

## **LA FIRMA ELECTRÓNICA EN LA CELEBRACIÓN DEL CONTRATO ELECTRÓNICO A TRAVÉS DE INTERNET\* ENTRE EMPRESAS (B2B)**

• I. Presentación: contrato electrónico y firma electrónica. Carácter internacional, regulación y objeto de estudio .....	2
• II. La firma electrónica como instrumento de seguridad en el contrato electrónico a través de Internet: efectos jurídicos de la firma electrónica .....	4
• 1. Introducción. ....	4
• 2. Perspectiva tecnológica de la Firma electrónica: Respuestas de la criptografía asimétrica. La Firma digital. ....	5
• 3. Perspectiva Jurídica: Regulación de la firma electrónica y de la firma digital .....	7
• 3.1. Clases de Firma Electrónica: la “simple” y la “avanzada” .....	7
• 3.2. Modalidades de Certificados: el “simple” y el “reconocido” .....	7
• 3.3. Los Prestadores de Servicios de Certificación. ....	8
• 3.4. Responsabilidad extracontractual de los Prestadores. ....	8
• 3.5. Efectos Jurídicos de la Firma Electrónica “simple” y “avanzada”. ....	9
• 3.6. Extraterritorialidad de los certificados. ....	10
• 3.7. Protección de Datos Personales. ....	10
• 4. Valoración práctica sobre la utilización de la firma electrónica. ....	10
• III. Firma electrónica y celebración del contrato electrónico: Competencia judicial internacional, Derecho aplicable y forma de celebración .....	11
• 1. Planteamiento .....	11
• 2. Lugar de celebración del contrato electrónico B2B y firma electrónica .....	12
• 2.1. Incidencia del lugar de celebración del contrato electrónico en la determinación de la competencia judicial internacional .....	12
• 2.2. Incidencia del lugar de celebración del contrato electrónico en la determinación del Derecho aplicable a la forma .....	14
• 3. Principio de libertad de forma y firma electrónica: Especial referencia a la compraventa internacional electrónica. ....	14
• 4. Papel de la Firma Electrónica en la expresión de la voluntad de contratar en la contratación electrónica. Especial referencia al Derecho estatal español. ....	16
• IV. Firma electrónica y perfección de los contratos electrónicos B2B: requisitos de la oferta y de la aceptación. ....	17
• 1. Planteamiento .....	17

• 2. ¿Cuándo existe una oferta y cuándo se produce la aceptación en un contrato electrónico B2B? .....	17
• 2.1. Requisitos de la oferta electrónica .....	17
• 2.2. Requisitos de la aceptación electrónica .....	18
• 3. El momento de perfección del contrato electrónico B2B y la firma electrónica .....	19
• V. Incidencia de la Firma electrónica en la prueba del contrato electrónico. ....	21
• 1. Planteamiento .....	21
• 2. Admisibilidad de la firma electrónica y del contrato electrónico como prueba en juicio. ....	21
• 3. ¿Qué se entiende probado a través de la firma electrónica? ...	22
• VI. Supuesto práctico .....	22
• VII. Conclusión .....	23

Realizado por:

Lydia ESTEVE GONZÁLEZ

Richard MAC BRIDE

Directora Académica y

Director Ejecutivo Proyecto UAIPIT.com

\* Este trabajo se inscribe en el Proyecto de investigación financiado por el Ministerio Español de Ciencia y Tecnología “DESISESIC: El Derecho al servicio de la integración de la sociedad y de la empresa en la sociedad de la información y del conocimiento”. Núm. BJU 20010850.

### ***1. Presentación: contrato electrónico y firma electrónica. Carácter internacional, regulación y objeto de estudio*** ➡

Durante mucho tiempo el contrato internacional se ha servido de fórmulas para garantizar la prueba de su existencia. Del pergamino al papel, pasando por otros medios más primitivos, las declaraciones de voluntad lograban permanecer mediante su grafía en los diversos soportes empleados y la firma confirmaba la autoría de tal declaración de voluntad. Hoy en día la informática ha reducido la grafía a unos bits: el soporte ya no es el papel sino un algo electrónico, digital y/u óptico y la firma pasa a ser electrónica y/o digital. En la actual sociedad de la información se celebran millones de contratos internacionales por vía electrónica y a través de Internet, la Red de redes, dando origen a una economía de libre mercado a escala planetaria que ha sido denominada “la nueva economía virtual”<sup>1</sup>, presidida por la figura del contrato electrónico.

Por contrato electrónico entendemos aquél acuerdo de voluntad entre dos o más partes que se formaliza “on line” por vía electrónica y singularmente a través de Internet (correo electrónico u otras aplicaciones, como páginas web)<sup>2</sup>. La firma electrónica, por su parte, es el conjunto de datos en forma electrónica anexos o asociados funcionalmente a otros datos electrónicos, utilizados<sup>3</sup> para identificar formalmente al autor o a los autores del documento que la recoge<sup>3</sup>. Cuando esta firma es generada mediante criptografía

asimétrica<sup>4</sup> se denomina firma digital, siendo ésta, por lo tanto, un tipo de firma electrónica caracterizada por el empleo de una determinada tecnología<sup>5</sup>.

Muchas veces, el contrato electrónico celebrado a través de Internet reviste carácter internacional, porque la naturaleza global de la Red de redes facilita la conexión del contrato con más de un ordenamiento jurídico. En estos casos es imprescindible determinar la jurisdicción internacionalmente competente, el Derecho aplicable al contrato electrónico y la extraterritorialidad de las decisiones<sup>6</sup>. Así, las situaciones privadas internacionales dejan de ser las excepcionales en la Sociedad de la Información y el Derecho llamado a dar una respuesta adecuada a estas situaciones jurídicas, el Derecho Internacional Privado, adquiere un protagonismo incuestionable.

En el ámbito de la UE, el carácter internacional de los contratos electrónicos obliga a los tribunales de los Estados miembros que se hayan declarado competentes a aplicar el Convenio de Roma de 1980 sobre ley aplicable a las obligaciones contractuales<sup>7</sup>. Tras determinar el Derecho designado como aplicable al contrato electrónico, deberán hallarse las respuestas a algunas de las cuestiones importantes que plantea esta forma de contratar. ¿Cómo se puede incrementar la seguridad en la operación de comercio electrónico que se está realizando? ¿Qué condiciones deben cumplirse para la adecuada celebración o perfeccionamiento de un contrato electrónico?, y dentro de esta, ¿es la firma un requisito para la validez y/o manifestación de consentimiento? o ¿es tan sólo un elemento de prueba del contrato electrónico?

Las Directivas 1999/93/CE sobre Firma electrónica ("Directiva 99/93")<sup>8</sup> y 2000/31/CE sobre comercio electrónico<sup>9</sup> marcan la pauta para la legislación de los Estados miembros de la UE en materia de la seguridad en las transacciones (firma electrónica) y de la libre prestación de servicios de la Sociedad de la Información en el mercado interior comunitario (comercio electrónico)<sup>10</sup>. Como declaración de principio de estas Directivas se desprende que la utilización del medio electrónico no altera las reglas establecidas por los Estados miembros relativas a la formación, interpretación o validez de los contratos en general, salvo disposición expresa de una norma imperativa. Dichos instrumentos jurídicos son acordes con los principios de la contratación: autonomía de la voluntad y libertad de forma, por lo que, no requiriendo el Derecho aplicable al contrato una forma solemne, son válidos como norma general, los contratos electrónicos sin firma electrónica<sup>11</sup>. Ésta, sin embargo, es el instrumento idóneo para proporcionar seguridad, que es una de las cuestiones más fundamentales en todo tipo de transacción comercial, especialmente en Internet debido a las características del medio<sup>12</sup>.

En efecto, proporcionar confianza a los contratantes, concediéndoles garantías sobre la identidad de las personas, la autenticidad y la integridad del contrato, su confidencialidad..., es una cuestión de suma importancia y es aquí donde la firma electrónica adquiere un papel fundamental. En aras de esta seguridad e integridad de las comunicaciones, ¿es necesaria o conveniente la firma electrónica en un contrato celebrado vía Internet? Sobre ello incide directamente el Real Decreto-Ley 14/1999, de 17 de diciembre, sobre firma electrónica ("RDLFE")<sup>13</sup> que, adelantándose a la Directiva 99/93/CE sobre firma electrónica ya citada, pretende garantizar la seguridad en las comunicaciones. El sistema establecido en el RDLFE, cuando se trata de firma electrónica avanzada<sup>14</sup> en la que ha intervenido un prestador de servicios de certificación, garantiza la autenticidad, la integridad del mensaje (contrato), la confidencialidad y el no repudio por parte del firmante. El art. 1.2 del RDLFE establece expresamente que las disposiciones del mismo "no alterarán las normas relativas a la celebración de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones". Sin embargo, lo cierto es que, allende las cuestiones de seguridad, sí que afecta de modo directo a dos aspectos fundamentales de toda contratación: primero, la forma de emisión de las declaraciones de voluntad, por tanto, la celebración o perfeccionamiento del contrato electrónico; y segundo, la prueba del mismo.

Teniendo en cuenta todo lo anterior, el objeto de las siguientes páginas es doble: por una parte, mostrar la importancia de la firma electrónica como instrumento de seguridad e integridad del contrato electrónico entre empresas (B2B) <sup>15</sup>; y por otra, presentar el papel de la firma electrónica en la celebración de este tipo de contratos realizados a través de Internet. Para ello, en este trabajo se estudia, en primer término, el rol de la firma electrónica como instrumento de seguridad del contrato electrónico realizado a través de Internet (II); en segundo lugar, el papel de la firma electrónica en la celebración del contrato electrónico B2B, analizando los problemas de la determinación del lugar de celebración a los efectos de determinar la competencia judicial internacional y el Derecho aplicable (III); en tercer término, se analiza la firma electrónica en relación a los requisitos que debe cumplir una verdadera oferta y aceptación en la perfección del contrato electrónico (IV); y, por último, la incidencia de la firma electrónica en la prueba del contrato electrónico (V). El presente estudio finaliza con un supuesto práctico (VI); y una conclusión (VII).

## **II. La firma electrónica como instrumento de seguridad en el contrato electrónico a través de Internet: efectos jurídicos de la firma electrónica** ➔

### **1. Introducción.** ➔

Las firmas de las personas han representado desde antaño una parte fundamental de los contratos comerciales <sup>16</sup>. Sus funciones principales son las de identificar a la persona que está firmando, indicando su voluntad de contratar, y la de comprobar que no se ha alterado el documento después de su firma <sup>17</sup>. Sobre el aspecto de la autenticidad de la firma, se ha creado toda una ciencia de análisis e identificación, la pericia caligráfica, cuyos peritos cobran cantidades considerables por analizar la firmeza o timidez con que se han trazado las líneas de una firma y dar su opinión sobre si tal o tal firma es genuina o falsa. Sobre el aspecto de la integridad de los documentos, la firma manuscrita pretende indicar el estado del acuerdo escrito al momento de firmarlo, pero firmar en una hoja no puede evitar que se sustituyan páginas, y ahora en la era digital, que se sustituyan párrafos o palabras <sup>18</sup>.

Con la irrupción de la llamada “sociedad de la información” y, con ella, las actividades comerciales en Internet, se ha inventado una nueva modalidad de comprobación de identidad, de consentimiento, de autenticidad y de integridad de contratos, la llamada firma electrónica. A diferencia de la firma manuscrita, que se hace directamente con la mano y un instrumento como una pluma o un bolígrafo, la firma electrónica implica la intermediación de un teclado electrónico y un ordenador. El teclado elimina el elemento principal que asegura, en mayor o menor grado, la autenticidad de las firmas manuscritas -que cada una es la manifestación única de la persona que firma-. El teclado obliga a todos los que se llamen Juan Pérez a que firmen de la misma manera, pulsando los botones J, u, a, n, etc. Si entendemos como “firma manuscrita” una manifestación única de identidad personal hecha con la mano, entonces, ¿de qué forma el sistema informatizado, limitado por los teclados como medio de acceso, puede ofrecer la facilidad de que una persona manifieste una firma única, no falsificable y comprobable? Y ¿puede el nuevo sistema ofrecer la nueva posibilidad de que una persona tenga muchas firmas, todas únicas, no falsificables y comprobables?

Además de este problema, que podemos llamar el problema de la autenticidad de la autoría de la firma, la digitalización de los documentos y los contratos nos plantea otros problemas relacionados: ¿cómo podemos protegernos contra la alteración no autorizada de los documentos y contratos electrónicos y el repudio de los mismos? En otras palabras ¿cómo se protege la integridad del contrato y se garantiza el no repudio de la parte

contratante? Finalmente, a la vista de la enorme facilidad con que los “hackers”<sup>19</sup> a veces intervienen en las comunicaciones privadas de Internet, ¿cómo se puede asegurar que un documento sólo llegue a los ojos del destinatario designado?

Abordamos estas cuestiones –autenticidad, integridad, confidencialidad y no repudio– desde dos perspectivas, la tecnológica y la jurídica. De entrada, es importante entender algunos términos especializados. “Encriptar”, “cifrar” y “codificar” y sus opuestos “desencriptar” etc. en este trabajo se refieren a los procesos de dotar una firma electrónica o un documento electrónico de una clave, de manera que no puede abrirse ni leerse sin una clave o “llave” electrónica especial. Como parte de la creación de un documento encriptado, también se usa una clave o “llave” electrónica especial de creación que tiene una relación con la llave usada para leerlo, como se explica seguidamente.

## **2.Perspectiva tecnológica de la Firma electrónica: Respuestas de la criptografía asimétrica. La Firma digital. ➔**

Para resolver los problemas delineados en la sección anterior –autenticidad, integridad, confidencialidad y no repudio–, se han ideado varios mecanismos posibles, por ejemplo, contraseñas, claves, llaves electrónicas, números de identificación personal (“PIN”), tarjetas y hasta mecanismos biométricos como el iris del ojo o la huella digital<sup>20</sup>. Entre todas estas ideas, las soluciones más difundidas hoy día utilizan la criptografía. Para explicar en qué consiste, hay que recordar que en la informática, todo documento electrónico se traduce en series de miles o millones de ceros y unos. Todo propietario de un ordenador personal posee en él una máquina capaz de cifrar y descifrar el lenguaje de los seres humanos, es decir, el alfabeto, al lenguaje de las máquinas, es decir de los ceros y los unos. La criptografía, por medio del uso de fórmulas matemáticas especiales, modifica los ceros y unos de la firma electrónica o del documento electrónico encriptándolo de forma que sólo lo pueden leer los que poseen una clave o “llave” electrónica especial para desencriptarlo<sup>21</sup>.

El sistema de criptografía informática más aceptado es la llamada criptografía asimétrica, basada en el uso de “llaves” vinculadas<sup>22</sup>. El titular de la firma electrónica, la persona que escribe y firma un documento electrónico, tiene otra clave o “llave” electrónica privada, que sólo él sabe utilizar, para cifrar el documento. El o los destinatarios del documento tienen una llave electrónica llamada “pública”<sup>23</sup>. Esta llave pública únicamente funciona para descifrar y abrir los documentos creados con la llave privada, que está vinculada a esa llave pública. Si alguien altera el documento después de su creación y encriptación, la llave pública no funcionará para abrirlo, indicando así que ha habido una alteración<sup>24</sup>. Nace así la denominada firma digital, caracterizada por el empleo de la criptografía asimétrica o de clave pública.

En este sistema, alguien tiene que crear las llaves privadas y públicas, emitir, regular y revocar certificaciones de titularidad de las llaves, asegurar la integridad del sistema y servir de garante de confianza para comprobar que todo el que afirma ser el titular de una llave privada realmente es el titular. Así, un elemento indispensable es el llamado prestador de servicios de certificación, que es el garante de la fiabilidad del sistema<sup>25</sup>. Para que éste funcione, es indispensable que los participantes tengan confianza en estos prestadores de servicios<sup>26</sup>. En la práctica, hay varias entidades que funcionan como prestadores de estos servicios<sup>27</sup>, que se pueden agrupar en dos categorías. Primera, empresas privadas con fines de lucro que emiten llaves y certificados como parte de su actividad comercial. Segunda, entidades públicas o privadas que emiten llaves y certificados para el uso de su propio personal. Estas entidades inspiran confianza entre el público en parte a través de sus llamadas Declaraciones de Prácticas de Certificación, una exposición de sus normas, reglas y procedimientos<sup>29</sup>.

Es interesante destacar que la figura del certificado emitido por el prestador de servicios se escalona en tres clases, de acuerdo con el nivel de seguridad requerido por el cliente y la cantidad que éste está dispuesto a pagar<sup>30</sup>. En el primer nivel, el prestador identifica al titular por declaración, sin presencia física. En el segundo nivel, el titular debe comparecer ante el prestador u organismo privado para comprobar su identidad. En el tercer nivel, el titular debe comparecer ante una entidad o autoridad de carácter público, para comprobar también su identidad. Además de estos tres niveles de seguridad se ofrecen tres clases de información en los certificados: certificados de atributos (identificación, antecedentes, y hasta un requerimiento de que el receptor del certificado acredite determinadas circunstancias); certificados de tiempo (día y hora de la firma electrónica); y certificados de seudónimo (cuando figura un alias en el certificado).

Volviendo a los problemas de seguridad del documento electrónico enumerados en la sección anterior, el sistema de criptografía asimétrica ofrece las respuestas siguientes:

- ¿Cómo el firmante puede evitar que alguien falsifique su firma?

El prestador de servicios de certificación sólo dará una llave privada a una persona identificada y si un recipiente de un documento electrónico duda de la identidad del titular de la llave privada, puede verificarlo con el prestador de servicios.

- ¿Cómo el firmante puede evitar que alguien altere un documento que el firmante ha firmado electrónicamente, y cómo un recipiente de un documento puede comprobar una alteración?

Si un documento firmado ha sido alterado, la llave pública usada por el recipiente para abrir el documento no funcionará. Así, esta falta de función de una llave pública despertará la sospecha de una alteración.

- ¿Cómo el recipiente del documento firmado puede evitar que el firmante repudie el documento, alegando que no fue él el que lo firmó?

El recipiente recurrirá al prestador de servicios de certificación, el cual deberá acreditar, mediante un certificado, que el firmante es el único titular de la llave privada usada para crear y encriptar el documento. En ese momento, el firmante debe explicar, si él no es el firmante del documento, cómo otra persona ha podido usar su llave privada exclusiva para cifrarlo.

- ¿Cómo puede el firmante de un documento mantener la confidencialidad de ese documento? Dicho de otra manera, ¿cómo el firmante puede conceder o negar acceso al documento a una o varias personas?

La confidencialidad y el acceso al documento está en manos del prestador de servicios de certificación, que tiene las facultades de emitir llaves públicas bajo instrucciones del firmante. Toda persona que tiene una copia de la llave pública designada para abrir un documento determinado podrá leer ese documento.

Los cambios tecnológicos, que en pocos años han propiciado la aparición de la firma electrónica en general y de la firma digital en particular, han presentado muchos desafíos al sistema jurídico a la hora de establecer un marco estable y confiable. Como se ha podido apreciar a lo largo de la exposición, el aspecto técnico es susceptible de experimentar numerosos cambios. Sin embargo, hay dos constantes dentro de la dinámica cambiante del ciber-mundo: primera, la búsqueda de software, hardware y técnicas cada vez más rápidas y fáciles de usar; y segunda, el juego de "gato y ratón" entre las fuerzas del orden público (incluyendo el sistema jurídico) y los "hackers" por crear, por parte de los primeros, y por destruir, por parte de los segundos, la seguridad y la confianza en el sistema<sup>31</sup>. Con esto en mente, examinemos ahora los aspectos jurídicos más relevantes de la firma electrónica.

### **3. Perspectiva Jurídica: Regulación de la firma electrónica y de la firma digital ➡**

Las primeras legislaciones que aparecieron sobre este tipo de firmas se centraban en la regulación de la firma digital. Así, la Ley de firma digital de Utah tuvo una gran influencia en otras leyes de otros Estados de los EE.UU.<sup>32</sup> y en determinadas leyes europeas como la Alemana o la Italiana<sup>33</sup>. Posteriormente, surgieron otras leyes motivadas por favorecer el uso de las firmas electrónicas en general, tanto en el ámbito nacional cuanto internacional, y que neutralizando los aspectos tecnológicos, promueven el principio de no discriminación y de equivalencia entre los documentos electrónicos y los documentos escritos<sup>34</sup>.

La normativa reguladora de la firma electrónica en el Derecho español se contiene básicamente en el Decreto-Ley 14/1999 sobre firma electrónica (RDLFE)<sup>35</sup>, cuyo régimen está directamente inspirado en la Propuesta de Directiva por la que se establece un marco comunitario común para la firma electrónica<sup>36</sup> y que dio origen más tarde a la Directiva 99/93 sobre firma electrónica<sup>37</sup>. Sin embargo, el hecho de que el RDLFE fuera adoptado con carácter previo a la aprobación de la Directiva 99/93, implica un riesgo de descoordinación con la armonización comunitaria<sup>38</sup>. Estos dos instrumentos legales se dirigen a los problemas delineados en la sección anterior – la autenticidad y no-repudio de la firma electrónica, integridad (no-alteración) y confidencialidad del documento electrónico-. El RDLFE no ha sido capaz de satisfacer el motivo que lo fundamentó: la necesidad de facilitar la rápida y segura difusión de la firma electrónica. Entre los obstáculos para ello se encuentran la fuerte intervención administrativa por parte de los prestadores de servicios de certificación y el gravoso régimen de responsabilidad y garantías. Por todo ello, se ha presentado un Proyecto de Ley de firma Electrónica que pretende fomentar el uso de la firma electrónica tanto en el ámbito de las administraciones públicas como del comercio electrónico, generando ante las empresas mayor seguridad ante la tramitación telemática de sus gestiones<sup>39</sup>. Corresponde a continuación realizar un análisis comparado del actual RDLFE y de la Directiva 99/93 que permitan comprender e ilustrar de la mejor manera sobre los aspectos más importantes de los instrumentos que en España regulan la firma electrónica.

#### **3.1. Clases de Firma Electrónica: la “simple” y la “avanzada” ➡**

Tanto el RDLFE como la Directiva 99/93 sobre firma electrónica distinguen entre una “firma electrónica” sin adjetivos, que podríamos denominar “simple”, y una “firma electrónica avanzada”<sup>40</sup>, que podría identificarse con la denominada “firma digital”. La simple se define como datos electrónicos asociados de manera lógica con otros datos y “utilizados como medio de autenticación” (la Directiva 99/93) o bien “utilizados como medio para identificar formalmente al autor” del documento (el RDLFE). Esta definición general no engloba el nivel de seguridad con que se pretende hacer útil la firma electrónica en el comercio. Sin embargo, puesto que hay muchas clases de software de firma electrónica de diversos niveles de seguridad en el mercado, esta definición general sirve para dar algún marco jurídico a todas ellas.

La firma electrónica avanzada, por contraste, se dirige específicamente a algunos de los problemas fundamentales. En los dos instrumentos legales, se define como aquella que está vinculada al firmante de manera única; permite la identificación del firmante; los medios de creación de la firma están bajo el control exclusivo del firmante; y la firma está vinculada con los datos de forma que se pueda detectar cualquier cambio<sup>41</sup>. Estos requisitos se dirigen a los problemas de autenticidad, repudio e integridad (no alteración).

#### **3.2. Modalidades de Certificados: el “simple” y el “reconocido” ➡**

De la misma manera que el legislador ha previsto dos niveles de firma, se contemplan dos niveles de certificado respecto de un firmante y de su identidad. El certificado que podemos llamar "simple" se define como una certificación electrónica que vincula datos de verificación de firma a un firmante y confirma su identidad<sup>42</sup>. No hay requisitos específicos sobre el contenido ni el emisor. Por contraste, los dos instrumentos legales definen el "certificado reconocido" por medio de requisitos tanto para el certificado mismo como para el prestador de servicios que lo emite<sup>43</sup>. Los requisitos para el certificado se destinan a asegurar la identificación del firmante y del prestador de servicios, y las características del certificado mismo<sup>44</sup>. Los requisitos para el prestador de servicios tienen diversas metas generales: asegurar que el prestador emplee personal cualificado y que tenga sistemas y tecnología seguros, condiciones financieras adecuadas y sistemas de archivos fiables<sup>45</sup>. La Directiva 99/93 insta a los Estados a que establezcan un sistema de supervisión de los prestadores de servicios de certificados reconocidos<sup>46</sup>.

### **3.3. Los Prestadores de Servicios de Certificación. ➔**

Los prestadores de servicios de certificación son la piedra angular del sistema, como señalamos en la sección sobre aspectos tecnológicos. La Directiva 99/93, y más aún el RDLFE, dedican gran extensión a su reglamentación, la cual se encamina a controlar su administración, registro, obligaciones, tasas o sanciones aplicables. Ya hemos visto en el párrafo anterior algunos de los controles que se imponen a los prestadores que emiten específicamente el certificado reconocido. En general, el sistema sigue con su concepto dual, por un lado, ampliando el espacio en teoría para cualquier prestador de servicios<sup>47</sup>, pero de hecho, definiendo un ámbito más reducido que por su nivel de detalle resulta sumamente restringido. La Directiva 99/93 por su parte insta a los Estados miembros a establecer sistemas de acreditación voluntarios, objetivos, transparentes, proporcionados y no discriminatorios<sup>48</sup>.

El RDLFE dedica varios artículos al cumplimiento práctico de la Directiva 99/93 (más precisamente, de la entonces Propuesta de directiva). Se permite el establecimiento del sistema voluntario de acreditación de prestadores de servicios de certificación, con principios generales sobre normas objetivas, razonables y no discriminatorias<sup>49</sup>. Se crea un registro obligatorio de Prestadores de Servicios de Certificación, que será público<sup>50</sup>. Entre los requisitos mínimos para cualquier prestador de servicios de certificación, sea o no expedidor de certificados reconocidos, destacan los siguientes: primero, poner a disposición del firmante los dispositivos de creación y verificación de la firma electrónica, sin almacenarlos; segundo, informar a los posibles clientes de los detalles del servicio, condiciones de uso, limitaciones, precios, etc.; tercero, mantener un registro de certificados con detalles; cuarto, registrarse y, en caso de cesar sus actividades, informar a los titulares de certificados y al Registro oficial<sup>51</sup>. En general, los prestadores de servicios están obligados a cooperar con la autoridad supervisora, la Secretaría General de Comunicaciones<sup>52</sup>.

### **3.4. Responsabilidad extracontractual de los Prestadores. ➔**

El objeto fundamental de todo el sistema es el de dotar de efectos jurídicos la firma electrónica, equiparándola a la firma manuscrita. Siendo esto así, existen riesgos para las partes involucradas si algo falla en el sistema por culpa de los prestadores de servicios. Por ende, tanto la Directiva 99/93 como el RDLFE regulan expresamente la responsabilidad civil de los prestadores de servicios.

La Directiva 99/93 limita sus requisitos a los prestadores de servicios que expiden certificados reconocidos, responsabilizándolos del perjuicio causado a cualquiera que haya confiado razonablemente en tal certificado en las siguientes cuatro áreas limitadas<sup>53</sup>: primera, la veracidad de la información en el certificado y la inclusión de toda la



información prescrita; segunda, la garantía de que en el momento de expedición, el firmante tenía los dispositivos de creación de firma correspondiente; tercera, la garantía de que los datos de creación y los datos de verificación puedan usarse en conjunto (en el caso de que el prestador haya generado ambos); y, cuarta, cuando ha confiado por no haberse registrado debidamente la revocación del certificado. El prestador tiene la posibilidad de una defensa en las dos últimas áreas (uso en conjunto de datos de creación y verificación, y certificados reconocidos revocados) si puede probar que actuó sin negligencia. La Directiva 99/93 concede al prestador de servicios una gran salida a los problemas de responsabilidad civil, sin embargo, con la previsión de que el prestador puede consignar en un certificado reconocido límites acerca de posibles usos y un valor límite de las transacciones que puedan realizarse con el certificado. Estos límites tienen que ser “reconocibles para terceros”<sup>54</sup>. Con todo, un prestador de servicios “cuidadoso” puede reducir considerablemente las probabilidades y la magnitud de demandas por responsabilidad civil; y en todo caso, tendrá la defensa de no haber sido “razonable” la confianza del usuario y además tiene que comprobarse la negligencia (en dos de las cuatro áreas).

El RDLFE va más allá de la Directiva 99/93 y transfiere la obligación de comprobar al prestador de servicios. Cualquier prestador, y no sólo los que expiden certificados reconocidos, deberá responder por los daños y perjuicios<sup>55</sup> que causen a cualquier persona cuando incumplan el RDLFE o actúen con negligencia<sup>55</sup>. A la hora de una acusación, al prestador de servicios le incumbe demostrar que actuó con la debida diligencia. Sin embargo, el RDLFE alivia la severidad de esta regla en cierta medida, disponiendo que en el caso de daños por uso indebido del certificado reconocido, el prestador puede cubrirse si ha consignado en el certificado un límite respecto de su uso o respecto del valor de las transacciones para las cuales puede usarse<sup>56</sup>.

### **3.5. Efectos Jurídicos de la Firma Electrónica “simple” y “avanzada”. ➡**

Tal y como expresamente se establece en el Preámbulo del RDLFE su principal objetivo es el de establecer una regulación clara del uso de la firma electrónica, atribuyéndole eficacia jurídica. Sin embargo, lejos de la claridad deseada, el reconocimiento de la eficacia jurídica depende de la adecuada comprensión y aplicación de conceptos como el de “firma electrónica” y “firma electrónica avanzada”, “dispositivo de creación de firma seguro” y “dispositivo seguro certificado”, “certificado” y “certificado reconocido”, “prestador” y “prestador que expide certificados reconocidos y prestados acreditado”<sup>57</sup>.

Como hemos señalado, los dos instrumentos jurídicos que estamos comentando distinguen entre los efectos jurídicos de la firma “simple” y los de la avanzada. Respecto de la simple, tanto la Directiva 99/93 cuanto el RDLFE disponen que no se le puede negar efecto jurídico, pero lo abordan de maneras distintas. Aquella insta a los Estados miembros a que no se niegue eficacia jurídica a la simple por estar en forma electrónica, por no basarse en certificado reconocido, no basarse en un certificado expedido por un prestador de servicios acreditado, o por no haberse creado a través de un “dispositivo seguro de creación de firma (según la definición de esto señalada en ella)”<sup>58</sup>. El RDLFE se enfoca en la firma avanzada, estableciendo que a la firma que no sea de certificado reconocido expedido por un prestador de servicios acreditado y con dispositivo seguro de creación -según se define allí- (o sea, la simple) no se le negará efectos jurídicos ni se la excluirá como prueba por el mero hecho de existir en forma electrónica<sup>59</sup>. Con todo, esta regulación deja ambigua la diferencia del efecto jurídico entre una firma simple y una firma avanzada.

Respecto de la firma avanzada, la Directiva 99/93 indica que si está basada en un certificado reconocido<sup>60</sup> y creada por un “dispositivo seguro de creación de firma”<sup>61</sup>, entonces los Estados miembros deberían procurar que satisfaga el requisito jurídico de una firma respecto de los datos electrónicos correspondientes, de la misma manera que una

firma manuscrita lo hace en relación con los datos en papel, y que además sea admisible como prueba en procedimientos judiciales <sup>62</sup>. El RDLFE recoge estos requisitos textualmente <sup>63</sup>, y para evitar el problema de la difícil prueba de los mismos se contempla la presunción de que una firma avanzada reúna las condiciones indicadas cuando el certificado reconocido correspondiente haya sido expedido por un prestador de servicios acreditado y el dispositivo seguro de creación de firma utilizado haya sido previamente certificado por el gobierno <sup>64</sup>. De esta forma, y en nuestra opinión, la firma electrónica avanzada consigue efectos superiores a la firma manuscrita pues proporciona integridad, autenticidad, confidencialidad y no rechazo en origen. Por ello, las iniciativas legislativas sobre firma electrónica la equiparan, con más o menos exigencias, a la firma manuscrita, estableciendo, además, presunciones a favor de la validez de la firma electrónica.

### **3.6. Extraterritorialidad de los certificados. ➡**

Para las transacciones comerciales internacionales la utilización de la firma electrónica plantea el problema de la eficacia extraterritorial de los certificados. Sin embargo, y puesto que la firma electrónica se ha generado en el contexto de la economía mundial globalizada, no es de sorprender que los dos instrumentos jurídicos objeto de comentario contengan cláusulas afines. Tanto la Directiva 99/93 como el RDLFE permiten el reconocimiento jurídico de los certificados expedidos por prestadores de servicios en un tercer país fuera de la Unión Europea, con tal de que cumplan con la normativa europea. Pueden hacer esto de tres formas: primera, que el prestador de servicios haya cumplido con la Directiva 99/93 y haya sido acreditado en el sistema voluntario de algún Estado miembro de la UE; segunda, que un prestador de servicios, dentro de la UE cumplidor de la Directiva 99/93, avale el certificado; o, tercera, que haya un acuerdo bilateral o multilateral entre la UE y terceros países u organizaciones internacionales, aplicable al certificado <sup>65</sup>.

Además, para los certificados procedentes de Estados miembros de la UE opera el principio de prohibición de restricciones y de no discriminación, que les permite participar en los sistemas de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica previstos en el RDLFE <sup>66</sup>.

### **3.7. Protección de Datos Personales. ➡**

Tanto la Directiva 99/93 cuanto el RDLFE se remiten a la normativa vigente sobre protección de datos personales <sup>67</sup>. Además, subrayan que los prestadores de servicios únicamente pueden recabar datos personales directamente del titular de los datos o previo consentimiento de éste, y sólo los datos mínimos necesarios para el certificado. Finalmente, respecto de los seudónimos, la Directiva 99/93 permite el uso de seudónimos, pero el RDLFE requiere que si el firmante lo pide, el prestador haga constar su identidad verdadera en el certificado, y en todo caso, el prestador debe revelar a los órganos judiciales en ejercicio de sus funciones la identidad de la persona en las circunstancias previstas bajo la ley <sup>68</sup>.

## **4. Valoración práctica sobre la utilización de la firma electrónica. ➡**

A pesar de las diversas ventajas del uso de la firma electrónica y las muchas protecciones que esta ofrece a los usuarios de Internet -y, por tanto, a los empresarios que comercializan a través de este medio-, la firma electrónica no ha sido adoptada en el mundo empresarial al nivel que se esperaba. El RDLFE no ha cumplido como se esperaba con su objetivo de regular y dar seguridad al tema de la validez de la firma electrónica y sobre todo de hacer de esta un instrumento útil y accesible. Para explicar esto, hay que tener en cuenta que las innovaciones electrónicas se adoptan conforme a su conveniencia, no tanto a las ventajas que puedan ofrecer, máxime cuando los usuarios ya tienen una solución confiable a la cual están acostumbrados. En este caso, la firma

electrónica requiere que las partes dispongan de un ordenador normal pero con un dispositivo lector de tarjetas de firma electrónica, un software especial, y una tarjeta inteligente con un "chip" que requiere una contraseña para funcionar<sup>69</sup>. De la práctica se desprende que el consumidor medio, o el comerciante medio, no se ha tomado la molestia de obtener estos dispositivos adicionales y de aprender su uso, tal vez debido en parte a que no ve la importante ventaja que conlleva para proporcionarle mayor seguridad en las transacciones que realiza en Internet.

Hasta aquí el estudio se ha centrado en los aspectos de seguridad que ofrece la firma electrónica al usuario de Internet. A partir de ahora se examina el papel de este instrumento como garantía de seguridad en la formación o celebración del contrato electrónico y en la prueba de su validez o existencia.

### **III. Firma electrónica y celebración del contrato electrónico: Competencia judicial internacional, Derecho aplicable y forma de celebración** ➔

#### **1. Planteamiento** ➔

En toda contratación internacional es preciso determinar el tribunal competente en caso de litigio y el derecho aplicable al contrato. En el ámbito comunitario, la competencia judicial internacional se determina por el Reglamento de Bruselas 44/2001, sobre competencia judicial internacional, reconocimiento y ejecución de decisiones en materia civil y mercantil<sup>70</sup>, que ha sustituido para todos los países excepto para Dinamarca al Convenio de Bruselas de 1968<sup>71</sup>. Para determinar el derecho aplicable, el juez comunitario competente aplicará el Convenio de Roma de 1980 sobre ley aplicable a las obligaciones contractuales<sup>72</sup>. Centrándonos en las cuestiones de forma, un contrato será válido en cuanto a la forma de celebración si reúne las condiciones exigidas por la propia ley del contrato o por la ley del lugar de celebración (art. 9). Determinar el lugar de celebración puede revestir de por sí gran dificultad, pero el advenimiento de Internet ha exacerbado en muchos casos esa dificultad debido a su naturaleza anónima y mundial y deslocalizada. Internet permite comunicaciones internacionales más complejas, más rápidas –e incluso simultáneas- y sobre todo más susceptibles de confusiones, engaños y distorsiones.

Además de determinar el lugar de celebración, relevante respecto de la validez formal del contrato, hay que determinar si realmente el contrato se ha perfeccionado. Si el Derecho aplicable a la forma fuese el español dicho Derecho no exige, con carácter general, ni la realización por escrito de un contrato ni la firma manuscrita como requisito de validez (art. 1258 Código civil). Para que exista un contrato electrónico, como en cualquier otra transacción, es necesario que se produzca un concurso entre la oferta y la aceptación. Sólo entonces se entenderá que el contrato se ha celebrado o perfeccionado. Pero en la contratación electrónica, la determinación de cuándo estamos ante una verdadera oferta o aceptación no siempre será fácil.

Hasta la fecha, la tecnología de Internet permite celebrar contratos de dos maneras: 1) por el intercambio de correos electrónicos, que son mensajes no estructurados en comparación con los mensajes de EDI<sup>73</sup> o 2) puede llevarse a cabo a través de páginas web interactivas en las que normalmente la voluntad de obligarse se realiza mediante la cumplimentación de un formulario electrónico elaborado por el prestador del contenido. Con los correos puede surgir el problema de distinguir entre lo que en sí constituye una oferta o una aceptación, especialmente cuando hay varios correos entrecruzados. Respecto de las páginas web, hay que distinguir a su vez entre páginas web interactivas y pasivas, lo que va a tener importantes consecuencias a la hora de determinar si estamos

ante una verdadera oferta. Cuando nos encontramos con una página web interactiva, que articula mecanismos de petición o formularios, podemos estar ante verdaderas ofertas. Por el contrario, las páginas web pasivas cuya función es publicitaria o de contacto nos sitúan ante invitaciones a ofertar, por lo que es posible que el comprador se convierta en el oferente y viceversa.

Por todo lo anterior, son tres las cuestiones que interesa ahora examinar respecto de los contratos y su relación con la firma electrónica: primera, la delimitación del lugar de celebración del contrato electrónico a los efectos de determinar la competencia judicial internacional y el Derecho aplicable (2); segunda, el principio de libertad de forma y la admisión de la forma electrónica en la celebración del contrato B2B, con especial referencia al contrato de compraventa internacional de mercaderías (3); y tercera, el papel de la firma electrónica en la expresión de la voluntad de contratar, con especial referencia al Derecho estatal o autónomo español (4).

## **2. Lugar de celebración del contrato electrónico B2B y firma electrónica ➡**

La determinación del lugar de celebración del contrato es siempre incierta cuando la contratación se realiza a distancia, porque al encontrarse los contratantes en países diferentes, el contrato puede entenderse celebrado en el lugar donde cualquiera de estos se encuentra o incluso en un tercer Estado<sup>74</sup>. La incertidumbre se acentúa en Internet, por las características intrínsecas a este medio global por naturaleza. Sin embargo, precisar el lugar de celebración del contrato muchas veces puede ser decisivo en la aplicación de ciertas normas de Derecho Internacional Privado, en particular, en lo relativo a la determinación de la competencia judicial internacional y, como hemos adelantado, respecto a la validez formal del contrato electrónico según el Derecho aplicable.

### **2.1. Incidencia del lugar de celebración del contrato electrónico en la determinación de la competencia judicial internacional ➡**

Debido a las dificultades de la concreción del “lugar de celebración”, este criterio ha sido obviado como determinante de la competencia judicial internacional en los instrumentos comunitarios. Ni el Reglamento de Bruselas 44/2001, sobre competencia judicial internacional, reconocimiento y ejecución de decisiones en materia civil y mercantil<sup>75</sup> -aplicable por los jueces de los Estados miembros UE para determinar su competencia judicial internacional- ni previamente el Convenio de Bruselas de 1968<sup>76</sup> contemplan el lugar de celebración del contrato a los efectos de determinar el tribunal competente<sup>77</sup>. En contraposición, el lugar de celebración de un contrato electrónico sí que es relevante cuando resulta de aplicación el art. 22.3 de la Ley Orgánica del Poder Judicial de España (LOPJ)<sup>78</sup>, bien por remisión del art. 4 del Reglamento 44/2001 o bien porque el litigio escapa del ámbito de aplicación de dicho Reglamento<sup>79</sup>. En virtud del art. 22.3 del la LOPJ, los tribunales españoles son competentes si el lugar de celebración del contrato electrónico es España –o si el contrato debe cumplirse en España-<sup>80</sup>.

Para determinar el lugar de celebración, y por tanto, deducir si el juez español es o no competente para conocer de un contrato electrónico en el que el demandado esté domiciliado fuera de un Estado miembro<sup>81</sup>, el juez español debe hacerlo conforme a la ley española. Aplicando tal ley, tres son sus opciones para concretar tal lugar de celebración: primera, acudir, en caso de contrato compraventa internacional de mercancías, al arts. 18- 24 de la Convención de Viena sobre Compraventa Internacional de Mercaderías de 1980 (Convenio de Viena)<sup>82</sup>; segunda, de no resultar aplicable el Convenio de Viena, acudir al art. 54 del Código de comercio –modificado por la Ley 34/2002, de comercio electrónico<sup>83</sup>- y, tercera, concretar el lugar de celebración en virtud aplicando el párrafo segundo del art. 29 de la Ley 34/2002 de comercio electrónico<sup>84</sup>.

El Convenio de Viena entiende perfeccionado el contrato en el lugar de la oferta (arts. 18-24), mientras que el art. 54 del Código de Comercio se inclina por el lugar de la manifestación de la aceptación. Más controvertido es, sin embargo, el art. 29.2 de la Ley 34/2002: “los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios”. Este precepto debe ser criticado por la dificultad o hasta imposibilidad práctica de aplicación a los contratos electrónicos que revistan carácter internacional, porque su aplicación para determinar el lugar de celebración de un contrato electrónico internacional podría conducir al resultado inadecuado de declarar como tal lugar un país sin ninguna vinculación con el asunto, por la casualidad de la presencia allí del prestador de servicios; con la agravante de que puede tratarse de un país con una débil protección de las comunicaciones electrónicas, un “paraíso informático” o incluso un lugar desconocido por las partes. Este resultado, en el sector de la competencia judicial internacional, podría traducirse en que a pesar de que la oferta, por ejemplo, se hubiese realizado en España, lugar donde además se encuentra establecido el comprador o el vendedor (hemos visto que la relación oferta-aceptación puede invertirse en la contratación electrónica con mucha facilidad), los tribunales españoles podrían declararse incompetentes en virtud de este criterio de competencia judicial internacional.

Al abordar la cuestión de la determinación del lugar de celebración o perfeccionamiento del contrato es importante tener en cuenta que lo esencial es, como afirma P.A. DE MIGUEL ASENSIO<sup>85</sup>, garantizar las legítimas expectativas de las partes y la seguridad jurídica, por lo que parece oportuno conceder un margen de apreciación al intérprete. En consecuencia, a los efectos de determinar el lugar de celebración de un contrato electrónico resulta importante distinguir con A.L. CALVO CARAVACA<sup>86</sup> dos supuestos que deberían condicionar la respuesta a la localización de tal lugar de celebración del contrato electrónico, dependiendo del medio utilizado: correo electrónico o página web.

Primero, si el contrato se ha celebrado a través de correo electrónico, lo relevante es el país desde el que se hace la oferta, del que parte el correo electrónico, sin importar el país del servidor que almacena la información o el país de destino del e-mail o aquél en el que se accede a su contenido. Por lo tanto, el contrato electrónico debe entenderse celebrado en el país de la oferta: si ésta ha tenido lugar en España serán competentes los tribunales españoles.

Segundo, si el contrato se celebra mediante una página web interactiva, el país desde el que parte la oferta es el país del servidor que aloja la página; sin embargo, en la medida en que esta respuesta lleva a “resultados absurdos”, es más adecuado considerar como país de celebración del contrato electrónico aquél en el que se encuentra el establecimiento de la empresa que ha creado la página web a través de la que se contrata electrónicamente.

Las anteriores reflexiones son acertadas, porque intentan evitar el resultado nada deseable de que una pequeña isla en el Pacífico (por poner un ejemplo) se convierta en la referencia jurídica de muchos contratos. Sin embargo, dejan abiertas otras interrogantes. Una regla que designa por defecto como país de la celebración el lugar de la procedencia del correo electrónico de oferta da una ventaja al oferente: puede enviar el correo desde el país en el que está establecido o bien llevar su ordenador portátil a un país de su elección y enviar el mensaje desde allí. Por otra parte, una regla que se basa en una bifurcación de decisión entre el país del servidor o bien si esto es “absurdo” el país del establecimiento del empresario, creador de la página web (generalmente el oferente) -además de cuestionar qué es “absurdo”- también da la ventaja al oferente. Con todo, el criterio del “lugar de celebración = oferta” nos parece más acertado que el propuesto por el mencionado art. 29 de la Ley 34/2002 (“lugar del prestador de servicios”), y en la medida en que el oferente puede ser el comprador o el vendedor no se está protegiendo a las partes por la posición compra o venta que estén realizando, sino por haber tomado la iniciativa de obligarse electrónicamente. Además, el lugar de la oferta puede coincidir con el lugar en el que se

entiende manifestado el consentimiento como veremos infra.

## **2.2. Incidencia del lugar de celebración del contrato electrónico en la determinación del Derecho aplicable a la forma ➡**

En el sector del Derecho aplicable el lugar de celebración del contrato puede tornarse una cuestión fundamental para determinar la validez formal del contrato electrónico. El Convenio de Roma de 1980 sobre ley aplicable a las obligaciones contractuales será aplicable por todos los jueces de la UE para determinar el Derecho aplicable a la validez formal del contrato, incluyendo el contrato electrónico<sup>87</sup>. La conexión "lugar de celebración del contrato" está recogida en el art. 9 como uno de los criterios fundamentales para determinar si un contrato es válido en cuanto a la forma. Por ello, tal y como se ha afirmado anteriormente, resulta imprescindible, para evitar resultados no adecuados, interpretar el mismo en aras a la protección de las expectativas de las partes y a la seguridad del tráfico comercial internacional, máxime si se tiene en cuenta que este convenio no fue redactado pensando en la contratación electrónica.

En este sentido, hay que tener presente que en la contratación electrónica es frecuente dar la apariencia de contratar desde un país cuando en realidad se está contratando desde otro diferente. Por esta razón, la doctrina ha señalado la conveniencia de que prevalezca el "lugar de situación aparente"<sup>88</sup>. Por consiguiente, si se celebra un contrato electrónico internacional entre partes que aparentemente se encuentran en un mismo país (aunque en realidad no lo están), dicho contrato "será válido en cuanto a la forma si reúne las condiciones de forma de la ley que lo rija en cuanto al fondo o de la ley del país en el que se haya celebrado" (art. 9.1); y un contrato celebrado entre personas que aparentemente se encuentran en países diferentes (pero que en realidad están en el mismo) "será válido en cuanto a la forma si reúne las condiciones de forma de la ley que lo rija en cuanto al fondo" o de "la ley de uno de estos países" (art. 9.2).

Ahora bien, relacionando el apartado 1 con el 2 del art. 9 el problema de la situación aparente o real ya no parece tan trascendente, habida cuenta de la importancia que debe adquirir el principio de favor negotii que parece informar dicho precepto. La determinación de la lex contractus se torna entonces crucial, puesto que si según la ley del lugar de celebración no es válido el contrato electrónico, pero sí lo es según la ley que rige el fondo del contrato, éste será válido. En virtud del artículo 3 del Convenio de Roma de 1980, la lex contractus es la ley elegida por las partes y, en su defecto, la determinada por el artículo 4, que será la ley con la que el contrato tiene los vínculos más estrechos, que en una compraventa internacional será la del país del establecimiento del vendedor, en tanto que ley de la parte que tiene que hacer la prestación característica (art. 4.2).

De todo lo anterior se deduce que el contrato será válido en cuanto a la forma si es válido según la ley de la oferta o según la ley del establecimiento del vendedor, que, como hemos dicho, no tienen por que ser coincidentes en la contratación realizada a través de Internet.

## **3. Principio de libertad de forma y firma electrónica: Especial referencia a la compraventa internacional electrónica. ➡**

En el ámbito internacional, la Ley modelo de UNCITRAL sobre comercio electrónico<sup>89</sup>, prevé que salvo pacto en contrario, la oferta y la aceptación contractuales podrán emitirse por medio de un mensaje de datos, afirmando que "no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos" (art. 5 bis).

En el supuesto de que el contrato electrónico versara sobre una compraventa internacional de mercaderías no sería necesaria ninguna formalidad de celebración si resultara aplicable

la Convención de Viena sobre compraventa internacional de Mercaderías de 1980<sup>90</sup>. Lo que ocurriría si se cumpliesen los requisitos exigidos en su art. 1 y 6 (que se trate de empresas establecidas en Estados contratantes diferentes o que las normas de Derecho Internacional Privado del foro declaren aplicable la ley de un Estado contratante) y las condiciones espaciales, materiales y voluntarias para su aplicación. El contrato de compraventa internacional regido por el Convenio de Viena de 1980 no tendrá que celebrarse ni probarse por escrito y no está sujeto a ningún otro requisito de forma. No es necesaria su firma para la validez del mismo (art. 11 Convenio Viena) y podrá celebrarse intercambiando correos electrónicos o pulsando en determinados lugares de una página web. Sin embargo, en el Derecho de algunos Estados contratantes sí se exige que el contrato se celebre por escrito, en cuyo caso dichos Estados pueden hacer una declaración en virtud de la cual el contrato deba celebrarse por escrito siempre que cualquiera de las partes de tal contrato esté establecida en ese Estado (art. 96 Convenio de Viena). Es importante tener en cuenta que cuando la forma escrita se exige como presupuesto de validez, se exige no sólo que el contrato conste por escrito, sino también su firma (manuscrita), lo que por las razones expuestas supra (equiparación de efectos jurídicos y seguridad), puede reemplazarse en el comercio electrónico a través de Internet con la firma electrónica avanzada.

Entre las condiciones materiales de aplicación del Convenio de Viena -y a los efectos de este trabajo- interesa destacar dos cuestiones fundamentales:

Primera. Que debe tratarse de “mercaderías”. Ello plantea la cuestión de interpretar si éstas deben ser siempre tangibles, o si el Convenio de Viena debe ser reinterpretado para su adecuada aplicación a la compraventa de las “mercancías” capaces de circular por Internet. Defender que es necesario que se trate de un bien mueble corporal tiene consecuencias importantes: por una parte, quedan excluidas las compraventas relativas a objetos inmateriales –derechos de autor, marcas, patentes- frecuentes en las compraventas realizadas por vía electrónica; y por otra, plantea el problema de si se aplica el concepto de mercadería a determinados productos digitales que también pueden adquirirse en formato tangible. En nuestra opinión, el Convenio de Viena debe, aplicarse a las adquisiciones de bienes on-line (software, música, vídeos...) y ello no sólo porque dichos productos pueden adquirirse también en soporte analógico, tratándose, por tanto, de una compraventa de un bien corporal<sup>91</sup>, sino también porque el objeto de lo que se está comprando o vendiendo es la “mercancía” en sí y no el derecho de propiedad intelectual o industrial.

Segunda, que se trate de una compraventa internacional, entendida como contrato entre empresas establecidas en Estados diferentes, por el que se entrega un bien a cambio de un precio. Se excluyen, en consecuencia, los contratos de licencias o cesiones de derechos de propiedad intelectual o industrial celebrados en Internet y los contratos electrónicos celebrados con consumidores.

Por todo lo anterior, las compraventas internacionales electrónicas incluidas en el ámbito de aplicación de los instrumentos jurídicos mencionados no requieren para su validez ni que se realicen por escrito ni que se formalicen mediante firma electrónica<sup>92</sup>. No obstante, para evitar los riesgos intrínsecos a esta forma de contratar –incertidumbre respecto del tribunal competente, derecho aplicable, perfeccionamiento del contrato, autenticidad, integridad, no repudio, confidencialidad, ataques de hackers...-, parece aconsejable la redacción de un contrato y que éste se desarrolle en un clima de confianza, garantizando que el mensaje electrónico proviene de la persona que dice que lo envía (autenticación), que no ha sido alterado (integridad), que el oferente no podrá negar su envío ni el aceptante su recepción (no-rechazo) y, en fin, que existe confidencialidad en las relaciones, aspectos que sólo garantizará la firma electrónica avanzada<sup>93</sup>.

#### **4. Papel de la Firma Electrónica en la expresión de la voluntad de contratar en la contratación electrónica. Especial referencia al Derecho estatal español. ➔**

El consentimiento electrónico es una modalidad más de declaración de la voluntad contractual. En Derecho español la validez de tal declaración no está supeditada a la existencia de un contrato escrito ni a su firma, por lo tanto, tampoco a su firma electrónica. La validez y la fuerza obligatoria de un contrato en principio no resulta afectada porque las declaraciones de voluntad se emitan de forma electrónica. Aunque bien es cierto que la firma es la forma más frecuente de expresar el consentimiento, sólo en instituciones como la letra de cambio o el cheque se requiere de forma explícita la firma manuscrita (o su equivalente digital) de los contratantes <sup>94</sup>.

El RDLFE, que al regular la firma electrónica, consagra y reconoce jurídicamente el comercio electrónico, no regula algunos de los aspectos que se ven directamente afectados por la forma utilizada en la contratación. Uno de los problemas que planteaba la aplicación del RDLFE era el de si el criterio de equivalencia funcional de los datos consignados en forma electrónica con los consignados en soporte papel, puede aplicarse a aquellos contratos en los que se exige como requisito para la validez el empleo de forma solemne. Según el art. 1.2 las disposiciones del Real Decreto-Ley no alteran las reglas relativas a la celebración, formalización, validez y eficacia de los contratos. En el mismo sentido la Directiva 99/93/CE de Firma Electrónica advierte en su art. 1.2 que no regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites contenidos en las legislaciones comunitarias que rigen el uso de documentos.

Es el art. 23 de la Ley 34/2002, de servicios de la sociedad de la información y del comercio electrónico el que parece resolver para España la duda a favor de la equivalencia entre forma electrónica y forma escrita:

“1. los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez. 2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos. 3. Siempre que la ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico”.

Por lo tanto, la necesidad de forma escrita que muchas leyes requieren en materia de contrato de seguro <sup>95</sup>, crédito al consumo <sup>96</sup>, viajes combinados <sup>97</sup>, venta a plazos de bienes muebles <sup>98</sup>, así como el requisito de que conste por escrito determinadas cláusulas de un contrato como la asunción de riesgos en el contrato de agencia <sup>99</sup>, o la cláusula de sumisión expresa del Reglamento 44/2001 (art. 23) queda cubierta con la forma electrónica, siempre que “proporcione un registro duradero”. Ahora bien, en la medida en que estos contratos deben ser firmados debería ser necesaria, en nuestra opinión, la utilización de la firma electrónica avanzada en la que ha intervenido un prestador de servicios reconocido, teniendo en este caso plena efectividad el principio de equivalencia funcional entre el soporte electrónico y el soporte papel.

Con todo, es interesante notar que en la práctica comercial la utilización de la firma electrónica como medio de expresar la voluntad de celebrar un contrato electrónico es escasa en comparación con el número de contratos electrónicos que se realizan. Los particulares todavía no acuden de manera habitual a las autoridades de certificación



electrónica para garantizar la estabilidad, integridad o autoría del contrato electrónico. En el tráfico empresarial la certificación privada (PGP o Pretty Good Privacy), la utilización de simples claves o la encriptación simple de documentos electrónicos (SSL o Secure Socket Layer) está más extendida que la certificación mediante la firma electrónica avanzada<sup>100</sup>. Es posible que, con el aumento del uso de Internet en general, la progresiva penetración a través del tiempo de los jóvenes en la economía y los ataques cada vez más dañinos de los "hackers", aumentará la popularidad de la firma electrónica avanzada por la mayor seguridad que brinda al comercio electrónico.

#### **IV. Firma electrónica y perfección de los contratos electrónicos B2B: requisitos de la oferta y de la aceptación.** ➔

##### **1. Planteamiento** ➔

En el tráfico comercial internacional el principio predominante es el de la libertad de forma, que resulta igualmente aplicable al comercio electrónico. La exigencia de ciertos requisitos formales en algunas legislaciones estatales puede impedir la celebración de un contrato electrónico o provocar inseguridad sobre su validez. En Derecho español la forma no es por lo general un elemento constitutivo de la estructura del negocio sino un instrumento para su manifestación. En la contratación comercial internacional y, en particular en la compraventa, es aconsejable, no obstante, celebrar el contrato por medios escritos y ello para evitar los riesgos derivados de la incertidumbre respecto del tribunal competente, Derecho aplicable y todas las cuestiones fundamentales relativas al perfeccionamiento del contrato y el cumplimiento de la obligación. La firma electrónica no es de ninguna manera un elemento constitutivo de la contratación electrónica. Sin embargo, los problemas prácticos que esta contratación presenta en torno a algo tan esencial como es la perfección del contrato, permiten afirmar que la firma electrónica puede ser un instrumento de suma utilidad para reducir riesgos intrínsecos a la contratación internacional celebrada a través de Internet.

Puesto que el contrato se perfecciona al surtir efecto la aceptación de la oferta (art. 23 convenio de Viena) corresponde, en primer lugar, analizar cuándo existe una oferta y una aceptación en un contrato electrónico B2B (2); y, a posteriori examinar en qué momento se perfecciona dicho contrato y si la firma electrónica aporta algún elemento jurídico indispensable o aconsejable que merezca tenerse en cuenta a la hora de perfeccionar un contrato electrónico de compraventa internacional (3).

##### **2.¿Cuándo existe una oferta y cuándo se produce la aceptación en un contrato electrónico B2B?** ➔

El Convenio de Viena regula detalladamente el régimen de la oferta y de la aceptación en los arts. 14-24. Sin embargo, como hemos expuesto, determinar cuándo estamos ante una verdadera oferta electrónica no siempre es fácil. Gran parte de las informaciones expuestas en Internet y numerosas comunicaciones comerciales remitidas por correo electrónico son más bien mensajes publicitarios o meras invitaciones a ofertar. En las páginas web interactivas existen auténticas ofertas, mientras que en las pasivas lo que encontramos son invitaciones a realizar ofertas o comunicarse por medio de correo electrónico.

###### **2.1.Requisitos de la oferta electrónica** ➔

En virtud del Convenio de Viena, una verdadera oferta debe cumplir una serie de

exigencias:

Primera. Debe dirigirse a una o varias personas determinadas. Una oferta por correo electrónico fácilmente cumplirá con este requisito, pero la oferta contenida en una página web de Internet a la que se puede acceder desde cualquier lugar del mundo y por cualquier persona ¿es una oferta o una mera invitación a la misma?. Como hemos adelantado, si la página web es pasiva, cuya función es publicitaria o de contacto, estamos tan sólo ante invitaciones a realizar ofertas y, en consecuencia, la posición tradicional vendedor-oferente comprador-aceptante se invierten. Por ello, quien sólo quiere incorporar invitaciones a realizar ofertas en su página web es importante que deje constancia de ello, advirtiendo que no quedará vinculado hasta su ulterior aceptación.

Segunda. Debe ser suficientemente precisa, lo que se cumple indicando las mercancías y expresa o tácitamente señalando la cantidad y el precio o previendo un medio para determinarlas, y debe indicar la intención del oferente de quedar obligado en caso de aceptación (art. 14 Convenio de Viena). Además, tanto la Directiva 31/2000 de comercio electrónico como la Ley 34/2002 de comercio electrónico<sup>101</sup> exigen la identificación de las comunicaciones comerciales y la indicación de la persona en cuyo nombre se realizan. Por lo tanto, las simples listas de precios, anuncios de productos o servicios o la existencia de una página web como reclamo publicitario no significan que exista una oferta en tanto no se especifiquen cuestiones como las características del producto, el precio y forma de pago, condiciones y plazo de entrega, etc., y se permita una suscripción o aceptación de la propuesta a través de mecanismos de la propia web<sup>102</sup>. La Directiva 31/2000 y la Ley 34/2002 exigen que se garantice que el oferente facilite antes de que se efectúe el pedido la información relativa a los diferentes pasos técnicos que deben darse para celebrar el contrato, si este va a registrarse o ser accesible, cuáles son las lenguas de formalización, y los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido (art. 10 y 11), lo que se aplicará, a falta de pacto en contrario, a la contratación mediante formato html o web y no en la contratación vía correo electrónico. En este caso también es importante recordar que “quedan prohibidas las comunicaciones comerciales no solicitadas a través de correo electrónico u otro medio equivalente que previamente no hayan sido solicitadas (art. 21 Ley 34/2002)<sup>103</sup> .

Tercero. La oferta surte efecto cuando llegue al destinatario (art. 15 Convenio Viena), lo que se presume que ocurre inmediatamente en la contratación electrónica a través de una web interactiva, ya que la oferta llega al destinatario de forma inmediata, pero no tiene por qué ser así en la oferta realizada mediante correo electrónico o a través de una página web pasiva<sup>104</sup> .

Cuarto. La oferta podrá ser retirada si su retiro llega al destinatario antes o al mismo tiempo que la oferta (art. 15.2 Convenio de Viena). La oferta electrónica difícilmente podrá ser retirada, porque su retiro no puede llegar al destinatario antes de la oferta en sí; como mucho podrá llegar al mismo tiempo. La oferta revocable puede ser retirada si su retiro llega al destinatario antes de que este haya manifestado la aceptación; y no puede retirarse si el destinatario podía “razonablemente” pensar que la oferta era irrevocable y ha actuado basándose en esa oferta (art. 16 Convenio de Viena).

## **2.2.Requisitos de la aceptación electrónica ➔**

La aceptación, por su parte, debe cumplir las siguientes exigencias previstas en los arts. 18-22 del Convenio de Viena:

Primera. Debe consistir en una declaración o acto del destinatario que indique asentimiento a una oferta, no constituyendo aceptación el silencio o la inacción por sí solos. En la contratación en formato EDI se fija cómo se formula la aceptación del contrato, mientras

que en la contratación en una red abierta o en Internet –o a falta de acuerdo expreso– existen múltiples formas de manifestar la aceptación: pulsar una tecla, un icono con “acepto” o similares, rellenar formularios o solicitudes, enviar correos electrónicos, el pago, la utilización del servicio o la descarga un archivo<sup>105</sup>. Es importante tener presente que el significado que tengan estas actuaciones puede ser distinto dependiendo del país o Derecho aplicable<sup>106</sup>. Por ello, es importante indicar claramente en la web qué se entenderá por aceptación y conceder al cliente el tiempo necesario para que lo haga<sup>107</sup>, así como tener certeza sobre cuál es la ley aplicable a la compraventa electrónica que se está realizando.

Pulsar en el espacio destinado a la aceptación en una página web o el intercambio afirmativo de correos electrónicos debe entenderse por aceptación en el sentido del Convenio de Viena de 1980. Dicha aceptación surte efecto en el momento en el que la indicación de asentimiento llegue al oferente (art. 23), lo que en la contratación electrónica mediante páginas web de Internet ocurre de modo instantáneo.

Segunda. La respuesta a una oferta sin modificaciones sustanciales se considera aceptación, pero si la respuesta que pretende ser una aceptación, contiene adiciones, limitaciones u otras modificaciones se considerará como rechazo y constituirá una contraoferta (art.19 Convenio Viena). Cualquier modificación respecto del precio, pago, cantidad o calidad de la mercancía, lugar o fecha de entrega, responsabilidad o resolución de controversias en la respuesta modifican elementos sustanciales que evitan que pueda considerarse como aceptación tal respuesta. La aceptación debe realizarse en el plazo establecido en la oferta y puede ser retirada si su retiro llega al oferente antes de que la aceptación haya surtido efecto o en ese momento (art. 20 Convenio de Viena), lo que es difícil que se produzca en la contratación electrónica realizada mediante páginas web<sup>108</sup>. Las páginas web normalmente no ofrecen mecanismos para que el usuario modifique la oferta hasta el punto de hacer una contraoferta. El intercambio de correos, por supuesto, sí lo permite.

### **3. El momento de perfección del contrato electrónico B2B y la firma electrónica ➡**

El momento de celebración del contrato es una de las cuestiones más debatidas y generadoras de inseguridad ya que según cuál sea el Derecho aplicable se puede dudar si tal momento es el del envío de la aceptación o el de la recepción de la misma. Tampoco está claro lo que significa la acción de pulsar en el icono de “aceptar”, que puede tener un significado diferente para cada Estado, lo que repercutirá en la determinación del momento en que se perfecciona el contrato. Una parte contratante puede entender, como hemos adelantado, que el contrato ya se ha celebrado con esta pulsación y la otra, de acuerdo con su legislación, entender que todavía no está vinculado por el contrato. Se trata, por lo tanto, de un problema íntimamente relacionado con la seguridad de las transacciones comerciales electrónicas y que podría atenuarse, en nuestra opinión, con el recurso a la firma electrónica.

En la contratación electrónica entre empresarios el criterio dominante será el establecido por las partes en su acuerdo, pues tanto la Ley modelo de UNCITRAL, como el Acuerdo Europeo de modelo EDI, los arts. 18.2 en relación con el 23 y 24 del Convenio de Viena e incluso el art. 54 del Código de Comercio tienen carácter dispositivo, ya que su aplicación depende de la autonomía de las partes contratantes.

A falta de acuerdo, se plantea un problema de divergencia de criterios. Según el art. 54 del Código de Comercio, para la perfección del contrato se exigiría el depósito de la aceptación en el servidor del correo electrónico o el envío del mensaje que contiene la aceptación<sup>109</sup>. En la contratación internacional mediante el Convenio de Viena (arts.

18-24) o a través del Acuerdo EDI se considerará perfeccionado el contrato cuando el correo electrónico llegue al servidor del oferente.

Ahora bien, ¿es posible concretar mediante la firma electrónica el momento de la perfección o celebración del contrato? Como hemos indicado, existe la firma electrónica simple y la avanzada. Si se utiliza la firma electrónica avanzada (la firma electrónica acreditada por un tercero en el documento electrónico ordinario), se puede comprobar con certeza el momento en el que el mensaje electrónico llega a un servidor ajeno al del emisor. Si se usa la firma simple, por contraste, será más difícil lograr el mismo nivel de confianza, por varios motivos. La fecha inscrita en el documento electrónico o la fecha del propio ordenador carecen de fiabilidad porque son fácilmente manipulables por el interesado. El Acuerdo EDI europeo contempla el deber de las partes de guardar un registro completo de todos los documentos EDI sin modificar y debidamente protegidos de conformidad con los plazos y disposiciones legales de su Derecho estatal y al menos durante 3 años (art. 8.1). El registro del emisor y del receptor puede contrastarse, pero debido a que no existe un mecanismo de verificación por tercero, pueden existir problemas en el caso de que los registros no coincidan. El peritaje informático no siempre revelará quien es el causante de la divergencia. Si se emite una factura telemática, existe en Derecho español un deber de establecer un registro histórico por sólo cinco años<sup>110</sup>. Por estos motivos, la firma electrónica avanzada, por las características ya expuestas, parece ser el medio más adecuado para evitar los problemas derivados de la falta de concreción de la perfección del contrato electrónico.

La propuesta de Directiva de Comercio electrónico, que condujo a la directiva actual<sup>111</sup>, preveía que el contrato quedara celebrado en el momento en que el destinatario del servicio aceptante hubiese recibido notificación electrónica acusando recibo de la aceptación del destinatario del servicio, pero finalmente se suprimió tal concreción. El art. 11 de la Directiva 2000/31/CE tan sólo establece que “el prestador de servicio debe acusar recibo del pedido del destinatario sin demora indebida y por vía electrónica”, considerándose que “se ha recibido el pedido y el acuse de recibo cuando las partes a las que se dirigen puedan tener acceso a los mismos”. Ley 34/2002 de comercio electrónico recoge esta obligación en el art. 28 si bien establece que “no será necesario confirmar la recepción de la aceptación de una oferta cuando a) ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor b) el contrato se haya celebrado exclusivamente mediante el intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación”. El problema fundamental es que no se especifica qué consecuencias tendría el incumplimiento de la obligación de enviar acuse de recibo. Además, ni la Directiva ni la Ley aclaran a qué tipo de acuse de recibo se refieren o si éste puede servir para concretar o probar la aceptación<sup>112</sup>.

Por estos motivos el acuse de recibo no parece indicar el momento de la perfección del contrato electrónico. Sin embargo, es útil como criterio de fijación del momento en el que la revocación de la aceptación deja de ser admisible o como medio de confirmación de la aceptación tardía del art. 21 del Convenio de Viena<sup>113</sup>.

En definitiva, uno de los principales problemas de los contratos electrónicos es, como acabamos de ver, la prueba de la aceptación de la oferta electrónica y de sus cláusulas en general. En la contratación electrónica los prestadores de servicios podrán acreditar conforme a sus registros informáticos en qué momento se produjeron los mensajes que constituyen la oferta y la aceptación y perfección del contrato. Pero es importante tener en cuenta que cuando no hay un tercero de confianza, como el prestador de servicios de certificación, el servidor desde el que se emite o recibe el mensaje puede pertenecer o estar bajo el control de una parte interesada. Por otra parte, el emisor, el receptor y el servidor pueden localizarse en países con distinta franja horaria. Si el contrato se realizara mediante firma electrónica avanzada o acreditada por una autoridad de certificación, ésta

podría acreditar las fechas y los contenidos de los mensajes, siendo un instrumento de gran utilidad en aras a la seguridad del comercio electrónico y al que siempre se podrá recurrir, si fuera necesario, como medio de prueba en juicio, como a continuación se estudia.

## **V. Incidencia de la Firma electrónica en la prueba del contrato electrónico.** ➡

### **1. Planteamiento** ➡

Ya sea manuscrita o electrónica la firma no es un elemento estrictamente necesario a efectos probatorios, sino que goza de un carácter meramente instrumental. La seguridad a efectos probatorios se traduce en la existencia de una posibilidad cierta de acreditar que algo jurídico existió, que se produjo entre los sujetos que se afirma y que tuvo el contenido que se alega. Así, al igual que la firma manuscrita constituye un vínculo de unión entre el escrito y el acto jurídico de manifestación de la voluntad, la firma electrónica es apta para satisfacer una función similar en el supuesto de documentos electrónicos. Además, al basarse en datos matemáticos una firma digital será siempre cierta, es decir que funciona o no funciona, sin que sea posible concederle una validez parcial<sup>114</sup>. Por el contrario, en la firma manuscrita los peritos pueden apreciar a través de un examen caligráfico, diferentes grados de probabilidades de autenticidad.

Tanto en un proceso civil internacional como en un proceso civil interno la prueba guarda una directa y estrecha relación con la tutela judicial efectiva que se pretende obtener ante los órganos jurisdiccionales. Si se tratara de un procedimiento abierto en España a la admisibilidad de los medios probatorios y a la fuerza probatoria de los mismos se les aplicará la *lex fori* (ley española, art. 3 Ley de Enjuiciamiento Civil), con excepción de las pruebas preconstituidas en el extranjero cuando cumplan los requisitos del art. 323 Ley de Enjuiciamiento Civil. En cuanto al objeto y la carga de la prueba deberán regirse por la ley aplicable al fondo del asunto (*lex causae* o ley del contrato).

Dos son las cuestiones fundamentales que vamos a tratar respecto de la prueba que aporta la firma electrónica: por una parte, su admisibilidad en juicio (2) y, por otra, los hechos que se entienden probados por su mera utilización en un contrato electrónico (3).

### **2. Admisibilidad de la firma electrónica y del contrato electrónico como prueba en juicio.** ➡

Si el Derecho aplicable a la admisibilidad de los medios de prueba resultara ser el español, el RDLFE establece en su artículo 3 que la firma electrónica equiparada a la manuscrita "será admisible como prueba en juicio"<sup>115</sup>. Esto debe interpretarse como que la actividad probatoria debe versar sobre el contenido del documento y sobre la firma a él asociada, siendo de plena aplicación las normas de reparto de la carga de la prueba, debiendo ser probada por la parte que la alega (art. 217 Ley de Enjuiciamiento Civil). Ahora bien, la admisibilidad como prueba son predicables en nuestro ordenamiento de cualquier firma electrónica, sea esta avanzada o digital o simple, tanto si reúne los requisitos del art. 3 del RDLFE como si no los reúne. Lo que las distingue y parece aportar el dato más relevante es que, si se trata de firma electrónica avanzada, basada en un certificado reconocido expedido por un prestador de servicios de certificación acreditado y producida a través de un dispositivo seguro de creación de firma certificado, es suficiente para probar la identidad del que firma y la integridad del contrato electrónico firmado, sin perjuicio, de que de otros medios de prueba se desprenda lo contrario. Esta parece, en nuestra opinión, una respuesta a la pregunta lanzada en el apartado II de este trabajo sobre la distinción real

entre ambos tipos de firma, recordando además que la avanzada goza de una presunción a su favor.

Por otra parte, si la firma electrónica es admisible como prueba en juicio, también lo es el contrato electrónico que la contiene. Como establece el art. 24 de la Ley 34/2002 de comercio electrónico: "1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetarán a las reglas generales del ordenamiento jurídico y, en su caso, a lo establecido en la legislación sobre firma electrónica. 2. en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental".

### **3. ¿Qué se entiende probado a través de la firma electrónica? ➡**

La cuestión fundamental es, en efecto, determinar qué se entiende probado a través de una firma electrónica. Cuatro aspectos, cuya consideración resulta enormemente importante a efectos de este trabajo, parecen probados con la utilización de una firma electrónica:

Primero. Que la firma pertenece a la persona titular, porque se ha generado mediante la clave privada correspondiente a la clave pública utilizada para verificarla.

Segundo. Que el signatario utilizó la firma en un contrato con plena conciencia de querer ser obligado, puesto que él conoce que por su mera utilización puede ser obligado jurídicamente.

Tercero. Que el contenido del archivo no fue alterado desde que le fue adjuntada la firma electrónica, no pudiéndose admitir afirmaciones relativas a su modificación por un tercero, pues de haberse producido el más mínimo cambio sería detectado inmediatamente.

Cuarto. La fecha y hora en que la firma fue estampada. La utilización de mecanismos de estampado de fecha y hora, que se encuentra cada vez más perfeccionados técnicamente, no se contempla con carácter general en el RDLFE, pero sí se deja abierta la posibilidad de que los prestadores de servicios de certificación proporcionen a sus usuarios otros servicios en relación con la firma electrónica (art. 2), entre los que podrían encontrarse el del marcado de la fecha y hora en el que se utiliza. Ello podría ser importante a la hora de determinar el momento en el que se produce, por ejemplo, la perfección de un contrato. Ahora bien, la ausencia de previsión legal sobre la eficacia de las marcas temporales, implica que el juzgador podrá apreciarlas como válidas en función de su fiabilidad técnica en los términos en que ésta sea presentada por las partes. Cabe advertir que dado que tales servicios pueden ser objeto de acreditación conjuntamente con la aptitud de los prestadores de servicios de certificación para la expedición de certificados reconocidos en los términos del art. 16 del Reglamento de Acreditación de prestadores de Servicios de Certificación y Certificación de determinados productos de firma electrónica<sup>116</sup>, satisfecho este requisito difícilmente podrá el juez desconocer su virtualidad probatoria<sup>117</sup>.

La firma electrónica es, por lo tanto, un instrumento de enorme importancia para probar la existencia del contrato electrónico o de cualquier cláusula del mismo como la elección de la lex contractus e, incluso, del momento de conclusión o perfección del contrato celebrado por medio de Internet.

### **VI. Supuesto práctico ➡**

Un supuesto práctico permite ilustrar lo que hemos visto hasta ahora:

Una empresa de EE.UU. ha posibilitado la compraventa de varios equipos de hardware por parte de una empresa española previo pago de una cantidad. El contrato se ha realizado mediante la página web interactiva de la empresa norteamericana, pulsando el icono "acepto" y sin utilización de firma electrónica alguna, aunque la propia página permitía su utilización. Se trata de un contrato de compraventa de mercancías que se ha formalizado on-line sin firma electrónica y que deberá ejecutarse off-line, y todo ello conforme al Convenio de Viena de 1980, que resulta aplicable por concurrir sus condiciones espaciales, voluntarias y materiales al efecto. La mercancía se entrega FOB Nueva York y el lugar de celebración del contrato electrónico, relevante a efectos de determinar la competencia judicial internacional, por remisión del art. 4 del Reglamento de Bruselas a la LOPJ es, en defecto de elección, el del domicilio del vendedor o prestador de servicios (EE.UU), no siendo relevante donde se encuentra el servidor, que podría estar situado en un lugar aleatorio y sin ninguna vinculación con el asunto. En el caso de incumplimiento -por ejemplo, el vendedor no cumple adecuadamente con su obligación de entrega sin vicios, cargas, etc.-, el comprador podrá demandarle ante los tribunales españoles sólo si concurre alguno de los foros contemplados en la LOPJ. Estando el demandado establecido en EE.UU., y siendo éste también el lugar de la entrega, parece que deja abierto tan sólo el recurso a la autonomía de la voluntad. El hecho de que el contrato electrónico se haya perfeccionado sin el recurso a la firma electrónica avanzada, dificulta, entre otras cosas, la prueba de la perfección del mismo, pero nada afecta a su validez formal.

En el supuesto de que la negociación entre las partes tuviese lugar por medio del intercambio de mensajes de correo electrónico, la firma electrónica sería útil tanto durante la negociación como después de la celebración del contrato. Durante las negociaciones, si el comprador tiene dudas sobre la identidad del vendedor, puede exigir una firma electrónica avanzada que puede verificarse con el prestador de servicios de certificación, firma que tendrá además efectos extraterritoriales si cumple con la normativa comunitaria. Si el comprador duda de la integridad de los mensajes, puede usar el sistema de llave privada / llave pública para comprobar su integridad. La confidencialidad de las negociaciones puede asegurarse igualmente mediante el uso de la firma electrónica avanzada. Finalmente, si después de la celebración del contrato el vendedor intenta repudiar el contrato, alegando que nunca lo firmó, el comprador puede acudir al uso de la firma electrónica avanzada para demostrar que únicamente el vendedor tenía acceso a la llave privada usada para encriptar la firma y el mensaje de aceptación del contrato.

## **VII. Conclusión ➔**

En conclusión, en todos los casos en los que el Derecho aplicable al contrato exija que éste se celebre por escrito y por ende la firma manuscrita para su validez, en la contratación electrónica será necesaria e imprescindible la firma electrónica avanzada, en la medida en que la ley aplicable equipare los efectos jurídicos de ambas y el documento electrónico al documento en formato papel. Esto sucederá en todos los países miembros de la Unión Europea y en los países donde siguen las pautas marcadas por los instrumentos internacionales mencionados *supra*<sup>118</sup>. En los ordenamientos jurídicos que no requieren la forma escrita para los contratos, ni como requisito de validez ni como expresión de voluntad, la firma electrónica puede tener un valor de enorme importancia como instrumento de seguridad y prueba del contrato, del momento y lugar de perfeccionamiento del mismo, en definitiva, de los aspectos importantes de la negociación del mismo.

Existe, no obstante, barreras de adopción, y en aras a la seguridad de la contratación internacional cada vez más en aumento en Internet, es muy importante que los ordenamientos jurídicos tomen medidas para hacer accesibles a los usuarios las firmas electrónicas y el reconocimiento de la extraterritorialidad de sus efectos. Hacer accesible

significa facilitar el acceso físico (tecnología), la comprensión del funcionamiento y los beneficios jurídicos y prácticos de la firma electrónica. De lo contrario, los comerciantes siempre tendrán el problema práctico de su aparente difícil uso y comprensión, y seguirán prefiriendo otras formas de contratar a pesar de los riesgos que éstas implican. ¿Cómo se puede, entonces, aumentar el uso de la firma electrónica? La respuesta vendrá de la mano del tiempo, de los cambios en el mercado y de una necesaria adaptación de la legislación que permita eliminar las trabas prácticas al uso de la firma electrónica. Esta necesidad se hace patente en el Proyecto español de firma electrónica que pretende corregir los defectos del prematuro RDLFE, haciendo por fin de la firma electrónica un instrumento más eficaz y útil. Por otra parte, conforme la generación joven que creció “con el ratón en la mano” (y por lo tanto se siente cómoda con la tecnología) asuma puestos directivos, seguramente irá creciendo el uso de la firma electrónica. También hay que tener en cuenta el crecimiento de ataques de “hackers” que pueden llegar a un nivel tal que a corto plazo los comerciantes se convencerán de que hay suficiente ventaja práctica en un sistema de firmas y documentos protegidos por la firma electrónica.

En la UE, se ha establecido un marco jurídico extenso y bien pensado para supervisar y fomentar el uso de la firma electrónica. De esta manera, y en nuestra opinión, la firma electrónica consigue efectos superiores a la firma manuscrita pues proporciona seguridad al contrato electrónico que se esté realizando: integridad, autenticidad, confidencialidad y no rechazo en origen. Por ello, las iniciativas legislativas sobre firma electrónica la equiparan, con más o menos exigencias, a la firma manuscrita, estableciendo, además, presunciones a favor de la validez de la firma electrónica. Queda por verse si en el mundo comercial, las ventajas superarán las desventajas para empujar a la comunidad empresarial nacional e internacional a su adopción como método usual de contratación B2B a través de Internet.

---

1: Vid. CALVO CARAVACA, A.L., “Contratos internacionales II. Algunos contratos”, en CALVO CARAVACA, A.L. y CARRASCOSA, J. (dir.), Derecho internacional Privado, vol. II, Comares, Granada, 2003, p. 460. Esta nueva economía es el resultado de la conjunción de tres factores: la proliferación de bienes intangibles, la creciente interconexión mediante redes de telecomunicaciones e Internet de los sujetos y bienes económicos y la globalización de la economía como consecuencia de las nuevas tecnologías y liberación de los mercados (Vid. BÁNEGAS NÚÑEZ, J., “El planeta Internet: la economía interconectada”, en CREMADES, J. e ILLESCAS, R. (coord.), Régimen jurídico de Internet, Madrid, La Ley, 2002, pp. 65. ➡

2: La categoría de contrato electrónico no es una realidad exclusiva de Internet. La Red de redes es sólo uno de los medios de comunicación utilizados para la formación del contrato electrónico. Existen además contratos concluidos mediante el intercambio electrónico de datos en redes cerradas (EDI). Los aspectos jurídicos controvertidos de ambos contratos electrónicos (valor jurídico, seguridad y prueba...) son coincidentes, aunque en los contratos electrónicos concluidos en Internet, se plantean en términos diferentes (Vid. DE MIGUEL ASENSIO, P. Derecho privado de Internet, 3ª ed., Civitas, Madrid, 2002, pp. 333 y ss.). ➡

3: Vid art. 2.1 Decreto-Ley 14/1999 sobre firma electrónica (RDLFE), BOE núm. 224, de 18 de septiembre de 1999. Disponible en <http://www.uaipit.com> . ➡

4: Vid. epígrafe correspondiente. ➡

5: Vid. DE MIGUEL ASENSIO, P. Derecho privado de Internet, cit., p.329. ➡

6: Como se ha reconocido, Internet es transnacional por naturaleza, vid. en este sentido, KESSEDJIAN, C., “Rapport de synthèse”, en BOLEE-WOELKI/ KESSEDJIAN, C. (Eds.), Internet, Which Court decides? Which Law applies? Quel Tribunal decide?, Kluwer, La Haya, 1998, 143-154; BURNSTEIN, M.R., “Conflicts on the Net: Choice of Law in transnational Ciberspace”, Vanderbilt Journal of Transnational Law, núm.29, 1996, pp. 75-110; PERRIT, JR., “Jurisdiction in Ciberspace”, Villalonga Law Journal, núm. 41, 1996, pp. 1-128; y CALVO CARAVACA, A.L. y CARRASCOSA, J., Conflictos de leyes y de jurisdicciones en Internet, Colex, Madrid, 2001. ➡

7: DOCE C27, de 26 de enero 1998; BOE núm. 171, de 19 de julio de 1993; corrección de errores, BOE núm. 189, de 9 de agosto de 1993. ➡

8: Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, DOCE, L 13 de 19 de enero 2000. ➡



**9:** Directiva 2000/31 del Parlamento europeo y del Consejo relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular del comercio electrónico en el mercado interior (Directiva sobre comercio electrónico) de 8 de junio de 2000, DOCE, L 178, de 17 julio 2000. ➡

**10:** Vid. DESANTES REAL, M. "La Directiva sobre el comercio electrónico. Mercado interior y servicios financieros de la sociedad de la información", en Derecho de Internet (contratación electrónica y firma digital), Aranzadi, Navarra, 2000, pp. 323-338. ➡

**11:** En el ámbito internacional organizaciones como UNCITRAL (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional), la Organización Mundial de Comercio o la Cámara de Comercio Internacional (CCI) han realizado iniciativas de regulación de los contratos electrónicos (SOERIEUL, R. "Brief Overview of International Initiatives for an Electronic Commerce Uniform Legal Framework", Uniform Law Review, 1999, pp. 908-926). Debido a las características de Internet, instrumentos flexibles como leyes modelo o códigos de conducta son los que más han fructificado y son una referencia al legislador estatal. Así, La Ley Modelo sobre Comercio Electrónico de UNCITRAL de 16 de diciembre de 1996 (disponible en <http://www.uncitral.org/spanish/texts/electcom/ml-ec.html>), ha tenido gran incidencia en las reformas legislativas de muchos países latinoamericanos y en la Uniform Electronic Transactions Act, adoptada en EE.UU. en julio de 1999 por la National Conference of Commissioners on Uniform State Laws (dichas leyes nacionales pueden encontrarse en <http://www.uaipit.com>). También debe destacarse La Ley Modelo sobre firmas electrónicas de 24 de enero de 2002 (disponible en <http://www.uncitral.org>); los Principios sobre contratos comerciales internacionales de UNIDROIT (Roma, 1995); y, en fin, la elaboración por la CCI de reglas que promueven la autorregulación en los contratos electrónicos como los E-terms, términos jurídicos susceptibles de ser incorporados por referencia en los contratos electrónicos. ➡

**12:** Vid., por todos, MARTINEZ NADAL, A., Comercio electrónico, firma digital y autoridades de certificación, 3ª ed., Civitas, Madrid, 2001, p. 25 y ss.; id., "Comercio electrónico", en BOTANA GARCÍA, G. y RUIZ MUÑOZ, M., Curso de protección jurídica de los consumidores, MacGraw-Hill, Madrid, 1999, p. 248. ➡

**13:** Cit. nota 3 supra. ➡

**14:** Sobre la definición de firma electrónica avanzada vid. infra II. ➡

**15:** Los contratos electrónicos pueden celebrarse entre empresas (business to bussines, B2B), entre empresas y administración (business to administration, B2A), entre empresas y consumidores (business to consumers, B2C), entre consumidores (consumers to consumers, C2C) o entre particulares (peer to peer P2P). Con la finalidad de centrar la exposición, las páginas que siguen se circunscriben a la primera modalidad señalada (B2B), con independencia de que muchos aspectos de la contratación B2B puedan aplicarse también a las otras modalidades. ➡

**16:** "Probablemente la forma más admitida en Derecho y más generalizada para acreditar la identidad de la persona es su firma." CALVO-SOTELO, A. y LOBO COELLO, M., "La Firma Electrónica", en CREMADES, J., FERNÁNDEZ-ORDONEZ, M. e ILLESCAS, R., (coord.) Régimen Jurídico de Internet, La Ley, Madrid, 2002, p. 1375. ➡

**17:** Vid. VILLAR, J., "Una aproximación a la firma electrónica", en MAREU ROS, R. y MÉNDEZ DE VIGO, J.M., Derecho de Internet. Contratación Electrónica y Firma Digital, Aranzadi, Madrid, p. 170. ➡

**18:** El problema de la sustitución de páginas, párrafos o palabras se puede combatir hasta cierto punto requiriendo que las partes firmen con sus iniciales cada página y hasta a veces cada párrafo importante (a veces la ley aplicable requiere las iniciales para la validez del contrato, especialmente cuando se trata de renunciar derechos fundamentales), pero este método tiene sus límites. Hay que tomar en consideración que en el mundo real, con muchas negociaciones y cambios de última hora en la redacción y formación de los contratos, es frecuente que las partes se envíen una a la otra varios fax y la firma final por fax, y no es muy práctico enviar por fax treinta, sesenta o cien páginas con iniciales. A menudo se envían la página que contiene las firmas y las páginas con los párrafos importantes con iniciales, con entrega posterior por courier de las páginas con firma manuscrita e iniciales. ➡

**19:** Por hackers se entiende: "Aquellos usuarios de Internet que, violando las barreras de seguridad, acceden a ordenadores de uso restringido y a la información en ellos contenida" (vid., MONTESINOS, A., La sociedad de la información e Internet. Fundamentos, aptitudes y uso de la red, San Pablo, Madrid, 1999, p. 103). ➡

**20:** MADRID PARRA, A., "Seguridad en el Comercio Electrónico," en F.J. ORDUÑA MORENO (dir.), Contratación y comercio electrónico, Tirant lo Blanch, Valencia, 20003, p. 130. ➡

**21:** Vid., por todos, BRAZELL, "Electronic Security: Encryption in the Real World", European Intellectual Property Review (EIPR), vol. 21, 1999, pp. 17-27. ➡

**22:** Vid. MARTINEZ NADAL, A., Comercio electrónico, firma digital..., cit. pp. 45 y ss. También existe la llamada simétrica, en la que la misma llave electrónica encripta y desencripta los documentos. Esta modalidad es mucho menos segura que la asimétrica, porque no es capaz de proveer información sobre posibles alteraciones del documento electrónico o sobre la autenticidad de firmas electrónicas. ➡

**23:** En muchos casos, las llaves públicas se publican para amplia difusión al público en general. En tales casos, no existe la intención de mantener la confidencialidad del documento, sino de acreditar la autoría y la integridad del documento, porque una llave pública sólo puede abrir el documento encriptado de su correspondiente llave privada, cuya titularidad se puede comprobar, y si el documento ha sido alterado, la llave pública no podrá abrirlo,

quedando patente así que alguien ha modificado el documento. ➡

**24:** KUNET, C. "Legal Aspects of Encryption in the Internet, International Business Lawyer, 1996, pp. 186-190. ➡

**25:** Por todos, MADRID PARRA, A., "Seguridad en el Comercio Electrónico, cit. supra, p. 131. ➡

**26:** RIBAGORDA GARNACHO, A., "Sistema de certificación: la firma y el certificado digital", en J. CREMADES y OTROS (dirs.), Régimen jurídico de Internet, cit. supra, p. 1332. ➡

**27:** Entre ellas en España, La Fábrica Nacional de Moneda y Timbre <http://www.fnmt.es/faq.html> , CAMERFIRMA (avalada por las Cámaras de Comercio) y la Agencia de Certificación Electrónica <http://www.ace.es> . Vid. CALVO-SOTELO, A. y LOBO COELLO, M., "La Firma Electrónica", en J. CREMADES y OTROS (dirs.), Régimen jurídico de Internet, cit., p. 1393. ➡

**28:** RIBAGORDA GARNACHO, A., cit. supra, p. 1333. ➡

**29:** MARTINEZ NADAL, A., Comercio..., cit. supra, pp. 63-77; y JACCARD, M., "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 H. Dessemont), Lausana, 1998, pp. 403-427. ➡

**30:** BARRIUSO RUIZ, C., La Contratación Electrónica, Editorial Dykinson, Madrid, 2002, pp. 349-350. ➡

**31:** Por ejemplo, en EEUU, un intento de conseguir un estándar fracasó con el denominado Digital Signature Standard, debido a que alguien logró descifrarla. BARRIUSO RUIZ, C., La Contratación Electrónica, Editorial Dykinson, Madrid, 2002, p. 309. ➡

**32:** Vid. RICHARDS, R.J., "The UTA Digital Signature Act As Model Legislation: A Critical Analysis", Journal of Computer & International Law, vol. XVII, 1999, pp. 873-907. ➡

**33:** Todas ellas pueden encontrarse en <http://www.uaipit.com> . ➡

**34:** En este sentido la Ley de los EE.UU a nivel federal: Electronic Signatures in Global and National Commerce Act de 2000. Disponible en <http://www.uaipit.com> . ➡

**35:** Real Decreto-Ley 14/1999, sobre firma electrónica, cit. supra. ➡

**36:** Así, el Preámbulo del RDLFE alude a la Propuesta de 13 de mayo de 1998 (COM (1999) 297 final) y a la Propuesta modificada de 29 de abril de 1999 (COM (1999) 195 final). ➡

**37:** Directiva 1999/93, sobre firma electrónica, cit. supra. ➡

**38:** Vid. MARTINEZ NADAL, A., La ley de firma electrónica, Madrid, 2000, pp. 15 y 16 y 312. Curiosamente esta apresuración en la regulación nacional también ocurrió en otros Estados miembros como Alemania e Italia. Dichas Leyes estatales de Firma electrónica pueden encontrarse en la sección de documentos de <http://www.uaipit.com> . ➡

**39:** Disponible en <http://www.mcyt.es> . Entre las modificaciones previstas en el Proyecto destacan: 1) el establecimiento de un marco básico para un documento Nacional de Identidad (DNI) electrónico, que permitirá a los ciudadanos identificarse y firmar documentos; y 2) la regulación de los certificados de firma electrónica de personas jurídicas. ➡

**40:** Directiva 99/93, art. 2 (1) y (2); RDLFE, art. 2 (a) y (b). ➡

**41:** Directiva 99/93, art. 2 (2); RDLFE, art. 2 (b). ➡

**42:** Directiva 99/93, art. 2 (9); RDLFE, art. 2 (i). ➡

**43:** Directiva 99/93, art. 2 (10); RDLFE, art. 2 (j). ➡

**44:** Por ejemplo, el período de validez del certificado y los límites de uso y valor de transacciones. Ver la Directiva 99/93, Anexo I; y el RDLFE, art. 8. ➡

**45:** Ver la Directiva 99/93, Anexo II; el art. 12. El RDLFE impone condiciones más específicas que la Directiva 99/93. Por ejemplo, el requisito del RDLFE de que la garantía por daños fija la cantidad inicial del 4 por ciento de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados emitidos, reducible al 2 por ciento posteriormente. La Directiva 99/93 simplemente requiere "recursos económicos suficientes" para afrontar el riesgo de responsabilidad por daños. También el RDLFE requiere la retención de la documentación relativa a certificados reconocidos por 15 años. Respecto de otros requisitos del RDLFE para todos los prestadores de servicios, ver infra. ➡

**46:** Art. 3 Directiva. ➡

**47:** "Los Estados miembros no condicionarán la prestación de servicios de certificación a la obtención de autorización previa" (art. 3 (1) Directiva). ➡

**48:** Art. 3.2 Directiva 99/93. ➡

**49:** RDLFE, art. 6. El Reglamento específico para estas funciones se aprobó con el Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de Acreditación de los Prestadores de Servicios de Certificación y de Certificación de determinados productos de firma electrónica de 22 de febrero (BOE núm. 45, 2000). ➡

**50:** Art. 7 RDLFE. ➡

51: Art. 11 RDLFE. ➡

52: Art. 17 RDLFE. ➡

53: Art. 6 de la Directiva 99/93. ➡

54: Art. 6. 3 y 4 Directiva 99/93. ➡

55: Art. 14 RDLFE. ➡

56: Art. 14.2 RDLFE. Tanto la Directiva 99/93 como el RDLFE contemplan una excepción respecto de la protección a consumidores (art. 6 Directiva 99/93, art. 6 (5); y art. 14.4 RDLFE). ➡

57: MARTINEZ NADAL, A., "La firma electrónica como equivalente funcional. Espejismo o realidad", en PERALES SANZ, J.L. (dir.), La seguridad jurídica en las transacciones electrónicas, Civitas, Madrid, pp. 177 y ss. esp. p. 199. ➡

58: Art. 5 Directiva 99/93. ➡

59: Art. 2.3. RDLFE. ➡

60: Vid. la explicación supra. ➡

61: Art. 2 (6) Directiva 99/93, que incorpora el Anexo III. ➡

62: Art. 5.1 Directiva 99/93. ➡

63: Art. 3.1 RDLFE. ➡

64: Art. 3.1 RDLFE. ➡

65: Art. 7 Directiva 99/93; art. 10 RDLFE. ➡

66: DE MIGUEL ASENSIO, P.A., Derecho privado de Internet, cit. p. 421. ➡

67: El art. 8 de la Directiva 99/93, remite a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (DOCE núm. 281, de 23 de noviembre de 1995); y el art. 15 RDLFE, envía a la Ley Orgánica 5/1992, de 29 de octubre, derogada por la Disposición Derogatoria Única de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE, núm. 151, de 25 de junio de 1999). Es importante tener en cuenta también la Directiva 97/66/CE del Parlamento europeo y del Consejo, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (DOCE núm. 24, de 30 de enero 1998). ➡

68: Directiva 99/93, art. 8 (3); RDLFE, art. 15 (3). Sobre protección de datos vid., por todos, ORTEGA GIMENEZ, A. "La protección de datos de carácter personal en Internet (con especial referencial referencia a la transferencia internacional de datos)", en la sección de publicaciones: trabajos de investigación "doctoraro" <http://www.uaipit.com>. ➡

69: BARRIUSO RUIZ, C., cit., p. 310. ➡

70: El 22 diciembre de 2000 se adoptó el Reglamento 44/2001 (DOCE L 12, de 16 enero, p. 3) que desde el 1 de marzo del 2002 ha sustituido al Convenio de Bruselas (vid. nota infra) relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (excepto en las relaciones con Dinamarca). ➡

71: Convenio relativo a la competencia judicial internacional y el reconocimiento y ejecución de decisiones en materia civil y mercantil (DOCE C 27, de 26 enero 1998, p. 1). En 1988 con un contenido prácticamente idéntico y con el mismo título que el Convenio de Bruselas se aprueba el Convenio de Lugano, llamado también "Convenio paralelo", aplicable por los jueces comunitarios y por los jueces del Espacio Europeo de Libre Cambio, para determinar la competencia judicial internacional a los litigios vinculados a Islandia, Liechtenstein, Noruega, Suiza y Polonia (BOE 251, de 20 de octubre de 1994). ➡

72: Cit. supra. ➡

73: La forma EDI (Electronic Data Interchange) es la forma más consolidada de comercio electrónico cerrado, normalmente requiere de una larga fase de negociación entre las partes implicadas en la transacción electrónica. Vid. JULIÁ BARCELÓ, R., Comercio electrónico entre empresarios, la formación y prueba del contrato electrónico (EDI), Tirant lo Blanc, Valencia, 2000; RUBIA, M., "EDI and Digital Signatures for Business to Business Electronic Commerce", JURISMETRICS, vol. 38, 1998, pp. 497 y ss. ➡

74: VIRGOS SORIANO, M., Lugar de celebración y de ejecución en la contratación internacional, Tecnos, Madrid, 1989. ➡

75: Cit supra. ➡

76: Cit supra. ➡

77: En virtud del Reglamento de Bruselas 44/2001, son competentes los tribunales del Estado parte al que los contratantes se hayan sometido tácitamente (art. 24) con independencia de donde estén domiciliados, o se hayan sometido expresamente (art. 23), si al menos una de las partes está domiciliada en la UE. En segundo término son competentes los tribunales del domicilio del demandado (art. 2), demandado contra el que también podrá

plantearse la demanda ante el tribunal del lugar donde hubiera sido o debiera ser cumplida la obligación que sirve de base a la demanda (art. 5.1). ➡

**78:** BOE núm. 157, de 2 de julio y corrección errores BOE núm. 264 de 4 de noviembre 1985. ➡

**79:** Según el art. 4 si el demandado no tuviere su domicilio en un Estado contratante, la competencia judicial internacional se determinará en cada Estado contratante por la ley de ese Estado (en España LOPJ), sin perjuicio de la aplicación de lo dispuesto en el art. 22 (ex 16 Convenio de Bruselas); o del art. 23 (ex art. 17 Convenio de Bruselas) dado que para su aplicación basta con que una de las partes esté domiciliada en un estado miembro; y del art. 24 (ex art. 18 Convenio de Bruselas), dado que este artículo se aplica con independencia del domicilio de las partes. ➡

**80:** Los tribunales españoles son competentes si las partes se han sometido expresa o tácitamente a los tribunales españoles o si el demandado está domiciliado en España (art. 22.2 LOPJ); en su defecto, también serán competentes en materia de obligaciones contractuales si estas han nacido o deben cumplirse en España (art. 22.3 LOPJ). ➡

**81:** El art. 4 del Reglamento 44/2001, del Convenio de Bruselas y del Convenio de Lugano sobre Competencia judicial internacional, reconocimiento y ejecución de decisiones establece que si el "demandado no estuviese domiciliado en un Estado miembro, la competencia judicial internacional se regirá en cada Estado miembro por la ley de ese Estado miembro...". ➡

**82:** Convención de las Naciones Unidas sobre los contratos de compraventa internacional de mercaderías, hecha en Viena el 11 de abril de 1980 (BOE, núm. 26, de 30 de enero 1981; corrección de errores, BOE núm. 282, de 22 de noviembre de 1996). ➡

**83:** Cit. supra. ➡

**84:** Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE núm. 166, de 12 de julio 2002. Disponible en <http://www.uaipit.com>. Dicha Ley transpone al Derecho español la Directiva 2000/31/CE de comercio electrónico, citada supra. ➡

**85:** DE MIGUEL ASENSIO, P.-A., Derecho privado de Internet, cit. p. 468. ➡

**86:** CALVO CARAVACA, A.-L., "Contratos internacionales business to business on line (B2B)", cit. supra, p. 465. ➡

**87:** En virtud del art. 2 del Convenio de Roma, éste tiene carácter universal dado que la ley designada por el Convenio se aplica incluso si esta es la ley de un Estado no contratante. Sobre el Convenio de Roma, vid., por todos, CALVO CARAVACA, A.L. y CARRASCOSA, J. "El Convenio de Roma sobre la ley aplicable a las obligaciones contractuales de 19 junio 1980" en A.L. CALVO CARAVACA y L. FERNÁNDEZ DE LA GANDARA, Contratos internacionales, Madrid, Tecnos, 1997. ➡

**88:** CALVO CARAVACA, A.L., "Contratos internacionales business to business on line (B2B)", cit. supra, p. 466; y DE MIGUEL ASENSIO, P.A., Derecho privado de Internet, cit. p. 513. ➡

**89:** Cit. supra. ➡

**90:** Cit. supra. ➡

**91:** En este sentido, CALVO CARAVACA, A.L. y CARRASCOSA, J., "Problemas de extraterritorialidad en la contratación electrónica", en ECHEVARRÍA SAÉN, J.-A. (coord.), El comercio electrónico, Edisofer, Madrid, 2001, p. 186. ➡

**92:** Si bien de lo dispuesto en los arts. 12 y 96 del Convenio de Viena se deduce la necesidad de considerar las soluciones previstas en materia de forma en una legislación nacional, por encima de lo establecido en el art. 11 del Convenio. ➡

**93:** No obstante, en el art. 3.2 RDLFE se establece que los documentos electrónicos no firmados a través de la firma electrónica avanzada sino de firmas electrónicas no garantizadas mediante una autoridad de certificación también gozan de efectos jurídicos. ➡

**94:** Vid. MATEU ROS, R. y CENDOYA, J.M., "El consentimiento y el proceso de contratación electrónica" en Derecho de Internet (contratación electrónica y firma digital), cit., p. 29. ➡

**95:** Arts. 3, 5, 83, a), 2 de la Ley 50/1980 de 8 de octubre de Contrato de Seguro. ➡

**96:** Arts. 6 y ss. Ley 7/1995, de 23 de marzo, de Crédito al Consumo. ➡

**97:** Arts. 3, 4 y 6 Ley 21/1995, de 6 de julio, de regulación de los Viajes Combinados. ➡

**98:** Art. 6 Ley 28/1998, de 13 de julio, de Venta a Plazo de Bienes Muebles. ➡

**99:** Art. 19 Ley 12/1992, sobre Contrato de Agencia ➡

**100:** ECHEVARRIA SAENZ, J.A., "El comercio electrónico entre empresarios", cit. p. 133 y 134. ➡

**101:** Citadas supra. ➡

**102:** Es aconsejable añadir en la oferta electrónica un plazo de validez, por ejemplo "la oferta será válida hasta que se modifique la web" (RIVAS, J., Aspectos jurídicos del comercio electrónico en Internet, Aranzadi, Madrid, p.

72) y también sería adecuado indicar los países para los que es válida la oferta. ➡

**103:** El sistema de listas positivas Opt-in se ha establecido en la mayoría de los países de la UE. Existen otros Estados que siguen el modelo Opt-out. El llamado "Spam" o publicidad no deseada queda prohibido en España bajo esta ley. ➡

**104:** Sobre las consecuencias del carácter instantáneo o no de los medios electrónicos, vid. RECALDE CASTELLS, A, "Comercio y contratación electrónica", Informática y Derecho, núms. 30-32, 1999, pp. 39-87. ➡

**105:** ECHEVARRIA SÁENZ, J.A., "El comercio electrónico entre empresarios", cit., p. 109. ➡

**106:** Así, la Jurisprudencia Norteamericana (Decisión de julio de 2001, Asunto Specht v. Nescape and AOL (S.D.N.Y.), 2001 U.S. Dist. LEXIS 9073) ha puesto de relieve que cuando la descarga a través de Internet de la información objeto de contrato tuvo lugar sin que el adquiriente hubiera manifestado la aceptación de los términos, que sólo se mostraban una vez que el programa hubiera sido descargado en el ordenador. Este tipo de adquisición por navegación en Internet que se ha denominado browse-wrap, no se considera aceptable, como sí lo son, sin embargo, shrink-wrap y click-through. Vid. DE MIGUEL ASENSIO, P., Derecho Privado de Internet, cit., p. 356. ➡

**107:** Más allá de los requisitos mínimos de la ley, cabe señalar que al comerciante le conviene dotar el sistema informático de una serie de pasos redundantes para reducir al mínimo la posibilidad de que el usuario indique su aceptación por confusión o accidente. Cualquier usuario frecuente de Internet puede comprobar que de hecho muchos comerciantes así lo hacen. ➡

**108:** Todo ello resulta más sencillo en los contratos electrónicos celebrados en el sistema EDI en la medida en que el sistema informático prediseñado establece que documento constituye oferta y cómo se formula y qué mensaje constituye aceptación. Este sistema debería inspirar la contratación en Internet. ➡

**109:** El actual art. 54 del Código de comercio, modificado por la Ley 34/2002, establece que "en los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación", por lo tanto, con independencia de si el oferente ha conocido esa manifestación de voluntad. ➡

**110:** Vid. Orden Ministerial de 22 de marzo de 1996. ➡

**111:** Directiva 2000/31/CE, cit. supra. ➡

**112:** La Directiva 2000/31/CE considera que el pedido o aceptación y el acuse de recibo han sido recibidos "cuando las partes a las que se dirigen puedan tener acceso a los mismos", mientras que la Ley 34/2002 establece que "se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello", entendiéndose que cuando la aceptación se confirme mediante acuse de recibo "se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que éste dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones". ➡

**113:** Vid. ECHEVARRIA, J.A., "El comercio electrónico entre empresas", cit., p. 114. ➡

**114:** Vid. PEREZ GIL, J., "Documento informático y firma electrónica: aspectos probatorios", en ECHEVARRIA, J.A., cit., pp. 219 y ss., esp. pp. 241-260. ➡

**115:** Art. 3. 1 en relación con el art. 3.2 RDLFE. Esta admisibilidad valdría tanto para la firma electrónica simple como para la avanzada. ➡

**116:** Inserto como Anexo y aprobado por la Orden de 21 de febrero de 2000 (BOE de 22 de febrero 2000). ➡

**117:** PÉREZ GIL, J., "Documento informático y firma electrónica: aspectos probatorios", en ECHEVARRIA, J.A., El comercio electrónico, cit., pp. 261 ➡

**118:** Vid. nota supra. ➡