REGULACIÓN DE LA FIRMA ELECTRÓNICA: BALANCE Y PERSPECTIVAS

Pedro Alberto DE MIGUEL ASENSIO *

Publicado en:

Direito da Sociedade da Informaçao, vol. V, Coimbra, Coimbra Editora - Associaçao Portuguesa de Direito Intelectual, 2004, pp. 115-143

ISBN: 972-32-1225-0,

* Catedrático de Derecho internacional privado
Facultad de Derecho
Universidad Complutense de Madrid
E- 28040 MADRID
pdmigue@der.ucm.es

Nota: Los números de las páginas no coinciden con los de la publicación, pero sí es idéntica la numeración de los párrafos, por lo que las citas a este documento pueden ir referidas a los números de los párrafos.

ABSTRACT

The 1999 Directive on electronic signatures establishes a common regulatory framework at European level in a field initially regarded as especially important for the development of electronic commerce. The study covers the requirements and effects of electronic signatures and the appearance of different kinds of signatures. The analysis focuses on the impact of legislation in this field on the evolution of electronic commerce and business models in the Internet.

Keywords: Electronic signatures, Electronic commerce, Internet, European Directive

RESUMEN

Tomando como punto de partida la Directiva sobre firma electrónico de 1999 es objeto de análisis la evolución de las legislaciones sobre firma electrónica en el ámbito de la Unión Europea. Junto con el estudio de los presupuestos y efectos de las firmas electrónicas, recibe especial atención el impacto de la regulación en este sector y de la aparición de diversas modalidades de firmas electrónicas sobre el desarrollo del comercio electrónico en Internet.

Palabras claves: Firma electrónica, Comercio electrónico, Internet, Directiva europea

Pedro A. De Miguel Asensio
"Regulación de la firma electrónica: Balance y perspectivas"
Direito da Sociedade da Informaçao, vol. V, Coimbra,
Coimbra Editora - Associaçao Portuguesa de Direito Intelectual, 2004, pp. 115-143

REGULACIÓN DE LA FIRMA ELECTRÓNICA: BALANCE Y PERSPECTIVAS

SUMARIO: I.- DELIMITACIÓN CONCEPTUAL Y FUNDAMENTOS TECNOLÓGICOS. II.- MODELOS DE REGLAMENTACIÓN. III.- ARMONIZACIÓN EUROPEA: LA DIRECTIVA SOBRE FIRMA ELECTRÓNICA DE 1999. 1. *Servicios de certificación y mercado interior*. 2. *Efectos jurídicos*. 3. *Contenido de los certificados*. 4. *Requisitos y responsabilidad de los proveedores de servicios*. IV. FIRMA ELECTRÓNICA Y DESARROLLO DEL COMERCIO EN INTERNET: UN PRIMER BALANCE. V. FORMACIÓN, VALIDEZ Y PRUEBA DE LOS NEGOCIOS ELECTRÓNICOS. VI. ACTIVIDAD NOTARIAL Y COMERCIO ELECTRÓNICO. VII. ASPECTOS DE PROTECCIÓN Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES. VIII. EFICACIA INTERNACIONAL DE LOS CERTIFICADOS.

I.- DELIMITACIÓN CONCEPTUAL Y FUNDAMENTOS TECNOLÓGICOS

1. Para favorecer el uso de las comunicaciones electrónicas y del comercio electrónico y superar la diversidad normativa entre los Estados miembros en materia de eficacia legal de la firma electrónica y acreditación de los proveedores de servicios de certificación, tuvo lugar la adopción el 13 de diciembre de 1999 de la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica[1]. En tanto que normativa común europea en la materia, su contenido resulta punto de partida obligado. El desarrollo de legislación es esta materia es especialmente importante para las actividades por Internet, pues en redes cerradas es habitual la existencia de acuerdos previos (como los acuerdos electrónicos de intercambio de datos o EDI) que pueden no sólo contemplar el empleo de mecanismos de firma electrónica, sino también incluir pactos que faciliten a prueba plena de las transacciones entre las partes.

2. Conforme al artículo 2.1) Directiva 1999/93/CE, el concepto de firma electrónica comprende "los datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con

[1] *DO* 2000 L 13/12. Para sus antecedentes, *vid.* Propuesta de 13-V-1998 -*COM (1998) 297 final*-, Propuesta modificada de 29-IV-1999 -*COM (1999) 195 final*- y Posición común 28/1999, aprobada por el Consejo el 28 de junio de 1999, con vistas a la adopción de la Directiva, *DO* 1999 C 243/33.

ellos, utilizados como medio de autenticación". Junto a esta definición tan amplia de firma electrónica, se singulariza una modalidad específica de firma electrónica, que se diferencia del resto por la presencia de ciertas características que, al proporcionar una mayor seguridad, resultan determinantes de la atribución por el ordenamiento de una eficacia específica a esta modalidad de firma electrónica, que recibe la denominación de firma electrónica avanzada. Para que una firma electrónica sea considerada avanzada debe reunir los siguientes requisitos: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; y d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.

3. La normativa europea adopta como punto de partida la neutralidad tecnológica, de manera que en principio la existencia de la firma electrónica no se vincula a una tecnología concreta. No obstante, al definir tanto los "datos de creación de firma", es decir los datos únicos que el firmante utiliza para crear la firma electrónica, como los "datos de verificación de firma", menciona de manera expresa que esos datos pueden ser en particular códigos o claves criptográficas, privadas en el caso de los datos de creación y públicas en el caso de los utilizados para verificar la firma electrónica. Las firmas electrónicas generadas mediante criptografía asimétrica o de clave pública reciben la denominación de firmas digitales; es decir, éstas son en puridad sólo un tipo de firma electrónica, caracterizado por el empleo de una determinada tecnología, como en Portugal recoge con claridad las definiciones de firma electrónica y firma digital, contenidas en el artículo 2 del *Decreto-Lei n.º* 290-D/99, que regula la firma digital[2].

Aunque la referencia expresa a las claves criptográficas entre los datos de creación y verificación de firma tiene lugar en la Directiva con carácter meramente enunciativo y no exhaustivo –de manera que no excluye el empleo de tecnologías diferentes que puedan beneficiarse de ese marco normativo-, en la actualidad la criptografía asimétrica o de clave pública (firma digital) constituye la tecnología esencial para proporcionar firmas electrónicas seguras[3], habida cuenta de la ausencia de estándares reconocidos respecto de

[2] Consultado en J.T. Ramos Pereira, *Direito da Internet e comércio electrónico*, Lisboa, *Quid Juris?*, 2001, pp. 37-122.

[3] *Vid.* A. Martínez Nadal, *Comercio electrónico, firma digital y autoridades de certificación*, 3ª ed., Madrid, Civitas, 2001, pp. 41-95

otras posibilidades tecnológicas, como los mecanismos de identificación biométrica[4]. De hecho, el mencionado *Decreto-Lei n.º* 290-D/99 no distingue entre firma electrónica y firma electrónica avanzada como hace la Directiva sino entre firma electrónica (*assinatura electrónica*) y firma digital (*assinatura digital*), de manera que no contempla la posibilidad de desarrollar firmas electrónicas con las características y efectos propias de las avanzadas mediante tecnologías diferentes a la criptografía asimétrica[5], lo que se corresponde con la circunstancia de que la neutralidad tecnológica en la que se basa la Directiva 1999/93/CE es más aparente que real, pues en el estado actual de la técnica únicamente las técnicas de criptografía asimétrica pueden proporcionar las características que se exigen a la firma electrónica avanzada[6].

La criptografía asimétrica o de clave pública que permite el intercambio de información cifrada sin necesidad de que los participantes compartan una clave secreta común fijada previamente[7], representa un desarrollo fundamental para el empleo de la criptografía con fines de aumento de la seguridad para la transmisión y almacenamiento de datos a través de las redes informáticas. La criptografía se basa en un proceso de transformación de los datos en formato ininteligible, que se denomina cifrado y se lleva a cabo a través de algoritmos. La recuperación de los datos en forma legible sólo es posible por medio de un proceso inverso de descifrado, que exige disponer de cierta información secreta, la clave. A diferencia de lo que sucede en la criptografía simétrica o de clave secreta, en la asimétrica, se utilizan pares de claves relacionadas matemáticamente: una pública, que puede ser conocida por todos los usuarios y que se emplea para cifrar mensajes (y para verificar firmas digitales), y otra privada, que debe conocer sólo su titular y que es imprescindible para descifrar mensajes cifrados con la correspondiente clave pública (y para crear firmas digitales que serán

[4] *Vid.* R.R. Jueneman, R.J. Robertson, "Biometrics and Digital Signatures in Electronic Commerce", *JURIMETRICS,* vol. 38, 1998, pp. 427-457, pp. 447-457.

[5] Respecto a que en la transposición en la legislación interna del término firma electrónica avanzada (*assinatura electrónica avançada*) de la Directiva su equivalente está constituido por el término *assinatura digital* del *Decreto-Lei n.º* 290-D/99, *vid.* J.T. Ramos Pereira, *Direito..., op. cit.,* p. 57.

[6] *Cf.* J. Bizer y A. Miedbrodt, "Die digitale Signatur im elektronischen Rechtsverkehr – Deutsches Signaturgesetz und Entwurf der Europäischen Richtlinie", D. Kröger y M.A. Gimmy, *Handbuch zum Internet-Recht*, Berlín, Springer, 2000, pp. 135-163, pp. pp. 154-155.

[7] *Vid.* G. Alcover Garau, "La firma electrónica como medio de prueba (valoración jurídica de los criptosistemas de claves asimétricas)", *CDC*, núm. 13, 1994, pp. 11-41.

verificadas con la correspondiente clave pública). La criptografía, como instrumento de seguridad no está exenta de límites, pues no impide que en determinadas circunstancias terceros no autorizados puedan acceder a los datos e incluso modificar su contenido, por ejemplo, en casos de pérdida, sustracción, revelación ilegítima o averiguación no autorizada de una clave secreta.

4. La firma digital –como modalidad especialmente desarrollada de la firma electrónica- es creada por medio de la clave privada del firmante (que genera una serie ininteligible de números y letras que representa la firma y que es diferente para cada documento que se firma) y es susceptible de ser verificada con la correspondiente clave pública, de modo que puede llegar a garantizar (típicamente con intervención -en particular para la autenticación- de un tercero que presta servicios de certificación) la autenticación e integridad del mensaje, así como su no repudio de origen. La firma digital constituye una aplicación de la criptografía de clave pública esencial en el ámbito de la contratación electrónica en redes abiertas, en la medida en que puede llegar a garantizar, incluso frente a terceros, la autenticidad, la integridad y el no repudio de la información transmitida en transacciones en las que los participantes no se conocen previamente.

El proceso técnico suele incluir el empleo de una función matemática, llamada función *hash*, que aplicando un algoritmo permite obtener una síntesis del mensaje, a partir de la cual no es posible recuperar el mensaje original, si bien aplicando de nuevo esa función a dicho mensaje se obtendrá la misma síntesis, siendo imposible que dos mensajes distintos den lugar a una síntesis idéntica -lo que permite verificar que el mensaje coincide con el original-). Para activar la firma electrónica se dispone típicamente de un soporte o tarjeta de identificación electrónica, accesible mediante la introducción del correspondiente número de identificación personal.

5. En la medida en que la criptografía asimétrica hace posible firmas digitales que proporcionan autenticidad, integridad y no repudio, de manera que pueden resultar tanto o más eficaces que la firma manuscrita en papel, se plantea la necesidad de su reconocimiento jurídico. A este respecto, la posibilidad de que la exigencia legal de firma -típicamente manuscrita- sea satisfecha por medios electrónicos respecto de los mensajes de datos está prevista con carácter general en el artículo 7 de la Ley modelo de la CNUDMI sobre comercio electrónico, según el cual la firma a través de medios

electrónicos será posible "(s)i 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… si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos…"; requisito este último muy flexible que parece ir unido a la admisibilidad de más de una solución. Al aparecer la firma electrónica como instrumento que permite satisfacer tales exigencias, tiende a considerarse equivalente funcional de la firma manuscrita, si bien para ello es imprescindible las claves empleadas y su proceso de generación revistan ciertas garantías: debe tratarse de claves seguras sin que sea posible a partir de la clave pública obtener la clave privada; y el proceso de generación debe asegurar que el par de claves sea único y que no es posible obtener la clave privada reproduciendo el procedimiento de generación[8].

6. Concepto básico en la normativa comunitaria es también el de "certificado", emitido por una tercera parte de confianza, cuya intervención es necesaria cuando la firma electrónica se utiliza en redes abiertas, típicamente entre personas que no se conocen previamente. Ahora bien, la normativa comunitaria junto a la categoría general de certificado, diferencia otra a la que por sus mayores requisitos de seguridad atribuye una especial eficacia. El concepto general de certificado se define en el artículo 2 Directiva 1999/93/CE como "la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta". Junto a la categoría general, el concepto de "certificado reconocido" se reserva para aquellos certificados que cumplen los requisitos establecidos en el anexo I de la Directiva y son suministrados por un proveedor de servicios de certificación que cumple los requisitos establecidos en su anexo II.

Esa tercera parte de confianza, que hace posible la comprobación de la identidad del firmante, mediante la expedición de certificados de firma electrónica recibe la denominación en el artículo 2 Directiva 1999/93 de "proveedor de servicios de certificación" y, conforme a la Directiva puede serlo una entidad o persona física o jurídica y puede prestar otros servicios en relación con la firma electrónica además de la fundamental de expedir certificados.

[8] *Cf., v. gr.,* A. Martínez Nadal, "La firma electrónica como equivalente funcional, espejismo o realidad", *La seguridad jurídica en las transacciones electrónicas*, Madrid, Civitas, 2002, pp. 179-203, pp. 182-183.

II.- MODELOS DE REGLAMENTACIÓN

7. Dentro del ámbito del comercio electrónico y las actividades a través de Internet, el sector de las firmas electrónicas ha sido posiblemente el que ha sido objeto de una regulación más temprana, tanto en el ámbito estatal, como comunitario europeo e internacional. En el ámbito nacional, cabe reseñar que desde 1995 empiezan a proliferar las legislaciones en esta materia que se expanden por todos los continentes, si bien con una viabilidad práctica limitada y que incluso en la Unión Europea varios Estados miembros, como es el caso de Alemania[9], Italia[10], Portugal[11] y España[12] consideraron

[9] Ley sobre firma digital de 22 de julio de 1997 (*Gesetz zur digitalen Signatur -Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste. Artikel 3-*), <*http://www.iid.de/rahmen/iukdg.html*>, pp. 5-10; y Reglamento sobre firma digital de 8 de octubre de 1997 (*Verordnung zur digitalen Signatur*), <*http://www.iid.de/rahmen/sigv.html*>, pp. 1-8. Esta normativa ha sido sustancialmente revisada mediante la entrada en vigor el 22 de mayo de 2001 de una nueva legislación (disponible en <*http://www.netlaw.de*>). Sobre el alcance de la reforma, *vid*. A. Rossnagel, "Das neue Recht elektronischer Signatur", *NJW*, vol. 54, 2001, pp. 1817-1826; y destacando en relación con la normativa anterior que estaba centrada específicamente en la regulación de la firma digital con un estricto control administrativo de las entidades emisoras de certificados, *vid.* J. Bizer y A. Miedbrodt, "Die digitale...", *loc. cit.*, pp. 147-151.

[10] *Regolamento recante criteri e modalità per la formazione, l'archiviazione e la transformazione di documenti con strumenti informatici e telematici* (Decreto del Presidente de la República de 10 de noviembre de 1997, núm. 513), que puede consultarse en *Dir. autore*, vol. LXIX, 1998, pp. 387-395, pp. 391-394. Para un elaborado análisis de esta norma y de las disposiciones de desarrollo de 1999, *vid.* G. Finocchiaro, *La firma digitale (Comentario del Codice Civile) (Scialoja-Branca)*, Bolonia-Roma, 2000.

[11] Decreto-ley 290-D/99, de 2 de agosto de 1999. *Vid.* J.T. Ramos Pereira, *Direito..., op. cit.*, pp. 37-122.

[12] Real Decreto-Ley 14/1999, de 17 de septiembre, sobre la firma electrónica (*BOE* núm. 224, de 18-IX-99). Para un análisis de conjunto, *vid.* A. Martínez Nadal, *La ley de firma electrónica*, Madrid, Civitas, 2000. Pese a las expectativas suscitadas, esta normativa no ha logrado realizar los que sirvieron de base para su adopción y justificaron el excepcional empleo de la figura del Real Decreto-ley, vinculados a la necesidad de facilitar la rápida introducción y difusión de la firma electrónica entre los usuarios con la debida seguridad. Esa extraordinaria urgencia justificó que el RDLFE fuera aprobado semanas antes que la versión definitiva de la Directiva en la materia. Como elemento básico de su desarrollo figura la Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación. Entre las principales carencias del Real Decreto-Ley 14/1999 destaca que el gravoso régimen de responsabilidades, infracciones y sanciones prevista para los prestadores de servicios de certificación ha disuadido a éstos de comenzar a operar hasta que ese marco reglamentario, con un alto contenido técnico esté desarrollado. El sistema instaurado se caracteriza por una excesiva intervención administrativa -por la

necesario legislar sobre la firma electrónica sin esperar a la aprobación de la Directiva comunitaria en la materia.

En lo que se refiere al Derecho comunitario, es fácil comprobar que la Directiva 1999/93 sobre firma electrónica es anterior a la regulación en el Derecho comunitario de la mayor parte de las cuestiones propias del comercio electrónico y de la adaptación del Derecho de los negocios a la sociedad de la información[13], como acredita la posterior regulación de materias como la contratación electrónica, el régimen de responsabilidad de los prestadores de servicios de la sociedad de la información, así como la adaptación de la legislación sobre propiedad intelectual y protección de datos personales.

En el plano internacional, ya la Ley Modelo de la CNUDMI/UNCITRAL sobre comercio electrónico aprobada mediante Resolución de la Asamblea General de Naciones Unidas el 16 de diciembre de 1996 contempla el cumplimiento de los requisitos de firma a través del empleo de medios electrónicos. Desde entonces la elaboración de una régimen modelo de regulación de las firmas electrónicas constituyo una de las prioridades en la labor de la CNUDMI/UNCITRAL, hasta que el 5 de julio de 2001 culminó la elaboración del texto de la Ley Modelo sobre firmas electrónicas de UNCITRAL[14], adoptada el 24 de enero de 2002 mediante Resolución

---

específica eficacia que atribuye el sistema al cumplimiento de ese entramado jurídico-público (la firma electrónica no avanzada y el certificado no reconocido constituyen categorías legales de muy escaso valor práctico)-, el gravoso régimen de responsabilidad de los prestadores de servicios de certificación de los prestadores de servicios y la imposición de cargas o costes que menoscaban el empleo generalizado de la firma electrónica (como la tasa fijada por el reconocimiento de acreditaciones y certificaciones y la obligación de las entidades de evaluación de abonar los gastos originados por la evaluación realizada para su acreditación). También la normativa del Real Decreto-Ley mejoraría si se revisara para tener en cuenta la oportunidad de exigir en ocasiones requisitos adicionales a los prestadores de servicios. Así, si bien el artículo 12.*a*) impone a los prestadores de servicios de emisión de certificados reconocidos "indicar la fecha y la hora en las que se expidió o dejó sin efecto un certificado", sería de interés que se adaptara la normativa para reflejar que también es importante el conocimiento del tiempo en que se firma electrónicamente el mensaje que se quiere verificar, respecto de lo cual en la actualidad no existe mención en los textos legales.

[13] Para el estudio de los diferentes sectores, *vid.* P.A. De Miguel Asensio, *Derecho privado de Internet*, 3.ª ed., Madrid, Civitas, 2002.

[14] Los textos de ambas leyes modelo pueden ser consultados en <*http://www.uncitral.org*>. A escala internacional y directamente influido por el texto de las leyes modelo reseñada y de manera muy especial por la legislación de EEUU, cabe hacer referencia también en el marco de la Organización de Estados Americanos al Proyecto de Normas Interamericanas Uniformes sobre Documentos

de la Asamblea General de Naciones Unidas[15]. El contenido de esta Ley Modelo refleja un creciente consenso internacional sobre la necesidad del empleo de sistemas de acreditación y certificación para la atribución de una eficacia reforzada a las firmas electrónicas.

Además, se trata de una cuestión que ya en los años noventa fue objeto de estudio o regulación por parte de organizaciones internacionales publicas, como la OCDE o privadas como la Cámara de Comercio Internacional (CCI). En particular, la CCI elaboró una recopilación de principios relativos a las firmas digitales, conocido como GUIDEC (*General Usage for International Digitally Ensured Commerce*)[16], que no resulta de aplicación a los contratos de consumo y cuyo objetivo es favorecer la capacidad de la comunidad empresarial internacional para concluir transacciones electrónicas seguras a través de Internet, para lo que incluye una terminología uniforme y un conjunto de requisitos de buenas prácticas (*best practices*)[17], cuyo impacto práctico se ha visto limitado por la proliferación de normas estatales en esta materia.

8. La comparación entre las diversas iniciativas legislativas en esta materia muestra básicamente la existencia de tres modelos diferentes de regulación, según el nivel de intervención[18]. Un primer enfoque se caracteriza por ser reglamentista, al atribuir reconocimiento legal en determinadas circunstancias a una modalidad específica de creación de firma electrónica –basada en el uso de la criptografía asimétrica de clave pública-, regular en detalle los requisitos a los que se subordina el funcionamiento de las entidades de certificación así como su régimen de responsabilidad, atribuir derechos y obligaciones a los titulares de las claves. Ejemplos

---

y Firmas Electrónicas de 3 de octubre de 2001, consultado en *Uniform Law Review*, vol. VI, 2002 (1), pp. 295-319.

[15] Acerca de su elaboración y contenido, *vid.* A. Madrid Parra, "Proyecto de Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Derecho de los Negocios,* núm. 128, 2001, pp. 1-32.

[16] *Vid*. <*http://www.iccwbo.org/home/guidec/guidec.asp*>.

[17] *Vid.* W.F. Fox Jr., "The International Chamber of Commerce's GUIDEC Principles: Private-Sector Rules for Digital Signatures", *The International Lawyer*, vol. 35, 2001, pp. 71-78, pp. 74-78.

[18] Clasificando, según su nivel de intervención, las diferentes legislaciones sobre la firma electrónica, *vid*. B.L. Smith, "The Third Industrial Revolution: Law and Policy for the Internet", *Recueil des Cours de l'Académie de droit international de La Haye.*, t. 282, 2000, pp. 231-464, pp. 338-340; y con referencia detallada a las diferentes iniciativas legislativas existentes en el mundo *vid.* el informe "An Analysis of International Electronic and Digital Signature Implementation Initiatives", consultado en <*http://www.ilpf.org/digsig/analysis_IEDSII.htm*>.

de esta opción son algunas de las normativas aprobadas inicialmente por algunos Estados miembros de la Unión Europea, en particular Alemania e Italia. Asimismo, aunque esa tendencia fue revisada a nivel federal, también algunas legislaciones estatales pioneras en materia de firma electrónica en los EEUU adoptaron como punto de partida de su regulación el régimen específico de las firmas digitales, como fue el caso del Estado de Utah[19].

En el otro extremo, un segundo modelo pretende facilitar en términos generales el empleo de las firmas electrónicas para eliminar dudas y obstáculos acerca de su eficacia, pero sin regular las especificaciones de medidas tecnológicas previstas a ese fin, limitándose a lo sumo a enumerar los requisitos que esas firmas deben satisfacer para ser equiparadas a las incluidas en soportes materiales. Este enfoque minimalista en lo regulatorio, que atribuye particular importancia a la autorregulación, ha sido el adoptado mayoritariamente por los países del ámbito del *common law*, como EEUU[20], Canadá, Australia o Nueva Zelanda. En la legislación federal de EEUU, la *Electronic Signatures in Global and National Commerce Act* de 2000 pretende favorecer el empleo de las firmas electrónicas en el consumo interestatal e internacional, promoviendo la no discriminación y la neutralidad tecnológica; se trata de una regulación escueta y estrictamente respetuosa con el principio de neutralidad tecnológica, a diferencia de las soluciones iniciales de ámbito estatal. Elemento fundamental de la nueva normativa es la regla general de que los documentos electrónicos se consideran equivalentes de los documentos escritos.

Un tercer modelo normativo se encontraría a medio camino entre los dos anteriores y trata de integrar elementos de ambos. De una parte, contempla la eficacia legal de las firmas electrónicas en términos muy amplios y flexibles, pero de otra parte regula de manera detallada los requisitos que deben cumplir ciertas firmas electrónicas a las que se atribuye una eficacia reforzada y que se

---

[19] En concreto su legislación de 1995 (*Utah Code* 46-3-101 y siguientes), modificada con posterioridad.

[20] L. Birnbaum-Sarcy y F. Darques-Lane, "La signature électronique comparación entre les législations française et americaine", *Revue de droit des affaires internationales/ International Business Law Journal RDAI/IBLJ*, pp. 543-553 destacan el contraste entre el planteamiento reglamentista prevalente en la Unión Europea y la situación en EEUU donde la legislación en esta materia atribuye un papel muy relevante a la autorregulación. Asimismo, pero al hilo de la comparación entre la situación en EEUU y en Alemania, S. Fina, "Die rechtliche Gleichstellung von elektronischen Signaturen mit handschriftlichen Unterschriften im Europäischen Gemeinschafstrecht und US-amerikanischen Bundesrecht", *ZfRV*, vol. 42, 2001, pp. 1-9.

vinculan en la práctica con el uso de técnicas de criptografía asimétrica. En principio, la Directiva 1999/93/CE respondería a este modelo, pues su artículo 5.2 prevé que los Estados miembros no negarán eficacia jurídica a la firma electrónica por el mero hecho de que se presente en forma electrónica o por no cumplir los requisitos exigidos para ser considerada una firma electrónica avanzada, lo que promovería la neutralidad tecnológica, deseable para hacer facilitar la eventual eficacia de nuevas tecnologías de firma. Pero, de otra parte, la Directiva incorpora una regulación elaborada de los requisitos de los que depende la operatividad de las firmas electrónicas avanzadas, incluidos los de los certificados reconocidos y los de los proveedores de servicios de certificación que los expiden.

III.- FUNDAMENTOS DE LA ARMONIZACIÓN EUROPEA: LA DIRECTIVA SOBRE FIRMA ELECTRÓNICA DE 1999

1. *Servicios de certificación y mercado interior*

9. El criterio de base en la Directiva 1999/93/CE, de 13 de diciembre de 1999, sobre la firma electrónica[21], es que la prestación de servicios de certificación no puede ser condicionada por los Estados miembros a la obtención de autorización previa (art. 3.1), pero el sistema instaurado en relación con las firmas electrónicas avanzadas atribuye un importante alcance a la intervención administrativa, no sólo por la posibilidad de establecer sistemas voluntarios de acreditación de tales prestadores sino sobre todo porque los Estados miembros han de garantizar la existencia de sistemas de supervisión de los proveedores de servicios, así como determinar la conformidad de los dispositivos seguros de creación de firma con los requisitos previstos en el Anexo III de la Directiva.

Mediante Decisión de 6 de noviembre de 2000[22] la Comisión ha fijado los criterios que deben tener en cuenta los Estados miembros para designar los organismos nacionales responsables de evaluar la conformidad de los dispositivos seguros de creación de firma. Dichos criterios se refieren a los límites al ejercicio de otras actividades por esos organismos y su personal, así como a su independencia, integridad profesional, fiabilidad, competencia

[21] *DO* 2000 L 13/12. Un comentario del articulado de la Directiva se contiene en J.M. Álvarez-Cienfuegos Suárez, *La firma y el comercio electrónico en España (Comentarios a la legislación vigente)*, Navarra, 2000, pp. 25-52.

[22] *DO* 2000 L 289.

técnica, formación, imparcialidad y garantía de confidencialidad y frente a posibles responsabilidades. Se trata, en todo caso, de una normativa que se limita a establecer criterios básicos y deja un amplio margen a las autoridades nacionales en la designación de esos organismos[23].

De la normativa comunitaria de armonización resulta un marco normativo en el que es posible la existencia de divergencias significativas entre las legislaciones de los Estados miembros, por ejemplo, en lo relativo a la posibilidad de establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación (art. 3.2 Directiva 1999/93) y respecto a la facultad de supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales (art. 3.7).

10. El ámbito de aplicación en el espacio de las diversas legislaciones nacionales en materia de firma electrónica adoptadas en transposición de la Directiva 1999/93, se halla directamente condicionado por lo dispuesto en su artículo 4.1 según el cual "(l)os Estados miembros aplicarán las disposiciones nacionales que adopten en cumplimiento de la presente Directiva a los proveedores de servicios de certificación establecidos en su territorio y a los servicios prestados por ellos".

En el marco de la garantía del correcto funcionamiento del mercado interior, un principio fundamental de la Directiva es asegurar que los proveedores de estos servicios puedan llevar a cabo libremente sus actividades transfronterizas dentro de la U.E. Por lo que en línea con el criterio del control en origen y del principio del reconocimiento mutuo propios del mercado interior, el artículo 3 de la Directiva prevé también la prohibición de que los Estados miembros restrinjan la prestación de servicios de certificación en los ámbitos regulados por la Directiva procedentes de otros Estados miembros. Asimismo, la Directiva impone a los Estados la obligación de garantizar que los productos de firma electrónica que se ajusten a

[23] En España la Orden de 21 de febrero de 2000 (*BOE* núm. 45, de 22-II-2000) aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. El órgano competente para acreditar a los prestadores de servicios y certificar los productos es la Secretaría General de Comunicaciones (art. 2.1). El otorgamiento de la acreditación o del certificado de conformidad tiene lugar previa evaluación del prestador o del producto por una entidad de evaluación independiente acreditada por la Entidad Nacional de Acreditación u otra aceptada en la Unión Europea (arts. 3 y 5-10). Acerca de la situación en Francia, *vid.* B. Poidevin, "Le cadre juridique de la certificaction", *Juriscom.net*, 1 de septiembre de 2002, <*http://www.juriscom.net*>, pp. 1-4.

lo dispuesto en ella puedan circular libremente en el mercado interior.

2. *Efectos jurídicos*

11. Aunque la normativa comunitaria de armonización contempla la regulación de las firmas electrónicas en general, a partir de un criterio de neutralidad tecnológica, su regulación detallada se limita a firmas electrónicas que proporcionan un nivel determinado de seguridad[24]. La eficacia atribuida en el artículo 5 Directiva 1999/93 varía decisivamente en función del nivel de fiabilidad de la firma electrónica, desempeñando un papel relevante sobre todo en las firmas digitales la presencia de un certificado de una tercera parte de confianza garante de la identidad del titular de la clave, especialmente si el certificado, el prestador de servicios de certificación y el dispositivo de creación de firma satisfacen determinados estándares de seguridad.

Únicamente respecto de la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma, la Directiva 1999/93 establece la equiparación de efectos con la firma manuscrita así como la obligación de su admisibilidad como prueba en procedimientos judiciales. Mientras que con respecto al resto de las firmas electrónicas que no satisfagan esos requisitos sólo se contempla que no serán privadas de eficacia jurídica por esas circunstancias, pero no se regula la atribución de ninguna eficacia en concreto. Si no concurren tales circunstancias no opera la equiparación que tiene su fundamento en el empleo efectivo de medios técnicos que proporcionan las garantías suficientes. En todo caso, incluso la equiparación de efectos con la firma manuscrita no es obstáculo para que pueda impugnarse la eficacia de la firma electrónica, por ejemplo, si se prueba que no fue consignada por el supuesto signatario[25], o si se acredita que en el caso concreto se ha vulnerado la integridad del mensaje. La aplicación de las soluciones generales sobre vicios del consentimiento en la contratación se impone también cuando la declaración de voluntad afectada por el vicio ha sido firmada electrónicamente.

La equiparación de efectos constituye un avance significativo en la medida en que puede resultar determinante de la posibilidad

[24] *Cf.* U. Blaurock y J. Adam, "Elektronische Signatur und europäisches Privatrecht", *Zeitschrift für europäisches Privatrecht*, 2001, pp. 93-115, p. 95

[25] Sobre estas cuestiones *vid.* J.M. Embid Irujo, "Eficacia de la voluntad suplantada por utilización de firma digital", *RCE*, núm. 14, 2001, pp. 3-18, pp. 9-16.

concluir por vía electrónica aquellos contratos para los que el ordenamiento, marginando el criterio general de libertad de forma, impone la forma escrita como presupuesto de su validez, no sólo como mero requisito *ad probationem*. Pero en las legislaciones de los Estados miembros de la UE la exigencia imperativa de forma escrita como presupuesto de la validez del acuerdo en el ámbito de las obligaciones contractuales resulta excepcional, pues la libertad de forma es el criterio general y la no exigencia del empleo de la firma electrónica avanzada como presupuesto necesario para la celebración de contrato por vía electrónica se ve reforzada por la tendencia a equiparar a los acuerdos celebrados por escrito todos aquellos que consten en formato electrónico y que sean susceptibles de ulterior consulta, como se indicará más adelante.

12. La utilidad de la firma electrónica de cara al empleo como prueba de mensajes de datos electrónicos radica en que su presencia con determinadas garantías es decisiva de la apreciación del valor probatorio del mensaje. En esta línea, en algunas legislaciones se atribuye una específica eficacia probatoria al documento informático que incorpora una firma electrónica con las especificaciones previstas en la normativa. El artículo 5.1 de la Directiva 1999/93/CE recoge que los Estados miembros procurarán que la firma electrónica que satisface los requisitos fijados en esa norma incluye el que sea "admisible como prueba en procedimientos judiciales". El dato fundamental es que, si bien la admisibilidad como prueba y el empleo para su valoración de las normas generales al respecto son predicables en la Directiva de cualquier firma electrónica, tanto si reúne los requisitos para ser considerada avanzada como si no; lo cierto, sin embargo, es que la circunstancia de que se trate de una firma electrónica avanzada, basada en un certificado reconocido expedido por un prestador de servicios de certificación acreditado y producida con un dispositivo seguro de creación de firma certificado, resulta normalmente bastante para probar la identidad del firmante y la integridad del mensaje electrónico firmado, sin perjuicio de que en el caso concreto otros medios de prueba puedan desvirtuar esa conclusión (por ejemplo, mediante la prueba de que no fue en realidad el pretendido signatario quien empleó esa firma electrónica).

En España la legislación establece con carácter general para los contratos electrónicos la admisión como medio de prueba documental de los soportes electrónicos incluso con independencia del empleo de cualquier firma electrónica, pues el artículo 24.2 de la Ley 34/2002 de Servicios de la Sociedad de la Información y

Comercio Electrónico establece, sin distinción, que "el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental". No obstante, el empleo de firma electrónica puede resultar determinante al determinar el valor probatorio de los diversos elementos del contrato en cuestión.

3. *Contenido de los certificados*

13. Para el empleo de las técnicas de criptografía de clave pública, la intervención de terceras partes de confianza, entre las que destacan aquellas que prestan servicios de certificación, resulta necesaria con el objetivo de garantizar la asociación entre un par de claves y una persona determinada así como para una distribución efectiva de las claves públicas: el certificado de un prestador de servicios de certificación vincula una clave pública con una persona concreta, precisando su identidad y asegurando que es el titular de la correspondiente clave privada (necesaria para crear la firma digital que se verifica por otros usuarios con la clave pública correspondiente -y precisa también para descifrar mensajes emitidos con esa clave pública por un tercero-). El certificado expedido por un prestador de servicios de certificación es firmado por éste con su correspondiente clave privada para garantizar frente a terceros (los usuarios que puedan confiar en el certificado) su integridad y su origen, lo que deja sin resolver el problema de quién garantiza la identidad de la autoridad de certificación.

14. Como la plenitud de los efectos jurídicos de la firma electrónica se subordina a que esté basada en un "certificado reconocido" y que haya sido producida por "un dispositivo seguro de creación de firma", (art. 5 Directiva), resulta de interés detenerse en la configuración de estos elementos. La Directiva opta por imponer un contenido imperativo mínimo de los certificados reconocidos, que aparece detallado en su Anexo I: a) indicación de que se expide como certificado reconocido; b) identificación del proveedor de servicios de certificación y del Estado de establecimiento; c) nombre y apellidos o seudónimo del firmante; d) un atributo específico del firmante si es significativo por la finalidad del certificado; e) los datos de verificación de firma -en las firmas digitales, la clave pública, un dato esencial del certificado- que correspondan a los datos de creación de firma bajo control del firmante; f) una indicación relativa al comienzo y fin del período de validez del certificado; g) el código identificativo del certificado; h) la

firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado; i) los límites de uso del certificado, si procede; y j) los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

Conforme a la definición contenida en el artículo 2 de la Directiva 1999/93 CE, firmante es: "la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa". Para que un signatario (persona física) vincule con la firma electrónica a una persona jurídica, una posibilidad es la inclusión en el certificado de la indicación del documento que acredite las facultades del firmante para actuar en nombre de la persona a la que represente. Ahora bien, caben otras posibilidades, como que esa circunstancia conste en el propio documento que se firma. Esta última opción evita dificultades propias de la referencia a las facultades de representación en el certificado, relativas a la eficacia de éste en caso de revocación del poder, a la responsabilidad respecto a la continuada exactitud de la información por parte del prestador de servicios de certificación (que puede tener dificultades para controlar la suerte posterior del poder de representación), o a las consecuencias de la posible descoordinación entre el Registro Mercantil y el contenido del certificado (que puede controlarse mediante la consignación en el certificado de los datos registrales que hagan posible verificar la vigencia de las facultades de representación). Por otra parte, entre las cuestiones relativas a los certificados reconocidos no son objeto de una armonización detallada de la Directiva 1999/93, por lo que existe un mayor margen de apreciación de los Estados miembros, se encuentran la determinación de los supuestos en los que los certificados pierden su vigencia o deben ser suspendidos por los proveedores de servicios, así como los términos en que los prestadores pueden incluir en los certificados límites en cuanto a sus posibles usos.

15. Como requisitos que deben satisfacer los dispositivos seguros de creación de firma, el Anexo III de la Directiva incluye los siguientes. En primer lugar, dichos dispositivos deben garantizar, como mínimo que: a) los datos utilizados para la generación de firma sólo pueden producirse una vez y se mantendrá su secreto; b) existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad; y c) los datos utilizados para la generación de firma pueden ser protegidos por el firmante legítimo contra su utilización

por terceros. En segundo lugar, los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de la firma.

Constituye este Anexo III una enumeración de los objetivos que esos dispositivos han de satisfacer para evitar los principales riesgos asociados al empleo de firmas electrónica, pero en la práctica el logro y la determinación de un nivel adecuado de seguridad con la tecnología actual puede resultar particularmente complejos, pues –conforme al apartado 15 del Preámbulo de la Directiva- los requisitos del Anexo III se refieren únicamente a los dispositivos de creación de firma pero no abarcan la totalidad del sistema en cuyo entorno operan esos dispositivos[26]. Además la evaluación del cumplimiento de esos requisitos por los dispositivos de creación de firma es una tarea atribuida a los organismos designados por cada Estado miembro conforme a los criterios para su designación fijados por la Comisión, conforme al artículo 3.4 de la Directiva 1999/93.

4. *Requisitos y responsabilidad de los prestadores de servicios*

16. Los requisitos exigibles a los proveedores de servicios de certificación aparecen contenidos en el Anexo II de la Directiva, que únicamente se ocupa de aquellos prestadores que expiden certificados reconocidos. Tales proveedores deberán:
a) demostrar la fiabilidad necesaria para prestar servicios de certificación; b) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato; c) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado; d) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido; e) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados; f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos; g) tomar medidas contra la falsificación de certificados y garantizar la confidencialidad durante el proceso de generación de datos de creación de firma; h) disponer de recursos económicos suficientes para operar de

[26] *Cf.* N. Bohm, Ian Brown y B Gladman, "Electronic Commerce: Who Carries the Risk of Fraud?", *Journal of Information Law ans Technplogy,* 2000 (3), <*http://elj.warwick.ac.uk/jilt/00-3/bohm.html*>, pp. 21-29, p. 23.

conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado; i) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado; j) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves; k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios; l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que sólo personas autorizadas puedan hacer anotaciones y modificaciones, pueda comprobarse la autenticidad de la información, los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados.

Pese a que entre los requisitos exigibles a estos prestadores figura garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado, la Directiva no exige el empleo de sellos temporales de la firma de los mensajes, de gran importancia práctica para asegurar el correcto funcionamiento del sistema de certificados[27]. Para la determinación del alcance concreto de estas obligaciones habrá que estar a lo dispuesto en la normativa nacional de transposición que resulte aplicable, por ejemplo, acerca de la cuantía de la garantía por las posibles responsabilidades o del plazo de registro obligatorio de la información relativa a un certificado.

17. Aspecto fundamental para el desarrollo de los servicios de certificación es el régimen de responsabilidad de los prestadores de servicios, que regula el artículo 6 Directiva 1999/93/CE. La responsabilidad de los prestadores que emiten o garanticen certificados reconocidos se impone respecto de "cualquier persona

[27] *Vid*. J.L. Ferrer Gomila y A. Martínez Nadal, "El problema temporal del sistema de certificados en el comercio electrónico", *Revista de la Contratación Electrónica*, núm. 1, 2000, pp. 29-47, pp. 44-47.

que confíe razonablemente en el certificado" y cubre no sólo la conformidad con los requisitos del Anexo I, sino también "la veracidad de toda la información contenida en el certificado" (salvo indicación contraria contenida en el certificado o que las inexactitudes resulten de la información facilitada por el titular del certificado -sólo, en este último caso, si el proveedor demuestra haber actuado con la máxima diligencia al verificar la información-), la garantía de que al expedirse el certificado reconocido obra en poder de su titular "el dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado" y, si el proveedor genera los dispositivos de creación y de verificación de firma "la garantía de que ambos funcionen junta y complementariamente". La responsabilidad sólo se excluye si el proveedor de servicios demuestra que no ha actuado con negligencia[28].

Para proporcionar seguridad a la posición de los proveedores de servicios de certificación y favorecer su desarrollo es de gran importancia que las legislaciones nacionales de transposición de la Directiva establezcan la posibilidad de que todo proveedor pueda consignar en un certificado reconocido límites –que deberán ser reconocibles para terceros- en cuanto a sus posibles usos o en cuanto al valor límite de las transacciones que puedan realizarse con el mismo. Cuando el certificado se emplee para fines o en cantidades que superen esos límites, el proveedor de servicios de certificación no deberá responder de los daños y perjuicios que ese empleo pueda causar.

18. Las reglas especiales sobre responsabilidad del artículo 6 de la Directiva se proyectan de manera muy especial sobre las relaciones entre el proveedor de servicios que expide un certificado reconocido y los destinatarios de mensajes suscritos con ese certificado. Tratándose de la responsabilidad respecto al titular del certificado existe una relación contractual, de manera que se impone

[28] Por ello, en la legislación española resulta cuestionable que el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre la firma electrónica en su artículo 14 agravara el régimen de responsabilidad previsto en la Directiva, al establecer un régimen de responsabilidad semiobjetivo en el que puede ser suficiente para generar responsabilidad el incumplimiento de alguna de las obligaciones del RD-Ley sin necesidad de concurrir negligencia. Por su parte, crítico con un sistema basado sólo en la culpa, por entender que un modelo de responsabilidad objetiva con límites fijados en el certificado bastaría para favorecer el desarrollo de las actividades de certificación y proporcionaría una mayor protección del tráfico, *vid*. G. Alcover Garau, "El Real-Decreto-ley sobre la firma electrónica", *Revista de la Contratación Electrónica*, núm. 1, 2000, pp. 7-27, p. 26.

en principio el recurso a los términos del acuerdo entre las partes -en especial, a las detalladas declaraciones de prácticas de certificación- y a las normas sobre contratos que resulten de aplicación. En la práctica, no es extraño que la exigencia de responsabilidad contractual en este contexto surja al hilo de la diligencia con la que el prestador de servicios de certificación ha cumplido determinadas instrucciones del signatario, por ejemplo, en relación con una eventual revocación por éste del certificado, para lo que las eventuales cláusulas de limitación de responsabilidad incorporadas en el acuerdo (que deben corresponderse con la clase de servicio ofrecido en el caso concreto vinculado con frecuencia al nivel de comprobación de la identidad del suscriptor) resultan de gran trascendencia[29], si bien la eficacia de éstas se subordina a su compatibilidad con el régimen de protección de los consumidores y de las normas sobre condiciones generales de la contratación.

IV. FIRMA ELECTRÓNICA Y DESARROLLO DEL COMERCIO EN INTERNET: UN PRIMER BALANCE

19. Pese a que el sector de la firma electrónica ha sido en la mayor parte de los países uno de los primeros ámbitos del comercio electrónico que ha sido objeto de atención[30] y legislación específica, su desarrollo práctico e impacto en la expansión del comercio electrónico han sido hasta la fecha muy limitados, como ilustra de manera clara la situación en la UE. Entre las causas determinantes de esa situación, se hallan ciertos condicionantes jurídicos, técnicos y económicos que han restringido la implantación de estas técnicas, cuyo empleo sí se ha extendido en mayor medida y ha permitido avances significativos en las relaciones por medios telemáticos entre los ciudadanos y la Administración, para simplificar ciertos trámites y hacer posible su realización por medios telemáticos.

En lo que respecta a las causas del limitado impacto de los sistemas de firma electrónica en el desarrollo del comercio electrónico por Internet cabe destacar lo siguiente. Por una parte, con carácter general, la libertad de forma en la perfección de los contratos se proyecta sobre la contratación electrónica, con independencia de la

[29] *Vid.* M. Jaccard, "Le rôle, le statut et la responsabilité de l'autorité de certification dans la transmission de données signées numériquement", *Les contrats de distribution (Contributions offertes au F. Dessemontet)*, Lausana, 1998, pp. 403-427, pp. 422-423.

[30] *Vid.* C. Kuner, "Rechtliche Aspekte der Datenverschlüselung im Internet", *NJW-CoR*, 1995, pp. 413-420, pp. 413-414.

normativa sobre firma electrónica, que no regula con carácter general los aspectos relacionados con la celebración y validez de los contratos (art. 1 Directiva 1999/93/CE).
Además, sobre todo, la equiparación entre documento escrito –cuando esta circunstancia es determinante para el cumplimiento de algún requisito de forma- y documento electrónico no se subordina al empleo en éste de dispositivos de firma electrónica, lo que determina que la introducción de los costosos mecanismos de firma electrónica avanzada no resulte imprescindible para las transacciones más habituales del comercio electrónico, en el que la prueba y constancia de la existencia y contenido de la transacción y la identidad de los participantes se logra por medios alternativos, que, si bien no proporcionan un nivel de seguridad jurídica equiparable a la firma electrónica avanzada, sí se consideran suficientes para las transacciones cotidianas en redes abiertas.

Asimismo, la difusión generalizada entre los usuarios de Internet de los mecanismos de firma electrónica avanzada previstos en la Directiva 1999/93/CE se ha visto dificultada por la complejidad de los procedimientos establecidos en las legislaciones nacionales, la imposición de un régimen muy gravoso y con intervención administrativa para los prestadores de servicios de certificación, los retrasos en la aprobación de las normas reglamentarias de desarrollo necesarias para la puesta en marcha de estos sistemas, las carencias en los logros de unificación internacional de los estándares aplicados a las firmas y los certificados, y la falta de incentivo e interés por parte de los usuarios de Internet en invertir en sistemas destinados especialmente a proporcionar seguridad a la contraparte[31].

20. Sólo la introducción de cambios estructurales que faciliten la difusión generalizada de mecanismos de firma electrónica pueden hacer posible que la situación se modifique en un plazo corto, de manera que la firma electrónica se convierta en un elemento promotor del comercio electrónico, para lo que sus funciones mantienen un indudable potencial. Un cambio radical a esos efectos vendría representado por la introducción por la Administración de elementos de identificación y firma electrónica en los documentos obligatorios de identificación.

[31] *Vid.* P. Mankowski, "Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?", *NJW*, 2002, pp. 2822-2828, pp. 2826-2827.

En España, el Anteproyecto de Ley de firma electrónica[32], que pretende modificar –ante su escasa difusión práctica- la legislación en la materia, contempla como singular novedad la previsión de incorporación al Documento Nacional de Identidad (DNI) de facilidades de identificación y firma electrónica, previendo expresamente que el DNI electrónico surtirá plenos efectos para la acreditación de la identidad y de los demás datos personales del titular que consten en el DNI. El desarrollo de este instrumento supondría un cambio notable y un aumento de las posibilidades de ciertas actividades a través de Internet, en la medida en que facilitara el conocimiento de la identidad o características personales de quien se encuentra conectado. Este cambio puede aportar más confianza y seguridad para el desarrollo de ciertos modelos de negocio, por ejemplo, al facilitar una vía de comprobación en línea de que quien contrata el acceso a ciertos contenidos reúne las circunstancias personales exigidas –como ser mayor de edad para visualizar ciertos contenidos, cuya difusión entre menores puede incluso estar considerada como un delito-.

V. FORMACIÓN, VALIDEZ Y PRUEBA DE LOS NEGOCIOS ELECTRÓNICOS

21. En la medida en que en materia contractual un ordenamiento jurídico proclama como principio de base –sin perjuicio de la existencia de importantes excepciones- la libertad de forma en materia contractual, una consecuencia admitida de manera generalizada es la posibilidad de celebrar los contratos mediante el intercambio de mensajes electrónicos[33], sin especiales requisitos en cuanto a su formalidad y, por lo tanto, sin necesidad de recurrir al empleo de firma electrónicas. Respecto de los contratos para los que según la legislación nacional rige el principio de libertad de forma –y, por lo tanto, pueden celebrarse, por ejemplo, oralmente-, la admisibilidad de su celebración por medios electrónicos sin especiales formalidades es una consecuencia que resulta

[32] Primer Borrador de 27 de diciembre de 2001 y segundo Borrador de 26 de julio de 2002. Textos consultados en <*http://www.mcyt.es*>. Para un análisis de conjunto sobre los cambios proyectados, *vid*. C. Vattier Fuenzalida, "De nuevo sobre el régimen legal de la firma electrónica (estudio del Anteproyecto de 26 de junio de 2002)", *Actualidad Civil*, núm. 6, 3-9 de febrero de 2003.

[33] Sobre estas cuestiones *vid.* C. Paz-Ares, M.I Saéz Lacave y N. Bermejo Gutiérrez, "La emisión de la declaración de voluntad en Internet", *La seguridad..., op.cit.* pp. 109-127.

necesariamente del artículo 9.1 Directiva sobre el comercio electrónico, según el cual "... Los Estados miembros garantizarán en particular que el régimen jurídico aplicable al proceso contractual no entorpezca la utilización real de los contratos por vía electrónica, ni conduzca a privar de efecto y de validez jurídica a este tipo de contratos en razón de su celebración por vía electrónica".

22. Tradicionalmente la exigencia imperativa de forma escrita como presupuesto de la formación de un contrato ha ido unida al requisito de la firma personal (manuscrita) del aceptante, lo que resultaría determinante de que, con carácter general, el contacto interactivo con una página web a través del teclado o del ratón del ordenador o el mero intercambio de mensajes de correo electrónico no cumplieran por sí solos el requisito de la firma (manuscrita) inherente a la exigencia legal de forma escrita solemne[34], que haría necesario recurrir al mecanismo que expresamente permite en el comercio electrónico satisfacer con toda seguridad, sin tener que recurrir al intercambio físico de los documentos firmados por los contratantes, la forma escrita cuando se exige como presupuesto de la validez del acuerdo: la firma electrónica avanzada, considerada, de conformidad con el artículo 5.1.*a*) Directiva 1999/93/CE, como equivalente (funcional) de la firma manuscrita.

No obstante, el impacto práctico de la firma electrónica se ve afectado por la tendencia a considerar la contratación hecha por escrito cuando tiene lugar mediante cualquier "transmisión efectuada por medios electrónicos que proporcione un registro duradero del acuerdo", como establece para los acuerdos se sumisión expresa a tribunales el artículo 23.3 Reglamento (CE) 44/2001 relativo a la competencia judicial y al reconocimiento y ejecución de decisiones. Este planteamiento ha sido establecido con carácter general en la legislación de algún Estado miembro. En concreto, en España el artículo 23.2 Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico, dispone que: "Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico".

Cuando estas normas resultan de aplicación, tienen como consecuencia que la exigencia legal de forma escrita –a la que suele ir unida el empleo de la firma manuscrita- pueda satisfacerse en el comercio electrónico a través del intercambio de mensajes de correo

[34] *Cf*. S. Ernst, "Der Mausklick als Rechtsproblem- Willenserklärung im Internet", *NJW-CoR*, 1997, pp. 165-167, p. 165.

electrónico o de información con un sitio de Internet, sin necesidad de incorporar mecanismos especiales de firma electrónica, pese a que sólo la firma electrónica avanzada esté legalmente equiparada a la firma manuscrita. La no exigencia de firma electrónica avanzada para que un contrato se considere celebrado por escrito –incluso cuando la ley exija de manera específica esa forma- provoca que la principal utilidad práctica en estos casos de la firma electrónica –y motivo para recurrir a ella- sea su utilidad en la prueba de la existencia, contenido y partes del contrato.

23. Conforme a su artículo 1, al margen de los aspectos relativos a la firma electrónica, la Directiva 1999/93/CE no regula otras cuestiones relacionadas con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislación aplicable, ni afectan a las normas y límites que rigen el uso de documentos. Sus normas, por lo tanto, no afectan tampoco a las funciones atribuidas a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos. Por lo tanto, en principio no altera ciertas exigencia legales de los distintos Estados miembros en virtud de las cuales determinados actos y contratos han de constar en documentos públicos, que deben ser autorizados por un notario o empleado público competente, con las solemnidades requeridas por la ley.

No contempla la Directiva 1999/93/CE que la eficacia jurídica de la firma electrónica esté limitada a algunas categorías de actos o negocios jurídicos, si bien su empleo para ciertos actos personalísimos -por ejemplo, en relación con disposiciones testamentarias- puede resultar cuestionable, al tiempo que su eficacia puede quedar subordinada a la fijación segura del momento de otorgamiento del documento. Este dato se relaciona con la tendencia de la armonización internacional a aceptar que las legislaciones nacionales puedan excluir la aplicación del criterio de la equiparación de efectos respecto a ciertas categorías de actos jurídicos, en línea con la tradicional exigencia de especial seguridad, por ejemplo, en el ámbito de las relaciones familiares o sucesorias. Asimismo, la utilización en la práctica de las firmas electrónicas puede resultar condicionada en ciertos países por la exclusión de los contratos que requieran la intervención de un fedatario público del régimen general de admisibilidad de la contratación electrónica (posibilidad que contempla el art. 9.2 de la Directiva 2000/31/CE sobre el comercio electrónico).

24. Con respecto a la evolución de la actividad notarial y su adaptación al comercio electrónico, cabe partir de que si bien los prestadores de servicios de certificación cumplen ciertas tareas próximas a algunas que son propias de la actividad notarial (por ejemplo, comprobar la identidad y circunstancias personales de los solicitantes de certificados y otras relativas al control de las claves), lo hacen con un alcance distinto. En concreto, si bien la asociación entre una persona y su clave privada está garantizada por el sistema de certificación, la autenticación notarial de la firma digital (ya certificada) puede ser relevante para asegurar en el caso concreto la identidad del firmante de una operación, excluyendo el empleo fraudulento de la clave privada.

En España, mediante la Sección 8ª del Capítulo XI de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social[35] se ha introducido un nuevo régimen legal encaminado a regular la atribución y uso de la firma electrónica por parte de los notarios y registradores de la propiedad, mercantiles y de bienes muebles, que constituye un avance significativo con respecto a la situación anterior[36], aunque su aplicación efectiva dependerá del desarrollo reglamentario de esas normas. La mencionada Sección, que lleva por título "Incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva" contempla la obligación de los notarios y registradores mencionados de disponer de sistemas telemáticos para la emisión, transmisión, comunicación y recepción de información, así como de firmas electrónicas con ciertos requisitos específicos que la normativa detalla. Se impone a los notarios y registradores mencionados la obligación de custodiar personalmente sus datos de creación de firma, con prohibición expresa de ceder su uso y obligación de denunciar inmediatamente su pérdida, extravío, deterioro o cualquier situación que pueda poner en peligro "el secreto o la unicidad del mecanismo", de modo que el prestador de servicios de certificación correspondiente pueda proceder inmediatamente a su suspensión o revocación.

Las finalidades básicas a que puede servir el uso de la firma electrónica, en los términos señalados, por parte de los notarios y registradores son relativas a la posibilidad de remisión de documentos públicos notariales, comunicaciones, partes

[35] *BOE* núm. 313, de 31-XII-01.

[36] *Vid.* J. Bolás Alfonso, "Firma electrónica, comercio electrónico y fe pública notarial", *Revista Jurídica del Notariado*, 2000, pp. 31-64 e Instrucción de la Dirección General de los Registros y el Notariado 19 de octubre de 2000 (*BOE* núm. 269, de 9-XI-2000).

declaraciones y autoliquidaciones tributarias, solicitudes o certificaciones por vía electrónica por parte de un notario o registrador. Notable trascendencia práctica debería alcanzar la posibilidad de formalización de negocios jurídicos a distancia, que se admite en la medida en que dos o más notarios se remitan por conducto electrónico, bajo su respectiva firma electrónica avanzada, "el contenido de los documentos públicos autorizados por cada uno de ellos que incorporen las declaraciones de voluntad dirigidas a conformar un único negocio jurídico", si bien la puesta en práctica de esta posibilidad aparece subordinada a que los requisitos para la integración de las declaraciones de voluntad en el negocio unitario y su plasmación en un único documento público se desarrollen reglamentariamente. Asimismo se establece, con carácter general, la posibilidad de que los documentos susceptibles de calificación e inscripción en los mencionados registros sean presentados por vía telemática con la firma electrónica avanzada del notario autorizante. Por último se contempla la admisión expresa de la figura de los instrumentos y documentos públicos electrónicos, que son aquellos redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes. La atribución a estos documentos electrónicos del carácter de documento público, por lo que gozan de fe pública y su contenido se presume veraz e íntegro, resulta de la exigencia de idénticas garantías y requisitos que al resto de los documentos públicos notariales.

VII. ASPECTOS DE PROTECCIÓN Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

25. El artículo 8 Directiva 1999/93/CE establece ciertas normas relativas a la protección de datos personales en relación con los servicios que prestan los proveedores de servicios de certificación, que serán típicamente responsables de ficheros con datos personales de los firmantes. En concreto, el apartado 2 de ese artículo 8 contiene una norma que en parte es expresión de principios relativos a la calidad de los datos recabados y a la legitimación de su tratamiento. En la medida en que la captación y tratamiento de los datos necesarios para la expedición y el mantenimiento del certificado son normalmente necesarios para la ejecución de un contrato en el que el firmante es parte, se comprende que la exigencia de consentimiento expreso del titular de los datos (normalmente, el firmante) sólo se exija en ese artículo 8 cuando los

proveedores de servicios de certificación pretenden obtener y tratar los datos personales con fines distintos a la expedición y mantenimiento del certificado.

26. Además el mencionado artículo 8 recoge con carácter general la aplicación a los proveedores de servicios de certificación de la normativa general sobre protección de datos, en particular, la derivada de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Para el adecuado funcionamiento de los sistemas de firma electrónica resulta normalmente imprescindible que los proveedores de servicios de certificación mantengan un registro de certificados -que típicamente constituirá un fichero de datos personales-, accesible por medios telemáticos para su consulta por los usuarios que hacen uso de los certificados.

Cabe plantearse en este entorno si las normas que imponen restricciones a la transferencia internacional de datos personales pueden condicionar la posibilidad de que la consulta se lleve a cabo desde cualquier país del mundo y de manera muy particular por quien se encuentre en alguno cuyo nivel de protección de datos personales adecuado en los términos del artículo 25 Directiva 95/46/CE. Pese a que en esas circunstancias, normalmente habrá que apreciar que tiene lugar un supuesto de transferencia internacional de datos personales[37], normalmente quedará incluido entre una de las excepciones que determinan la licitud de la transferencia incluso cuando el país de destino no presenta un nivel de protección adecuado. En concreto, cabe entender que en los supuestos típicos esas transferencias se benefician de la excepción en virtud de la cual las transferencias a esos países están liberalizadas cuando son necesarias para la ejecución de un contrato entre el interesado (firmante) y el responsable del tratamiento (proveedor de servicios de certificación).

VIII. EFICACIA INTERNACIONAL DE LOS CERTIFICADOS

27. A escala mundial, las diversas normativas sobre acreditación o certificación de productos y servicios en materia de firma electrónica no garantizan la interoperabilidad de los distintos

[37] En relación con la práctica en España, *vid.* Agencia de Protección de Datos, *Memoria 2001*, Madrid, pp. 72-73.

mecanismos de firma electrónica, debido a la ausencia de criterios comunes. Para el desarrollo de determinadas transacciones internacionales mediante el empleo de firmas electrónicas surge como dificultad añadida la necesidad de garantizar la eficacia en varios países de los certificados emitidos por un proveedor de servicios de certificación. Las legislaciones que únicamente consideran válidas las firmas electrónicas basadas en un certificado emitido por un prestador de servicios de certificación autorizado para operar en el foro son ineficaces al imponer una restricción que a largo plazo menoscaba la posición competitiva y el potencial de las empresas de ese país para el comercio electrónico internacional. Las alternativas contempladas para hacer frente a la eficacia transfronteriza de los certificados en las diversas iniciativas de reglamentación ofrecen un panorama variado, producto de la incertidumbre en este ámbito y de la ausencia de criterios aceptados generalizadamente, lo que determina la dificultad de establecer un régimen internacional, lo que se refleja en el limitado progreso que en la regulación de esta materia representan las disposiciones la Ley Modelo de la CNUDMI/UNCITRAL sobre firmas electrónicas, que dedica a esta cuestión su artículo 12.

Al regular el reconocimiento de certificados y firmas electrónicas extranjeros, la Ley Modelo establece como criterio de partida que la determinación de la eficacia jurídica de un certificado o una firma electrónica no se hará depender del lugar de emisión, creación o uso, ni del lugar del centro de negocios del emisor o del firmante. Se afirma, con carácter general, que la equiparación de efectos con los certificados o firmas nacionales debe admitirse cuando los extranjeros tengan un nivel equivalente de fiabilidad. No obstante, la apreciación de la existencia de ese nivel equivalente se hace depender de lo dispuesto en los estándares reconocidos a nivel internacional o en otros factores relevantes, sin ulteriores precisiones, lo que limita la eficacia práctica de esta norma en la actualidad. Por último, admite también la posibilidad de que las partes se pongan de acuerdo sobre el reconocimiento de eficacia transfronteriza de ciertas categorías de certificados o de firmas –lo que puede ser de especial importancia en redes cerradas-, siempre que esos acuerdos no se hallen prohibidos o carezcan de eficacia conforme a la ley aplicable.

28. Dentro de la Unión Europea, el artículo 7 Directiva 1999/93/CE regula los aspectos internacionales de las firmas electrónicas, si bien en el ámbito intracomunitario las normas básicas aparecen en el artículo 4 que prohíbe a los Estados miembros la posibilidad de establecer restricciones en los ámbitos regulados en la

Directiva a la prestación de servicios de certificación procedentes de otro Estado miembro e impone la obligación de que los productos de firma electrónica que se ajusten a lo dispuesto en la Directiva puedan circular libremente en el mercado interior. Por lo tanto, el artículo 7 sólo contempla el reconocimiento y eficacia de los certificados expedidos por proveedores establecidos en un tercer Estado.

Fuera del ámbito comunitario existe la posibilidad –hasta ahora poco utilizada- de celebrar convenios bilaterales o multilaterales que fijen las condiciones bajo las que tiene lugar el reconocimiento recíproco de la eficacia de estos certificados; pese a la gran eficacia potencial de los convenios internacionales de este tipo, se trata de una posibilidad apenas desarrollada hasta ahora.

El régimen de reconocimiento establecido en el artículo 7 de la Directiva establece un régimen elaborado de control, cuya aplicación práctica no resulta sencilla. Estas normas contemplan la eficacia en los Estados miembros de certificados expedidos por entidades de certificación extranjeras, bajo ciertos controles, que son de dos tipos y operan con carácter alternativo, según se centren en el prestador de servicios de certificación extranjero o en el propio certificado expedido. Cuando el control va referido al prestador de servicios, lo determinante para admitir la eficacia de sus certificados es que el proveedor de servicios establecido en el extranjero satisfaga los requisitos impuestos en la normativa comunitaria para ese tipo de entidades y esta circunstancia haya sido verificada por un organismo de supervisión de un Estado miembro, ante el que se ha solicitado la pertinente acreditación (o autorización, según los ordenamientos). Cuando se trata de controlar directamente los certificados cuya equivalencia de efectos con los de entidades establecidas en algún Estado miembro se pretende, resulta determinante que el certificado del proveedor de servicios extranjero cumpla los requisitos exigidos en el foro y esté avalado que un proveedor de servicios de certificación establecido en la Comunidad. Asimismo, se admite la equiparación de efectos cuando el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales, si bien esta posibilidad está pendiente de desarrollo.