como medio de prueba (Valoración jurídica de los criptosistemas de claves asimétricas)*, Cuadernos de Derecho y Comercio, núm. 13, 1994, pgs. 11-41.

Concluyendo, desde un punto de vista técnico, para que la firma digital como mecanismo técnico cumpla las mismas funciones de la firma manuscrita es necesario que vaya acompañada de la de los medios técnicos necesarios, sean certificados emitidos por terceros de confianza o bases de datos públicas que contengan tales certificados, o ambos, que hagan operable el uso de la firma digital.

V. REGULACION JURIDICA: ESTADO ACTUAL

A nivel de la Unión Europea en la actualidad no existen leyes vigentes que regulen la firma digital y los terceros de confianza o Trusted Third Parties[13], a pesar de los numerosos proyectos comunitarios al respecto y, de las recomendaciones de ámbito internacional (ver más abajo).

Lo que no quiere decir que la firma digital no se utilice ni que los Terceros de confianza no existan. En efecto, el mercado, sensible a la necesidad de este producto, ha creado, por un lado, softwares que fabrican firmas digitales; por el otro, a Terceros de confianza. Todo ello es ofrecido a los usuarios de los medios de comunicación a través de *relaciones contractuales*. Por tanto, los usuarios pueden ya utilizar estos servicios a través de contratos por los cuales el usuario obtiene la certificación bajo pago de una cantidad.

Los bancos son quienes han empezado ofreciendo los servicios de Terceros de confianza a sus usuarios. Así, en España tenemos el caso de Banesto[14]. En Bélgica existe el Tercero Certificador llamado Systèeme Isabel, que ofrece servicios certificadores a socios financieros y comerciales. Otro sector que ha mostrado su interés en desempeñar funciones notariales son las Cámaras de Comercio. También en Bélgica, la Cámara de Comercio, unida a la empresa Belsign (versión belga de Verisign) ha formado un Trusted Third Party en el cual la Cámara de Comercio hace las funciones de Registro y Belsign hace las funciones notariales[15].

La cuestión que se plantea en la actualidad es si sería conveniente establecer un marco legal para los terceros de confianza.

En previsión de ello, a conocimiento del autor, se han llevado a cabo varios proyectos de ley sobre firma y proyectos de ley sobre terceros. También hay que destacar algunas recomendaciones a nivel internacional. Veamos algunas de ellas:

1. En la Unión Europea.

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

13. Ello no quiere decir que no existan disposiciones a nivel de Derecho público que hayan acogido un concepto amplio de firma. A nivel internacional una muestra de legislación sobre firma que acoge todo mecanismo capaz de proporcionar las funciones de la firma manuscrita sin ceñirse a un tipo concreto de tecnología es la «Massachusetts Electronic Records and Signatures Act», de 1996.
14. http:\\WWW. Banesto. es.
15. LENOIR, A., *Reliable organisation identification for EDI*, EDI Trusted Third Parties Workshop, Barcelona, 8-10 February 1995, Spain; BELSIGN Certification Practice Statement, Leuven, 1996.

y terceros de confianza. En 1994 la Dirección General XIII emitió un Libro verde «Green Paper on the Security of Information Systems», con carácter consultivo y que nunca salió a la luz como documento oficial[16]. El Libro Verde recoge las conclusiones a las que llegó el grupo de expertos SOG-IS. Entre ellas está la propuesta de una armonización legal comunitaria en materia de Trusted Third Parties así como en materia de prueba de documentos informáticos.

Ultimamente, la Unión Europea ha aprovechado forums especializados en la materia para anunciar próximas medidas legislativas respecto a Trusted Third Parties. Como hemos anticipado mas arriba, hace apenas una semana, salió una Comunicación de la Comisión Europea (elaborada conjuntamente del Cabinete de Monti y de Bangemmann) titulada «A European Initiative in Electronic Commerce» en la que, entre otros, se anticipa que la Comisión Europea emprenderá medidas legislativas en breve plazo en dos niveles: 1.°– Para evitar los obstáculos legales (exigencia de formalismos) a la realización de contratos electrónicos –incluyendo pagos– y de otros actos administrativos; 2.°– Para regular la firma digital y Trusted Third Parties[17].

A nivel nacional hay que destacar el Proyecto de Ley alemana «German Draft Digital Signature Law» del 19 septiembre de 1996, que fija un marco legal para los Terceros de confianza[18]. Similar enfoque ha sido tomado en el proyecto de ley del Reino Unido, Suiza y Dinamarca (estos tres últimos no han tenido la difusión de la alemana[19]).

2. A nivel internacional.

La Recomendación de la OCDE (Organización para la Cooperación y de Desarrollo Económico)[20] sobre la utilización de criptografía (Guidelines for Cryptography Policy) fue aprobada el 27 de marzo de 1997. Esta recomendación, que, como su nombre indica, es una «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.

Hay que tener en cuenta también las actividades emprendidas por la Organización de las Naciones Unidas para el Desarrollo del Derecho Mercantil (UNCITRAL). Esta organización, una vez adoptada la «Ley sobre Comercio Electrónico» en junio de 1996, se ha comprometido en el estudio de la firma digital y de terceros certificadores, tomando como base los trabajos realizados por la American Bar Association.

16. De manera extraoficial se ha alegado que el motivo por el cual no salió a la luz es por el hecho de que la criptografía es considerada un asunto de seguridad nacional sobre el cual los Estados miembros son soberanos. Precisamente, este es uno de los aspectos que, hasta el momento presente, han frenado cualquier tipo de iniciativa legisladora sobre terceros
17. http://www.ispo.cec.be/Ecommerce.
18. Es interesante observar que este proyecto de ley se limite a fijar el marco legal para los Terceros de confianza sin llegar a solucionar los del tema de los requisitos legales de firma manuscrita y de escrito para llevar a cabo determinados actos jurídicos, así como en materia de prueba.
19. International Technology Newsletter, vol. 14, núm. 2, August, 1996.
20. En adelante OECD.

3. Estados Unidos.

En Estados Unidos la primera ley sobre firma digital, y en concreto sobre terceros, es la llamada «Utah Digital Signature Act», de mayo de 1995. Esta ley establece el marco legal de los Terceros, y ha sido seguida por numerosos proyectos de ley en el ámbito de los distintos estados que forman Estados Unidos. A su vez, hay que destacar la Digital Signature Guidelines llevada a cabo por la American Bar Association con la finalidad de constituir una guía para los legisladores en materia de Trusted Third Parties[21].

Por motivos de tiempo, este artículo no puede abarcar todos los aspectos que cubren la regulación sobre Terceros de cada uno de los proyectos de ley y Recomendaciones mencionadas. Sin embargo, a continuación expondremos las principales líneas argumentales sobre dicha regulación.

VI. NECESIDAD DE UN MARCO LEGAL PARA LA FIRMA DIGITAL Y PARA TRUSTED THIRD PARTIES: ARGUMENTOS PARA SU REGULACION JURIDICA

Como dice la primera recomendación de «Guidelines for Crytography Policy» de la OECD, la regulación de los terceros a pesar de que pueda ofrecerse simplemente por las empresas de seguridad informática mediante relaciones contractuales, o bien mediante regulación legal. En nuestra opinión una regulación legal de los servicios de TTP, de modo que el gobierno otorgara licencias a todos aquellos deseosos de ofrecer los servicios de TTP y que cumplieran los requisitos establecidos por la ley ofrecería las siguientes ventajas: primero, ofrecería un mayor grado de confianza en estos métodos a los actores involucrados en la utilización de la firma digital, así como a los jueces (si llegado el caso, surge un litigio) si están regulados por una ley que imponga ciertos requisitos para ofrecer este servicio. Segundo, proveería un claro marco legal que definiría los deberes y obligaciones de ambos, usuarios y proveedores del servicio. Esto evitaría que el consumidor tuviera que sufrir cláusulas abusivas (por ejemplo, exoneración total o parcial de responsabilidad por negligencia). Tercero, la elección de criterios, que cualquier actor deseoso de llevar a cabo la función de TTP puede cumplir y convertirse en un TTP, juega en favor de la libre competencia y evita la creación de monopolios. Cuarto, tal regulación podría dar como resultado la proliferación de TTP's. Por lo tanto, se daría el resultado positivo de que el usuario podría elegir el TTP que deseara, tal y como se recomienda en la «Guidelines for Crytography Policy» de la OECD.

Dicha regulación debiera cumplir una serie de principios básicos: primero, debe tratarse de una entidad neutral, sin interés alguno en las operaciones de base; segundo, sus servicios deben ser interoperables, de modo que el usuario del TTP X pueda reconocer la firma del usuario del TTP; y, tercero, debe dar lugar a libertad de elección de los Terceros por parte de los Usuarios.

Las condiciones para convertirse en un Trusted Third Party, siguiendo la Utah Law, podrían ser las siguientes: primero, cumplimiento de condiciones financieras capaces de

21. Security Committe, Secction of Science & Technology, Amercian Bar Association, *Digital Signature Guidelines*, 1996.

asegurar posibles responsabilidades; segundo, cumplimiento de las suficientes garantías técnicas; tercero, posesión de las adecuadas licencias de hardware y de software; cuarto, cumplimiento de criterios de calidad de los empleados.

Un aspecto muy importante es la responsabilidad de los Trusted Third Parties. La «Guidelines for Crytography Policy» de la OECD establece como principio que la responsabilidad, sea por medio de contrato, sea por ley, debe ser definida claramente. Desde nuestro punto de vista es inadmisible la exoneración total o casi total de responsabilidad que presentan la mayoría de los actuales servicios de TTP's. Por el contrario, la ley debiera prever una situación de equilibrio que respetara por un lado el derecho de los usuarios a exigir responsabilidades cuando los terceros hayan fallado en las funciones de registro y certificación de sus llaves públicas. Por otro, el nivel de responsabilidad no debiera ser tal que desalentara la prestación de tales servicios por aquellas compañías interesadas.

Consideramos además que debiera contemplarse el mantenimiento de un servicio con el cual los usuarios que hubieran visto sus llaves robadas o perdidas, pudieran cancelar los certificados. Por otro lado, los poseedores de un certificado debieran tener la obligación de notificar la pérdida o robo del certificado en unos plazos convenidos.

VII. SITUACION EN ESPAÑA

A nivel español, podemos hacer varias observaciones generales:

Primero, en materia de contratos, el principio de libertad de forma (Código civil y Código de Comercio) implica la inexistencia general de trabas para formalizar contratos mercantiles. Cierto es que para específicos contratos, los llamados contratos solemnes, la exigencia de forma tiene condición de validez.

Segundo, en materia de Derecho Público, existen provisiones legales que amparan el uso de la firma digital[22].

Tercero, en Derecho de la prueba, en España no se da una peso especial al tipo de prueba documental. Así pues, el documento electrónico, al margen de que efectivamente puede entrar como prueba documental, puede también constituir otro tipo de prueba.

En conclusión, consideramos que la legislación española actual, así como 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.

22. Ver MADRID PARRA, A., *Systems in which the Possibiltiy to Make Use of EDI or other Electronic Means is Considered*, The EDI Law Review, The EDI Law Review, núm. 3, 1996, pgs. 91 y ss.

Al margen de ello, en lo referente a Terceros de confianza, en España no parece hasta el momento presente haber ningún proyecto de ley al respecto. En el supuesto que se emitiera una Directiva Comunitaria, España se vería obligada a incorporarla a la ley interna.