

## LA FIRMA ELECTRÓNICA EN EL DERECHO PRIVADO

LUIS FAJARDO LÓPEZ\*

*SUMARIO:* I. INTRODUCCIÓN. II ¿QUÉ ES LA FIRMA ELECTRÓNICA? III. ANÁLISIS JURÍDICO DE LA FIRMA ELECTRÓNICA. 1. El marco comunitario. 2. La forma del contrato. a) En otros países comunitarios. Especial referencia a Alemania. b) En España. 3. La prueba del contrato. Firma electrónica en los procesos civiles: a) En Alemania. b) En España. IV CONCLUSIONES. 1. De Derecho privado. 2. De Derecho constitucional.

### I. INTRODUCCIÓN

Buenas tardes. En primer lugar quiero agradecer la invitación y el esfuerzo de coordinación realizado por la RJUAM para organizar estas Jornadas, y muy especialmente a quienes, por lo que me consta, más directamente han llevado el peso de la misma, Raquel Escutia y Mario Maraver<sup>1</sup>.

Me es muy grato volver a este lugar, a esta Facultad de Derecho, con la presencia de muchos amigos y compañeros que hoy reencuentro en las mismas aulas donde aprendimos que la ciencia que estudiamos, la Ciencia del Derecho, solamente se justifica en la medida en la que contribuya a solucionar problemas sociales. Es por eso que creo que hay que partir de la base del conocimiento de los problemas que se pretenden estudiar. De sus implicaciones sociales, económicas y, en las sociedades en que vivimos, y muy especialmente en lo que atañe al tema de estas jornadas, técnicas. Sólo entonces podremos aclarar el Derecho que le es de aplicación, que sin duda es el mismo que rige el resto de las relaciones humanas, pues no hay ninguna relación nueva

---

\* Prof. Asoc. de Derecho Civil de la Universidad de Gerona

<sup>1</sup>. Agradezco también la inestimable ayuda de mi amigo y colega Till PENSE, abogado en Frankfurt am Main y doctorando de la Humboldt Universität zu Berlin, en la comprensión de algunos aspectos relativos al ordenamiento alemán, y sin el cual esta ponencia sería muy distinta.

bajo el paraguas de las nuevas tecnologías, sino tan sólo una nueva forma de manifestar las mismas ancestrales relaciones sociales.

De ahí que mantendré que las exigencias de la técnica lo que exige, en su caso, son modificaciones aclaratorias, y no tanto una nuevas regulaciones. Lo que requiere es recomponer la sistemática de unos códigos decimonónicos superados en parte por el devenir de los tiempos, por las profundas modificaciones culturales y técnicas que ha experimentado el mundo desde que Alonso Martínez y sus contemporáneos dieran a España un Código que ha sabido aguantar el paso de más de un siglo de historia. Lejos de esto, las nuevas normas nacionales, están creando un nuevo y especial derecho “general” de obligaciones y contratos electrónicos. Supone sin duda una peligrosa tendencia desde el punto de vista de la técnica legislativa, de la claridad del sistema, de su coherencia interna, y del respeto al principio de igualdad, porque no me parece que el distinto tratamiento que reciben los negocios celebrados por medios telemáticos y en forma tradicional esté justificado de ninguna manera. Es más, el propio legislador no es consciente de estar creando una doble legislación, y así en las exposiciones de motivos<sup>2</sup> de estos textos dice no hacer otra cosa que interpretar y aclarar el ordenamiento jurídico existente.

Por todo ello considero conveniente analizar cómo se están solucionando estos problemas en Alemania, país que está abordando la mayor reforma jamás habida de su histórico Código civil y cuyo contraste con nuestras normas puede alumbrar mucha luz sobre lo que está significando este modo de hacer legislación.

Pero antes de meternos en faena es necesario saber, como he dicho, cuál es la base fáctica real, técnica, o socioeconómica que vamos a regular, o cuya regulación queremos analizar. Empecemos con ello.

## II. ¿QUÉ ES LA FIRMA ELECTRÓNICA?

El escaso conocimiento sobre las técnicas que se pueden emplear para firmar cualquier documento electrónico exige explicar, siquiera sea brevemente, qué debe entenderse cuando hablamos de firma electrónica y de documento firmado electrónicamente.

---

<sup>2</sup> Así el R.D. 14/1999 sobre firma electrónica, o el anteproyecto de Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (última versión de 30 de abril de 2001). Esta misma idea de respeto a los ordenamientos nacionales existentes está también en la Directiva 31/2000/CE de comercio electrónico.

Comencemos por ver qué es un documento electrónico: Un documento es, a nuestros efectos, una serie de caracteres; esto es, todo conjunto de letras, números y otros símbolos previamente establecidos convencionalmente. Estos conjuntos pueden dar lugar a archivos de texto, a correos electrónicos, e incluso a programas de ordenador y, en general, cualquier archivo electrónico puede ser en última instancia reducido a una serie de símbolos<sup>3</sup>. Limitaremos nuestro ámbito de estudio a los documentos que contengan texto, que son los que pueden ser vehículo de declaraciones de voluntad.

La firma electrónica no es otra cosa que una técnica para verificar que un documento ha sido realizado por el poseedor de determinado algoritmo (lo que se conoce como llave privada). Firmar electrónicamente consiste en realizar una operación matemática que convierte el documento original en otro nuevo, cuyos caracteres guardan con el original una relación matemática basada en el algoritmo de cifrado. Este nuevo documento es ininteligible, y sólo sirve para verificar que el documento original (que poseemos y contiene una declaración de voluntad inteligible) guarda con el segundo la esperada relación matemática basada en el algoritmo de cifrado<sup>4</sup>.

Esta comprobación se puede efectuar de dos formas. La primera, distribuyendo al emisor y al receptor el algoritmo de cifrado (firma simétrica), lo que servirá dentro de una misma organización para evitar interceptaciones de información por terceros, o cuando las partes tengan unos mismos intereses, pero no para contratar<sup>5</sup>, ya que entonces se parte de la base de que hay que poner de acuerdo determinados intereses. Esto es, no sirve para garantizar que la declaración de voluntad no ha sido manipulada por el receptor de la misma, pues éste también posee el algoritmo de cifrado.

---

<sup>3</sup> Ciertamente dependiendo del archivo del que se trate ese conjunto puede verse reducido, hasta poder llegar al nivel mínimo compuesto por unos y ceros, sobre el que se basa cualquier información guardada de modo electrónico. No trataremos esta cuestión aquí, pues lo que perseguimos es encontrar la manera en la que puede garantizarse la veracidad de una voluntad negocial emitida por medio electrónico.

<sup>4</sup> Los algoritmos de cifrados usados hasta la actualidad (RSA, DSA, DSAE) se basan en el problema matemático de la factorización entera, o en el de algoritmos en grupos abelianos; la computación cuántica ha hecho inútiles estos tipos de algoritmos, lo que se ha solucionado cambiando la base matemática de esos mismos criptosistemas, pasando a basarse en el problema de Lattices, o de retículas.

<sup>5</sup> Salvo acuerdo previo o relación de tracto continuado, lo que sólo es una parte de la contratación en red.

Para conseguir este último fin, se recurre al sistema de firma asimétrica<sup>6</sup>. Ésta se basa en dos algoritmos distintos, que a su vez guardan una relación entre sí, de tal modo que es posible usar uno (llamado llave privada) para producir el documento ininteligible, y otro (llamado llave pública) para comprobar que dicho documento guarda la relación esperada con el documento original. Es lo que se refleja en el gráfico 1.

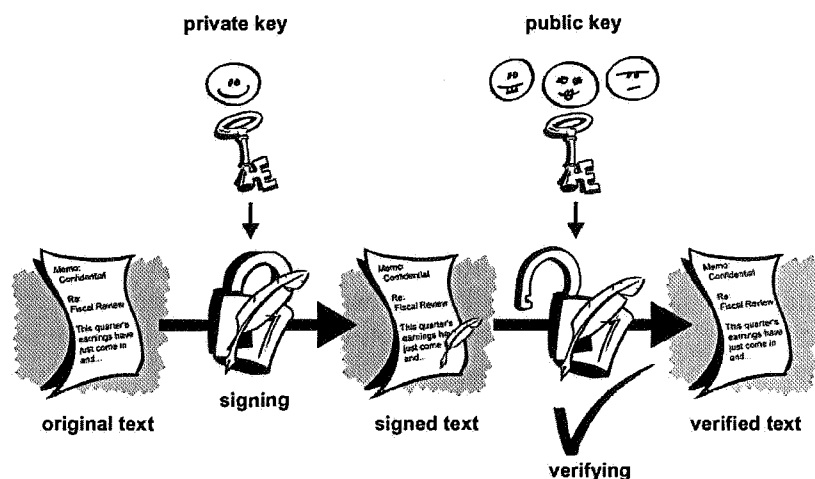


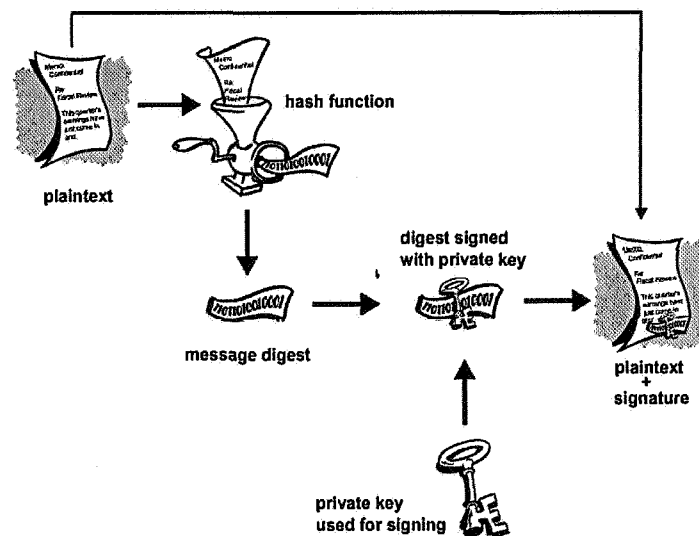
Gráfico 1 - Fuente: Manual de PGP.

El problema de esta operación en transacciones celebradas a través de internet (lo habitual), es que consumen un gran ancho de banda, ya que el documento ininteligible que sirve de base para comprobar la autenticidad del original ocupa mayor espacio que éste.

Para resolverlo se recurre a realizar antes de la firma un resumen (*digest*, usando el término inglés) automático del original. No se trata lógicamente de un resumen en el sentido de extraer las ideas principales del documento, sino, en el sentido de obtener un texto que, sea cual sea la longitud del documento original, siempre tendrá la misma brevísima extensión de un par de líneas de texto. Ello se hace de tal forma que la modificación de una sola coma o de cualquier otro carácter en el documento original, generaría un resumen totalmente distinto. Esta técnica se denomina *hash*. Realizada esta operación de resumen procedemos a firmar éste, y no el documento original, con lo que

<sup>6</sup> Los sistemas más usados en la práctica se basan todos en firma asimétrica, por lo que en lo que sigue me centro únicamente en estos, y más concretamente en PGP (Pretty Good Privacy), por ser el más claro e instructivo, y estar gratuitamente a disposición de todo aquél que quiera probarlo.

tenemos un pequeñísimo documento igualmente ininteligible y también siempre de la misma extensión, que es el que habrá de acompañar al documento original. A ello responde el gráfico 2.



**Gráfico 2 - Fuente: Manual de PGP.**

Se ha explicado aquí lo que es la firma electrónica utilizando PGP, un sistema de código abierto<sup>7</sup> y de libre y gratuita distribución para uso no comercial. El estándar del mercado, sin embargo, es el denominado X-509. Intentaré demostrar en esta charla que no es necesario optar legalmente por uno u otro sistema, según los principios inspiradores de nuestro ordenamiento y, en especial, según el principio espiritualista que rige la forma de los contratos. No es necesario optar, al menos para considerar si existe o no contrato.

Lo que he pretendido con estas explicaciones introductorias es ponerles a ustedes en antecedente de lo que significa la firma electrónica en la práctica, y

<sup>7</sup> Pretty Good Privacy fue originariamente un programa de ordenador de código abierto (la última versión para Windows en código abierto es la 6.5.8, y puede obtenerse en <http://www.pgpi.org/>), esto es, en el que los autores aportan el código fuente o programación para permitir de este modo la colaboración y el desarrollo por otras personas. En los programas que implementan medidas de seguridad, el código abierto asegura que los autores no tienen "puertas traseras", o posibilidades de vulnerar los mecanismos de protección establecidos para los usuarios. Esta garantía viene de que cualquiera con los conocimientos técnicos precisos puede comprobar la forma en la que el programa funciona.

alejarme de las prácticas oscurantistas de los mal llamados *hackers*<sup>8</sup> que hoy en día lo es cualquiera que, sin necesidad de tener especiales conocimientos de informática, tiene el tiempo suficiente como para buscar en la red algún programa ya preparado con el que poder causar algún estrago a su vecino<sup>9</sup>, amparado únicamente en la vulnerabilidad del sistema operativo más extendido del planeta (que a pesar de ser de código propietario y de pago, ha sabido liderar el mercado mundial, sin aportar grandes diferencias a otros sistemas gratuitos y abiertos).

Esta vulnerabilidad es un hecho que no se suele admitir. Los sistemas informáticos fallan, y seguirán fallando dada la creciente complejidad de los mismos: El código de Windows 3.11 tenía aproximadamente 500.000 líneas de código, mientras que el de Windows 2000 tiene 45 millones. En menos de veinte años se ha pasado de un software más claro y sencillo, a otro con una gran complejidad, que utiliza básicamente la misma técnica de programación. Además, la forma de crear los programas de ordenador por módulos, hace que las personas que programan una parte no conozcan cómo funcionan las otras. Eso crea problemas de ejecución de los programas, pero tras breves pruebas se ponen en el mercado, a pesar de saberse que darán errores, y que algunos de ellos darán importantes problemas de seguridad (estos errores se conocen como *bugs*, y son usados por los *hackers* sin demasiados conocimientos para atacar máquinas que no han instalado el parche correspondiente, de ahí la importancia de las actualizaciones de software).

Ante una industria así, podemos aceptar el código propietario, desconocido y con múltiples *bugs* (errores) en juegos, procesadores de textos, y en

---

<sup>8</sup> En realidad los hackers eran los técnicos informáticos que, ilusionados por el alcance de la técnica, colaboraban entre sí para aportar distintas soluciones. Eran los que sabían o tenían la habilidad para "saltarse" determinadas restricciones de los embrionarios sistemas operativos y de las aplicaciones que sobre ellos se implementaban. De esta facilidad para "romper" o "hacer explotar" el sistema es de donde le viene el nombre, y era una habilidad que habitualmente se utilizaba para colaborar al desarrollo de nuevas herramientas. Actualmente los antiguos hackers se han refugiado en el término *ciberpunk*, libertario de la red o, simplemente, ciberciudadano. Para nosotros estos términos son muchos más cercanos, y reflejan con mayor fidelidad lo que era el movimiento *hacker* en sus orígenes.

<sup>9</sup> Piérdanle el miedo a la técnica y a estos *hackers-de-manual-de-instrucciones*, pero estén advertidos de que ni a ellos ni a las empresas les interesa que aprendan a utilizar su ordenador. Por eso lo que resulta simple, como la firma electrónica y la encriptación, puede parecer complejo a los ojos de la mayor parte de los usuarios: pocos salen ganando si los usuarios aprenden a esconder sus datos de las técnicas de marketing de las empresas, o si queda patente que lo que parecía virtuoso no es más que el uso de técnicas simples aunque poco conocidas.

según qué programas de gestión (tal vez no en la llevanza de la contabilidad de las empresas y gestiones similares, es una decisión del usuario), pero desde luego no parece muy razonable utilizarlo en mecanismos de seguridad como la firma electrónica.

La normativa que voy a tratar aquí no tiene en cuenta estos problemas, aunque es cierto que el Gobierno alemán, incorporando la normativa europea, ha dejado la puerta abierta para que convivan los sistemas de firma electrónica basados en código libre y oculto<sup>10</sup>.

Por si la idea no hubiese quedado clara, les informaré de una última cuestión: Ya les he hablado de PGP como programa de firma electrónica avanzada de código abierto (aunque propietario). Este programa fue desarrollado por Zimmermann<sup>11</sup>, y mientras éste controló su producción estuvo prohibida su exportación de EE.UU., al ser considerado de interés militar. Poco después de que Zimmermann vendiera su empresa a la firma NAI, ésta dejó de liberar el código fuente de las nuevas versiones de su programa, y casi instantáneamente cayeron las barreras del gobierno norteamericano para la exportación del producto. No es éste el lugar para hablarles de las muchas técnicas que han sido y son usadas para el espionaje industrial, por ejemplo, y que cuentan con datos contrastados por el propio Parlamento Europeo como la existencia de la red de espionaje norteamericana Echelon, que permite la escucha de cualquier teléfono en cualquier lugar del mundo, o de su nuevo programa de filtrado de las comunicaciones por internet "Carnivore". Las técnicas de encriptación y los propios programas de ordenador también son controlados mediante la instalación de puertas traseras en el software. La única forma de garantizar la privacidad en las comunicaciones es mediante los programas de ordenador de código abierto.

Volviendo a la firma electrónica, y para terminar su explicación, nada mejor que proyectar un ejemplo de un mensaje firmado electrónicamente. En la imagen (figura 3), podemos ver el pie de un mensaje firmado digitalmente utilizando PGP, enviado por una prestigiosa revista electrónica sobre criptografía, seguridad y ciberderechos, Kriptópolis.

---

<sup>10</sup> Normalmente llamado código o software "propietario", aunque este término sea más amplio, ya que se refiere al código del cual el titular de los derechos de explotación económica (sobre los derechos de autor) no permite su copia o distribución libre, con independencia de que muestre o no cómo está realizada la programación. Un ejemplo de un programa propietario pero con código abierto es el navegador web Netscape.

<sup>11</sup> Pretty Good Privacy fue desarrollado por Philip ZIMMERMANN en 1991. Ståle SCHUMACHER realizó la versión internacional del mismo.

EDITA Y COORDINA:  
José Manuel Gómez  
jmg@kriptopolis.com

(C) KRIPTÓPOLIS, 2001

Reproducción permitida citando fuente y URL.  
Cualquier otro uso requerirá autorización expresa del editor.

---

¡No al correo no solicitado! / We hate spam!  
PARA DARSE DE BAJA / TO UNSUBSCRIBE PLEASE VISIT :  
<http://www.kriptopolis.com/baja.html>

---

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.4 (GNU/Linux)

Comment: Clave en <http://www.kriptopolis.com/claves/kp.asc>

iD8DBQE6wMp/bjqYzNM6IsRAtSkAJ9xqAzblc0G1SaR4ZZZYd27OKdx1gCcC5Sw  
lecZU3cdATpzWG9hptZ4QGM=  
=nhGz

-----END PGP SIGNATURE-----

El texto irá encabezado (no se muestra en la imagen 3) con el mensaje en inglés indicador de que comienza el texto original y de que lo que se firma es el resumen o abstract usando uno de los procedimientos de hash existentes (como por ejemplo SHA1) “-----BEGIN PGP SIGNED MESSAGE-----”, y a renglón seguido: “Hash: SHA1”. La línea siguiente contendrá ya el texto del mensaje original que queremos transmitir firmado. Tras el texto, y sin solución de continuidad encontraremos las señales de comienzo y final de la firma, y que encierran en su interior la firma del resumen del mensaje original, en ocasiones (como es el caso en la figura 3) señalando normalmente dónde o cómo se puede conseguir el archivo con la llave pública que permite verificar la autenticidad del mensaje (en este caso, en una página web).

Muchas empresas que prestan servicios en internet reclaman que se use la firma electrónica para solucionar no sólo los problemas de *integridad* y *autenticidad* del texto. Buscan asegurar también el *no repudio* (que quien firma no niegue después que la firma le pertenece). Para ello recurren a la certificación:



Hemos visto que cualquier documento puede ser resumido y firmado electrónicamente usando una clave privada, para después comprobar su origen e identidad mediante una clave pública. Dichas claves, o llaves, en realidad son algoritmos que se conservan en dos archivos informáticos (el de la clave privada protegido por contraseña). Estos archivos pueden por tanto, al igual que cualquier otro documento, ser firmado digitalmente. Para asegurar que el titular de la llave privada es quien dice ser, e impedir que niegue posteriormente haber efectuado la declaración de voluntad, se puede recurrir a un tercero que firme la llave pública de ambas partes, y dé fe de su identidad. Aquí entran las terceras partes de confianza (TPC)<sup>12</sup>, más conocidas por sus siglas en inglés de Autoridades de Certificación (CA)<sup>13</sup>, y citadas también por su nombre en la legislación española: Prestadores de Servicios de Certificación (PSC).

Resumiendo: si uno puede demostrar que determinada declaración de voluntad contenida en un documento (archivo de texto, correo electrónico, página web o similares, incluso en un impreso) es íntegra (sin que se haya añadido, enmendado ni quitado nada); es auténtica por cuanto ha sido firmada usando la llave privada de determinada persona<sup>14</sup>, y además podemos vincular dicha llave a determinada persona física o jurídica mediante un tercero en el que ambos confiamos, evitaremos el posible repudio por parte del emisor de la declaración de voluntad firmada de esta forma.

Evidentemente, las terceras partes de confianza no son siempre necesarias. Es posible demostrar que periódicamente se han celebrado otros contratos con determinada llave, y que éstos han sido cumplidos puntualmente por determinada persona física o jurídica. Esto ha de ser prueba suficiente para entender que dicha firma pertenece al emisor de la declaración de voluntad. De la misma forma pueden suscribirse contratos en soporte papel, donde

---

<sup>12</sup> Los dispositivos de clave pública se remontan, desde un punto de vista teórico, a 1976, cuando DIFFIE y HELLMAN hicieron públicas su idea de utilizar una pareja de claves. A partir de ahí se comenzaron a diseñar distintas infraestructuras de red (las PKI, *Public Key Infrastructure*), para conseguir de manera fiable las llaves públicas de aquellos con quienes nos queremos relacionar, que son albergadas en estos servidores.

<sup>13</sup> Certification Authority. En realidad se tratan de empresas o instituciones privadas en su mayor parte, y no ejercen ninguna función pública o, al menos, no ha delegado la administración función alguna en ellos. Parece que, junto a las certificaciones de terceros, debería existir para determinadas operaciones, certificados oficiales (así es entre nosotros, como más adelante detallaré).

<sup>14</sup> Recuerden que para poder firmar electrónicamente un documento es necesario poseer esta llave (privada) y la contraseña del archivo que la contiene.

conste impresa la llave pública (una serie de caracteres ininteligibles) de ambas partes que desean mantener relaciones comerciales a través de internet. O remitir la llave mediante cualquier otro medio técnico, como el fax (esto resulta innecesario y hasta absurdo, dada la mayor facilidad para falsificar un fax que un correo electrónico, sin embargo es el fax el que viene siendo aceptado como prueba en los Tribunales). En un sistema donde la norma es que los contratos no estén sometidos a especiales requisitos de forma, habrá contrato desde que existe acuerdo, y éste puede sobradamente probarse sin necesidad de recurrir a terceras partes de confianza. No quiero decir que las terceras partes de confianza no sean útiles en determinadas situaciones, pero hay que ser conscientes de que no podemos importar directamente las adaptaciones legales sobre la firma o contratación electrónica de sistemas que exigen forma escrita en muchos contratos.

Tanto la firma simétrica (o de clave privada) como la asimétrica (llamada también de clave o llave pública, aunque como ya sabemos, propiamente hablando, existe una clave pública y otra privada) pueden servir de base no sólo para firmar un documento o mensaje, sino también para encriptarlo<sup>15</sup>, haciendo que sólo el destinatario pueda conocer su contenido.

El sistema consiste básicamente en enviar únicamente el texto firmado (el ininteligible —y no su resumen firmado, sino el propio texto—), sin el texto original, si bien en los métodos basados en firma asimétrica se complica algo más al usar para realizar dicha operación, no sólo la clave privada del emisor, sino también la pública del destinatario, con lo que sólo el destinatario podrá, usando su llave o clave privada, desencriptar el mensaje y tener acceso a su contenido.

El uso de estos sistemas de encriptación es la única forma de, en una red basada en un protocolo tremendamente inseguro, como lo es el protocolo TCP/IP, garantizar la privacidad de las comunicaciones. Debe tenerse en cuenta que la topología o diseño de la red, ideada por los servicios de la inteligencia de los Estados Unidos de Norteamérica, está pensada para que todos los ordenadores compartan la información, de tal forma que si uno deja de funcionar todos los demás puedan seguir comunicándose. Por ello resulta extre-

---

<sup>15</sup> Estas dos operaciones se conocen con el nombre de “firma en claro” (cualquiera puede leer el mensaje, pero sólo los poseedores de la clave o llave pública del emisor pueden comprobar su integridad y procedencia) o “firma encriptada” (sólo el destinatario o destinatarios puede/n comprobar la integridad y procedencia del mensaje, así como conocer su contenido una vez desencriptado).

madamente fácil interceptar la información que viaja de un ordenador a otro, ya que todos ellos colaboran (o pueden hacerlo) para hacer llegar la información de una parte a otra de la red. Si dicha información no está codificada (encriptada) cualquiera puede leerla. La firma electrónica es el medio idóneo para encriptar mensajes de correo electrónico. Existen otras técnicas que se usan para encriptar los datos en otras comunicaciones (como las comunicaciones http o web, que usan fundamentalmente el sistema denominado SSL, desarrollado por la empresa Netscape, y con el que se realizan la mayoría de los pagos por internet, especialmente los que se giran contra tarjetas de crédito o débito)<sup>16</sup>.

Aceptemos como necesario para efectuar pagos de forma segura usando la red, el empleo de algún tipo de cifrado, y como conveniente el uso de la firma electrónica. Sin embargo, ni uno ni otra son exigencias de orden jurídico. No es nulo un pago realizado por el envío de la numeración de una tarjeta de crédito mediante correo electrónico, número que posteriormente es (debe ser) validado y confirmado por el acreedor. Lógicamente, si partimos de una

---

<sup>16</sup> SSL, *Secure Sockets Layer*, es un protocolo para establecer comunicaciones seguras incorporado en 1994 por la empresa *Netscape Communications Corporation*, en su entonces extendido navegador web *Navigator*. En este sistema la información confidencial viaja en un canal diferente, y tiene la principal ventaja de no requerir que el servidor disponga de capacidades especiales para el comercio electrónico (puede ser implementado en los más usuales servidores web, como Apache, Netscape Server, o Microsoft IS). El principal problema está en el lado del cliente: requiere que el usuario sea consciente de los riesgos de la red, y actualice su navegador a una versión que soporte encriptación fuerte (claves de al menos 128 bits de longitud), ya que las primeras versiones encriptaban sobre claves de 40 bits, lo que supone una seguridad muy fácil de violar. Otro problema que suele citarse es que sólo sirve para comunicaciones bidireccionales, mientras que los pagos con tarjetas requieren la intervención simultánea de tres partes: los contratantes y el banco autorizante de la operación, si no se le quieren dar los datos de la tarjeta al comerciante, o si éste quiere comprobar la aceptación del cargo por el banco del cliente. Aunque existe otro estándar llamado *Secure Electronic Transaction* (SET) que, desarrollado por Visa, Master Card, IBM, Microsoft y Netscape, soluciona estos problemas, éste no se está imponiendo, ya que requiere la coordinación de muchos elementos, entre ellos que el cliente utilice un software específico, frente a SSL que tan sólo requiere un navegador web que lo soporte (lo que cumple la inmensa mayoría de estos productos). Por eso las últimas soluciones pasan por utilizar SSL exclusivamente y, una vez que el cliente ha seleccionado el producto y recibe un número de pedido, este número es remitido al banco junto al importe y el cliente es conectado a una página del banco del comerciante, a quién suministra sus datos de tarjeta. Es éste el que se pone en contacto con el banco del cliente, a través de las redes bancarias dedicadas, confirma el cargo, y envía la aceptación al comerciante, quien remite entonces el justificante de la operación al cliente. Esto se realiza sin solución de continuidad.

red insegura donde todo el mundo puede potencialmente “escuchar” los mensajes ajenos, la encriptación es más que recomendable. Con los contratos sucede lo mismo: pueden ser celebrados sin mayor problema por correo electrónico (al menos aquellos que no exigen el otorgamiento de una forma especial, que en nuestro ordenamiento son los menos). Su prueba puede consistir en una tercera persona a quien le llega una copia de los mensajes (por ejemplo), y, dada la necesidad de demostrar que el mensaje ha llegado al ámbito de control del destinatario, por una certificación del proveedor de correo del destinatario en la que conste que dicho mensaje llegó a la cuenta de correo del destinatario en determinada fecha. Esto es, a mi juicio, una prueba más fuerte que el comprobante de transmisión de un fax, que puede ser fácilmente manipulado. También lo pueden ser los mensajes de correo electrónico, pero los conocimientos técnicos que son necesarios para hacerlo no están al alcance de cualquiera y deberá por tanto el Juez valorar dichas pruebas, al menos, según las reglas de la sana crítica.

Podemos por tanto preguntarnos para qué entonces sirve la firma electrónica, cuya regulación vamos a pasar a estudiar de inmediato. La firma electrónica cumple su papel en la contratación electrónica al asegurar la integridad y veracidad de un mensaje y, cuando exista un acuerdo previo entre las partes, o cuando la llave pública esté depositada en algún tipo de registro público que pueda dar fe de la identidad del usuario de la firma electrónica asociada a dicha llave, también el no repudio (basado en poder demostrar que dicha declaración de voluntad fue emitida por la persona física a la que va asociada la llave pública). Será la libre decisión de las partes la que lleve a formalizar un contrato utilizando firma electrónica o no, y la que lleve también a realizar o no acuerdos previos sobre su uso, o a interponer a terceros de las más variadas maneras. Sin duda se llegará a unas cuantas fórmulas estándares para realizar estas operaciones, pero no corresponde a la ley señalar cuál es la más adecuada, sino únicamente establecer los requisitos que a éstas se les ha de exigir.

El empleo más importante a mi juicio de la firma electrónica está en la intimidad. Ya les he señalado que la red es altamente insegura. El cifrado que posibilita la firma electrónica puede garantizar desde correos electrónicos, hasta redes privadas virtuales (entre ordenadores o sistemas de ordenadores distanciados geográficamente, en cualquier punto del planeta, que intercambian información de forma segura entre ellos). Ello es una herramienta muy potente para defender la privacidad en las comunicaciones, que guarda una muy estrecha relación con valores como el libre desarrollo de la personalidad,

la libertad de expresión y, en definitiva, con los valores democráticos de nuestra sociedad.<sup>17</sup>

Veamos cómo todas estas cuestiones son tratadas por la nueva regulación sobre firma electrónica.

### III. ANÁLISIS JURÍDICO DE LA FIRMA ELECTRÓNICA

Los debates jurídicos que plantea la firma electrónica vienen referidos a tres ramas del Derecho, a saber: 1) al Derecho privado, como declaración de voluntad que es<sup>18</sup>; 2) al constitucional, al estar estrechamente ligada al respeto a la intimidad del individuo y a la libertad de expresión, aunque estos problemas conectan con otros de naturaleza jurídico-privada<sup>19</sup>, y, finalmente; al Derecho penal, aunque ni la falsificación (teóricamente imposible si no se sustrae la llave privada)<sup>20</sup>, ni la preparación de delitos utilizando esta tecnología, tienen a mi juicio relevancia jurídica por sí mismas, sí la tiene la discusión

---

<sup>17</sup> En la fecha en la que reviso estas páginas, con los atentados de el WTC de Nueva York, y del Pentágono en Washington, parece que quienes abogan por un recorte de las libertades (dentro y fuera de la red) tienen un nuevo argumento en la posibilidad de que la encriptación la utilicen también grupos terroristas. La verdad es que son muchos los medios que existen para comunicarse de forma privada (basta pensar en el correo ordinario), y no por ello nadie va a prohibir ni a fiscalizar el correo ordinario. No hay argumentos para aplicar otro criterio al correo electrónico, pues el valor jurídico que está en juego es exactamente el mismo. Además, resulta inviable prohibir por ley el uso de técnicas de encriptado fácilmente disponibles (basta una hoja de cálculo como Excel y una serie de algoritmos muy conocidos para poder encriptar, como afirma el especialista Dr. Dan Boneh, de la Universidad de Stanford). El problema está en la gran capacidad de cálculo de los ordenadores modernos, cosa que no parece conveniente restringir.

<sup>18</sup> Algún problema adicional, que viene también por ser declaración de voluntad, podría plantearse por la forma de revocar la validez de dichas firmas a la muerte del legítimo usuario de las mismas, y las consecuencias de su uso posterior ilegítimo. Similar problema se plantea con la extinción de la persona jurídica, y con la modificación de los representantes de la misma.

<sup>19</sup> El derecho a la intimidad se convierte en la defensa de la libre competencia y tiene su plasmación en las normas de competencia desleal desde el momento en que un operador invade abusivamente dicha esfera privada en beneficio propio. También influye en la libre formación de la voluntad, y en la expresión de la misma.

<sup>20</sup> Hasta la fecha, y refiriéndome a PGP, todas las vulnerabilidades lo han sido una vez se obtiene la llave privada del usuario, consiguiendo entonces romper las contraseñas y firmar o desencriptar como si fuese el usuario legítimo de la firma. Por tanto es necesario acceso al ordenador o dispositivo donde dicha llave privada se encuentre.

política de si resulta o no conveniente ampliar los tipos legales para incluir en su estricta definición nuevos medios de cometer antiguos delitos. De estos problemas el más importante es sin duda el segundo de ellos, el de la intimidad, por su trascendental alcance en la formulación de la sociedad moderna. En esta breve ponencia dejaré de lado los aspectos penales, para centrarme en los del Derecho privado y, si da tiempo, haré una breve valoración de los problemas jurídico-constitucionales.

## 1. Panorama comunitario

La legislación europea en esta materia está presidida por la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica<sup>21</sup>, y que iré explicando a medida que vayamos analizando su incorporación a los ordenamientos alemán y español. Debemos tener también en cuenta la Directiva 31/2000/CE, sobre comercio electrónico<sup>22</sup>, aún sin incorporar en España y sólo parcialmente en Alemania. Esta norma viene a cerrar la regulación básica sobre firma electrónica, al hacer un uso práctico de la Directiva sobre firma electrónica.

Desde el punto de vista del Derecho privado, la firma electrónica plantea dos problemas: uno es relativo a la forma de los contratos; el otro, a su valor como prueba. Creo especialmente útil comparar por ello las normas existentes en nuestro ordenamiento, basado como he recordado en el principio espiritualista, con las del ordenamiento alemán, en el que la forma, cuando es exigida, lo es *ad solemnitatem*.

## 2. La forma del contrato

### a) *En otros países comunitarios. Especial referencia a Alemania*

En Alemania los requisitos de la firma electrónica (llamada "Signatur", frente a la "Unterschrift" o firma tradicional) se regularon inicialmente por la Ley (alemana) de Firma Electrónica, de 1997 (*Signaturgesetz*, o *SigG* como se

<sup>21</sup>. DOCE L 013, 19 de enero de 2000, pp. 12 ss.

<sup>22</sup>. DOCE L 178, de 17 de julio de 2000, pp. 1 a 16, relativa a determinados aspectos de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

conoce abreviadamente). Ésta significó un hito mundial al ser la primera ley de ámbito estatal reguladora de la firma electrónica<sup>23</sup>. Recientemente ha sido reemplazada por otra con el mismo nombre, de 16 de mayo de 2001,<sup>24</sup> que, además de incorporar al Derecho alemán la Directiva 1999/93/CE, recoge la experiencia de la Ley del 97 y de varios proyectos llevados a cabo en la Administración alemana<sup>25</sup>.

La vigente ley clasifica la firma electrónica en firmas simples, avanzadas y cualificadas, según el grado de confianza que otorgan. Así, mientras una firma simple puede serlo la imagen escaneada de una firma autógrafa, y no aporta seguridad apenas (dada la facilidad de su reproducción electrónica por cualquiera), la firma avanzada asegura la integridad y, bajo determinadas circunstancias, también la autoría, mediante el empleo de los mecanismos que hemos analizado anteriormente. Finalmente, la cualificada otorga también una altísima seguridad en la determinación del autor de la declaración signada, recurriendo a las certificaciones.

Posteriormente ampliaremos los contenidos de esta ley. Sin embargo, las mayores consecuencias jurídico-privadas de la aplicación de la firma electrónica no provienen de ella, sino de la Ley de Adaptación de los requisitos de forma del Derecho Privado al Tráfico Jurídico Moderno<sup>26</sup>, que se completará con la mayor reforma jamás llevada a cabo en el BGB, la de todo el Derecho de obligaciones<sup>27</sup>. No existe en España un proyecto de este calibre, con pretensiones de regular de forma duradera el Derecho de los contratos del siglo XXI, sin fracturas entre las “nuevas” formas de contratar (como el consentimiento otorgado en relaciones de desigualdad empresario-consumidor, o la

<sup>23</sup>. Formó parte de la Ley de Servicios de Información y Comunicación, de 22 de julio de 1997 (*Informations- und Kommunikationsdienstegesetz*, BGBl I, pp. 1870 ss.), y precedió por unos meses a su homóloga italiana.

<sup>24</sup>. BGBl I S. 876. Para un estudio de detalle sobre la misma puede verse Roßnagel, Alexander, “Das neue Recht elektronischer Signaturen”, *Neue Juristische Wochenschrift* (NJW), 25, 2001, pp. 1817 a 1826.

<sup>25</sup>. Entre ellos cabe destacar el llevado a cabo por la Administración de Baja Sajonia, dotando a los funcionarios de firma electrónica contenida en tarjetas con chip inteligente; e impulsando su uso por las PYMES (600 empresas y administraciones y 12.000 puestos de trabajo disfrutaban de estas medidas).

<sup>26</sup>. *Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr*, BGBl. I pp. 1542.

<sup>27</sup>. Que se completa con la reforma del Derecho de obligaciones, que ya se tramita en el Bundestag, bajo el nombre de *Gesetzentwurf zur Umsetzung der Verkaufsgüterkaufrichtlinie und zur Modernisierung des Schuldrechts (Schuldrechtsmodernisierungsgesetz)*, Bundestag-Drucksache (BT-Dr) 14/6040, del 14 de mayo de 2001.

contratación por medio de condiciones generales de la contratación), entre las nuevas vías de relacionarse, ofrecer y emitir las declaraciones de voluntad (uso de nuevas y aún de futuras tecnologías para la que hace falta establecer criterios generales de a los que deban someterse), con los consolidados principios de nuestro enraizado sistema jurídico, que probablemente haya que revisar y, si resulta necesario, modificar, pero con la conciencia clara de qué se está haciendo, y con amplitud de miras hacia lo que el futuro nos pueda deparar.

Veamos cuáles son las modificaciones ya introducidas en el ordenamiento alemán, fruto de esta Ley de Adaptación, por lo que respecta a la firma electrónica:

Según el Derecho civil alemán, siempre se han podido celebrar por vía electrónica aquellos contratos para los que la ley no exige una forma específica, como la forma por escrito. Esto es una cuestión pacífica en la doctrina<sup>28</sup>.

Hay que recordar, que, con diferencia significativa al Derecho español, en el régimen civil alemán, las declaraciones de voluntad que no reúnen los requisitos de forma legalmente exigidos, son nulas (nulidad de forma, § 125 BGB), y no pueden dar lugar a contrato alguno.

En concreto, es el § 126 el que regula la manera en la que se cumple el requisito de la forma escrita cuando la ley lo exige. Tradicionalmente dividido en tres epígrafes, la ley que comentamos, de adaptación al tráfico jurídico moderno, ha venido a insertar entre el segundo y el tercero (ahora reenumerado como 126.4) un nuevo § 126.3 BGB, que señala que “la forma escrita puede ser satisfecha mediante forma electrónica, siempre que la ley no establezca otra cosa”<sup>29</sup>. Dentro de estas excepciones podemos citar, de modo señalado

<sup>28</sup>. ROBNAGEL, *opus cit.*, p. 1825. Por ello no considero acertada la afirmación de RODRÍGUEZ ADRADOS de que la ley alemana deja “fuera de su regulación las firmas digitales que no reúnan las condiciones que la misma ley establece... pero sin reconocer a aquellas que las cumplan la consideración de forma negocial, ni una mayor eficacia de prueba legal”. Muy acertado resulta al señalar, comparando las leyes alemana e italiana de 1997, que esta última “desborda en ambas direcciones, en la de forma y en la de prueba, el limitado contenido de la Ley alemana”, y así en la ley italiana “los documentos con firma electrónica satisfacen el requisito legal de la forma escrita, tienen el valor probatorio de los documentos privados, y pueden ser autenticados por Notario”, aunque “sin llegar a alcanzar la consideración de documentos públicos”, “ni como forma, ni como prueba” (RODRÍGUEZ ADRADOS, Antonio, “La firma electrónica”, *Revista de Derecho Privado*, diciembre de 2000, p. 914).

<sup>29</sup>. § 126.3: Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.



aunque no exclusivo, los contratos de crédito al consumo, en los que expresamente se excluye la forma electrónica, exigiéndose la escrita para su perfección<sup>30</sup>; o los procedimientos ante registros públicos, como el de la propiedad. Por supuesto, los negocios jurídicos sobre bienes inmuebles, que requieren la inscripción en el Registro de la Propiedad, y la previa escritura pública, no pueden realizarse por vía electrónica.

El modo de dar cumplimiento a esta forma electrónica, para que sea equiparable a la de los documentos privados, está regulado en un nuevo párrafo, el 126a BGB<sup>31</sup>. Dividido en dos epígrafes, el primero establece que “cuando se dé cumplimiento a la forma escrita a través de la forma electrónica, el emisor de la declaración tendrá que incluir su nombre en el documento electrónico, que firmará con una firma cualificada, conforme a la Ley de Firma Electrónica”, lo que el § 127.1 BGB extiende también a los negocios jurídicos. El segundo epígrafe se limita a asegurar que ambas partes reciben una copia del contrato con la firma de las otras partes, como requisito de validez del contrato.

Para entender lo que es la firma electrónica cualificada, definida por el § 2 No 3 SigG, debemos de explicar previamente la *firma electrónica avanzada*. Esta última es aquella firma electrónica que permite la identificación del firmante, al que está vinculada de manera única, y cuya técnica implica que la creación de la firma esté bajo el exclusivo control del signatario (definida por el art. 2.2 de la Directiva y por el § 2 No 2 SigG): prácticamente cualquier sistema de clave pública es también de firma avanzada.

La *firma electrónica cualificada* es aquella firma avanzada que, además, se basa en un certificado cualificado para su creación (certificado definido a su vez por el art. 5 de la Directiva y el § 2 no. 7 SigG), reconocido y creado por un dispositivo seguro de creación de firma. Dicho de otra forma: la firma cualificada es aquella cuya llave pública se encuentra firmada por una entidad “prestadora de servicios de certificación”.

<sup>30</sup>. § 4.1 de la Ley (alemana) de Crédito al Consumo, *Verbraucherkreditgesetz (VerbrKrG)*, de 17 de diciembre de 1990 (BGBl. I pp. 2840 ss.): “...Der Abschluss des Vertrages in elektronischer Form ist ausgeschlossen”.

<sup>31</sup>. § 126a BGB: (1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen. (2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

Existen algunos problemas que habrá que ver cómo se van resolviendo de acuerdo a la regulación alemana<sup>32</sup>, pero puede valorarse muy positivamente la integración de la regulación sobre firma electrónica, como vehículo de expresión de una declaración de voluntad que es, en el Código civil (BGB) y en la Ley de Enjuiciamiento Civil (ZPO), ya que ello aporta gran solidez y coherencia al sistema, que puede servirse con mayor facilidad de las construcciones doctrinales existentes, rompiendo con las tristemente hoy típicas regulaciones especiales, o por vía de excepción.

No obstante, estas definiciones de la Directiva y de la SigG han sido criticadas, al basarse únicamente en las técnicas de encriptado asimétricas con infraestructura de clave pública (PKI), no ajustándose a los requisitos de estas normas el empleo de otras tecnologías<sup>33</sup>. Aunque, ciertamente, se ha definido de forma amplia el estándar de la industria, no parece que sea este tipo de normas las que deban recoger estos estándares, sino que éstas deberían establecer unos criterios generales, y remitirse a regulación de orden inferior o a la certificación para la señalización de la tecnología que cumple dichos criterios (lo que en ocasiones dependerá también del tipo de contratación en el que pretende utilizarse –así, por ejemplo, no será lo mismo en B2B que en B2C-).

El § 127.3 BGB admite incluso la celebración de este tipo de negocios con firma electrónica simple (§ 1.2 SigG), siempre que medie acuerdo previo entre las partes admitiendo esta forma. En estos supuestos tan sólo se exime del requisito de forma *ad solemnitatem*, no teniendo por tanto la sanción del §

<sup>32</sup>. Así por ejemplo (ROßNAGEL, *opus cit.*, p. 1825, quien cita la doctrina más relevante que ha detectado estos problemas), la necesidad de añadir el nombre a la declaración afecta a la protección de datos del consumidor cuando éste quiera actuar bajo un seudónimo, a pesar de que el § 12 BGB permite el uso de seudónimos que identifiquen inequívocamente al usuario (PALANDT-HEINRICH, *Kommentar zum Bürgerlichen Gesetzbuch*, 60ª edición, 2001, § 12 Rdnr. 8), derecho que es también reconocido por el § 4.6 del Proyecto de Ley de protección de datos en servicios a distancia (que da nueva redacción a la TDDSG, incorporando al ordenamiento alemán algunos artículos de la Directiva 31/2000/CE, relativa al comercio electrónico), que obliga a los prestadores de servicios de la sociedad de la información a ofrecer sus servicios de forma anónima siempre que sea técnicamente posible. Cierta doctrina alemana señala como un problema el que no se exija la incorporación del certificado en la firma, esto es, que no se firme la llave pública, ya que se puede reemplazar un certificado por otro, permitiendo fraudes. Creo que esto es fácil de evitar si se incorporan las llaves públicas en los certificados, como obliga la ley alemana en coherencia con la Directiva, con lo que se protege la intimidad del usuario, ya que su firma cualificada no tiene por qué desvelar su identidad.

<sup>33</sup>. ROßNAGEL, *opus cit.*, p. 1819, y su cita en la nota 43.

125 BGB, pero se sigue manteniendo *ad probationem*, por lo que las partes pueden solicitarse cumplir dichos requisitos mediante el uso de la firma electrónica cualificada o, en caso de no disponer la otra parte de ella, de los mecanismos recogidos en el § 126 (como la elevación a público del documento). Esto es, se articula un procedimiento similar al del artículo 1279 Cc. Ciertamente estas normas sólo operan cuando existe un acuerdo previo entre las partes, pero es bastante más (y especialmente más clarificador) que lo que dispone la normativa española que en breve pasaremos a analizar.

De forma más modesta, también en Francia se ha optado por insertar la regulación básica sobre los efectos jurídico-privados de la firma electrónica en el Código civil, en lugar de en legislación especial. En concreto, en los artículos que regulan la prueba literal (arts. 1316.1 a 1316.4 del Código civil francés)<sup>34</sup>, dotando de la misma fuerza probatoria a los documentos electrónicos que a los realizados en soporte papel, siempre que se identifique a la persona de la que emana y se pueda probar su integridad, lo que se presume cuando vaya firmado electrónicamente conforme a los requisitos que sobre la firma electrónica se establezca por Decreto del Consejo de Estado. Se prevé que la expedición de documentos electrónicos por un *officier public*, por lo que éstos podrían llegar a tener carácter de documentos públicos<sup>35</sup>.

#### b) En España

En nuestro país las normas fundamentales en la materia son el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica<sup>36</sup>, y la O. M. Fomento de 21 de febrero de 2000, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica<sup>37</sup>.

Otras normas a tener en cuenta son Real Decreto 1290/1999, de 23 de junio, por el que se desarrolla el artículo 81 de la Ley 66/1997, de medidas fis-

<sup>34</sup>. El contenido básico de dicha regulación puede verse en RODRÍGUEZ ADRADOS, *opus cit.*, pp. 918-920, y curiosamente admite (art. 1326.2) el reconocimiento de deuda hecho en documento firmado electrónicamente, que no es admitido en el sistema alemán (§ 781 BGB), por exigencias formales obvias inherentes a este último ordenamiento.

<sup>35</sup>. *Ibidem*, p. 919.

<sup>36</sup>. BOE de 18 de septiembre de 1999, convalidado por Resolución del Congreso de los Diputados de 21 de octubre (BOE del 27).

<sup>37</sup>. BOE de 22 de febrero de 2000, p. 33593.

cales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos, entre las Administraciones públicas entre sí y de éstas con los particulares<sup>38</sup> (medidas cuyo uso viene avalado por los arts. 38.3 y, especialmente, 45 de la LRJPAC 30/92, de 26 de noviembre)<sup>39</sup>, y los artículos 265.1.2º en relación con los artículos 299.2, 382.2 y 384 de la nueva Ley 1/2000, de Enjuiciamiento Civil.

Finalmente encontramos un último grupo de normas que, sin ser tan ambiciosas en su ámbito de aplicación, sí pueden considerarse una punta de lanza en la introducción de la firma electrónica en la práctica legal española. Me refiero a las siguientes: 1) Orden de 10 de abril de 2001, por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones de los impuestos de la renta y del patrimonio ; 2) Instrucción de la DGRNot de 30 de diciembre de 1999 sobre la presentación de las cuentas anuales de los empresarios y demás entidades inscritas en los Registros Mercantiles, a través de soporte informático con uso de firma electrónica; 3) Instrucción de la DGRNot de 31 de diciembre de 1999 sobre procedimientos telemáticos de legalización de los libros de los empresarios en los Registros Mercantiles; 4) Instrucción de la DGRNot de 10 de abril de 2000 sobre la publicidad formal e instrumental de los Registros de la Propiedad a través del correo electrónico; 5) Y, finalmente<sup>40</sup>, la Instrucción de la DGRNot de 19 de octubre de 2000, sobre el uso de la firma electrónica por los fedatarios públicos, y que establece que el Consejo General del Notariado y el Colegio de Registradores de la Propiedad y Mercantiles de España, deberán constituirse en PSC acreditados para certificar “la identidad, cualidad profesional y situación administrativa de los miembros en activo integrados” en ambas corporaciones.

Realmente es esta “normativa menor”, la que está consiguiendo, de forma muy tímida, eso sí, el empleo de la firma electrónica en nuestro país. Es precisamente en estas aplicaciones administrativas de la firma electrónica dónde

---

<sup>38.</sup> BOE de 10 de agosto de 1999, p. 29452.

<sup>39.</sup> BOE de 27 de noviembre de 1992

<sup>40.</sup> A la hora de revisar este texto se confirma que la DGRNot está trabajando en un borrador de regulación sobre el uso de la firma electrónica por Notarías y Registros, que posiblemente extender el ámbito de la fe pública a los nuevos soportes electrónicos (BOCG del Congreso, Serie D, 263, de 14 de septiembre de 2001, pregunta número 184/011598).

nuestro país está destacando muy especialmente, aunque la forma de llevarlo a cabo esté teniendo numerosas críticas<sup>41</sup>.

Por lo que respecta al grueso de la legislación anteriormente citada, tenemos básicamente la misma regulación que en Alemania, al responder a las Directivas europeas 1999/93/CE y 2000/31/CE anteriormente citadas, con la notable diferencia de que este último país cumple con el objetivo de la Directiva sobre firma electrónica de que “no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de” presentarse en forma electrónica, no basarse en un certificado reconocido, no estar éste expedido por un PSC acreditado, o, finalmente, no estar creada por un dispositivo seguro de creación de firma (art. 5.2 Directiva).

En nuestro país se niega eficacia jurídica incluso a las firmas avanzadas. No es cierto, como generalmente se dice<sup>42</sup>, que el art. 3.1 R.D 14/1999 de firma electrónica atribuya a aquellas “el mismo valor jurídico que a la firma manuscrita”. Ello sólo será así cuando “esté basada en un certificado reconocido”, lo que equivale al concepto alemán de firma cualificada, desconocido en nuestro país, y que significa en aquel ordenamiento la equiparación con la forma escrita. Es decir, que para celebrar contratos, incluso los que no requieren forma documental (que en nuestro ordenamiento son la mayoría), tendremos que equipararlo a aquella forma electrónica cualificada, al menos si queremos tener la protección del R.D. 14/1999.

---

<sup>41</sup>. Es cierto que los sistemas técnicos con los que estas medidas se están llevando a cabo apuestan por una “tecnología propietaria”, cuando se podría hacer sobre estándares abiertos, e incluso sobre software abierto, lo que no sólo implicaría un fuerte ahorro económico para el Estado, sino que significaría no decantarse desde las instituciones públicas por ninguno de los operadores que actúan en este sector del tráfico, lo que sin duda sería más acorde a los criterios con los que debe actuar la Administración Pública. Al decantarse ésta por unos estándares “propietarios”, obliga a todo el sector privado a seguir el mismo camino, con el objetivo de “ser compatible” con los requerimientos técnicos que exige la Administración para sus relaciones telemáticas con los ciudadanos. A modo de ejemplo, hasta hace poco sólo era posible presentar las declaraciones tributarias sobre plataformas Windows, y aún sigue siendo imposible hacerlo sobre los sistemas operativos más profesionales (UNIX, OS/2,...), algunos de ellos de código abierto (LINUX, FreeBSD, ...), por lo que los usuarios de estos sistemas se quejan de haber elegidos técnicas propietarias, cuando se podía haber hecho compatible con todos estos sistemas de forma fácil y, posiblemente, más económica.

<sup>42</sup>. Por todos SANCHÍS CRESPO, Carolina, “La prueba por soportes informáticos en la LEC 1/2000”, *Actualidad Informática Aranzadi*, 3, 2000.

Ciertamente que, a renglón seguido, el R.D. establece que aunque la firma no reúna estos requisitos no por ello “se le negarán efectos jurídicos ni será excluida como prueba en juicio” (art. 3.2). Pero esto no es, a mi juicio, forma de asegurar que no quede excluida de dichos efectos perseguidos, como vimos, por la Directiva. El Derecho alemán claramente establece que la firma avanzada sirve para celebrar negocios que no requieran forma documental<sup>43</sup>, el Derecho español sólo reconoce expresamente valor jurídico a la firma cualificada, que, además se valora en juicio no como la prueba por documentos, sino según las reglas de la sana crítica (art. 384 LEC 1/2000).

Esto es, la exigencia de firma cualificada (o en términos del R.D. 14/99, de firma avanzada basada en un certificado reconocido) sirve para bien poco, o casi para nada, en nuestro ordenamiento, ya que como requisito de forma en los contratos su equiparación al documento privado aporta muy poco en un sistema espiritualista<sup>44</sup>; y porque en cuanto a la prueba en juicio, no se valora como la prueba documental, sino que se hará según las reglas de la sana crítica, esto es, igual que la firma avanzada, e incluso igual que la firma electrónica simple (por ejemplo el documento escaneado con una firma manuscrita) unida a otros medios de prueba.

El resto de la regulación contenida en el R.D. de firma electrónica se limita a exigir unos requisitos muy estrictos a los PSC, y a los evaluadores de éstos (aún no se presta este servicio por empresa alguna), hasta tal punto que se hace casi imposible su establecimiento en nuestro país (donde aún no existen más entidades de certificación reconocidas que la FNMT, a pesar de que varias empresas prestan servicios de certificación voluntarios, o no reconocidos). Es muy posible que la norma española infrinja el principio de no autorización previa para el establecimiento de los PSC, al incorporar medidas que pueden

---

<sup>43</sup>. Pudiendo las partes exigirse, además, que se otorgue un nuevo documento con firma cualificada si se dispone de ella, o por los medios tradicionales si alguna de las partes no dispone de esta tecnología.

<sup>44</sup>. De hecho no hay nada nuevo en nuestro ordenamiento y, si antes la jurisprudencia no recelaba a la hora de admitir la forma electrónica de los documentos, y aún la firma electrónica, no está tan claro lo que ocurrirá con la confusa normativa existente. Como ejemplos de la referida jurisprudencia pueden verse las SSTs de 30 de noviembre de 1981, 24 de noviembre de 1984, 5 de febrero de 1988, 15 de febrero de 1990: Se acepta el documento electrónico por vía analógica, otorgándole validez, siempre que sea auténtico y haya sido obtenido lícitamente. La STS de 3 de octubre de 1997, yendo más lejos, afirma que este documento es firmable, en el sentido de que el requisito de firma autógrafa o equivalente puede ser sustituida por medio de cifras o signos, códigos u otros atributos numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido.

considerarse que tienen un efecto equivalente, como las fuertes sanciones y el extraordinario régimen de responsabilidad al que se someten, o las elevadísimas cauciones (de hasta mil millones de pesetas) que deben prestar para poder operar. Baste con esto, pues este tema excede el objeto de esta charla.

### 3. La prueba del contrato. Firma electrónica en los procesos civiles

#### a) *En Alemania*

Con respecto a las cuestiones procesales, y comenzando nuevamente con Alemania, la firma electrónica también ha sido introducida en el ordenamiento procesal de este país. Además, se ha creado una presunción indiciaria<sup>45</sup> para documentos firmados electrónicamente.

De acuerdo con el nuevo § 130a.1 de la Ley procesal civil alemana (ZPO), los escritos de las partes, incluyendo la prueba, en cuanto la ley prevea la forma por escrito, podrá cumplirse con ella mediante su aportación como documento electrónico, con ciertas limitaciones en función de los medios técnicos disponibles en el Juzgado, a determinar por cada Land<sup>46</sup>.

Para facilitar la prueba al destinatario de una firma electrónica, el § 292 a ZPO establece la presunción de la autenticidad de aquellas declaraciones de voluntad que cumplen con los requisitos del § 126a BGB<sup>47</sup>. Esta presunción sólo decaerá ante hechos que justifiquen serias dudas de que la declaración se haya realizado conforme a la voluntad del firmante.

#### b) *En España*

Ya he señalado la escasa utilidad que tiene nuestra legislación sobre firma electrónica, que en cuanto al valor probatorio de la firma electrónica se limita a establecer que la avanzada tendrá el de la sana crítica. Parece ser que éste será no

---

<sup>45.</sup> *Beweiserleichterung*, implica que, en la medida en la que no se cree una duda razonable, la firma electrónica avanzada gozará de la presunción de ser cierta y por tanto, también se entenderá que el documento con ella firmado es íntegro.

<sup>46.</sup> El § 130 a.2 ZPO apodera respectivamente al Gobierno Federal (Bund) y a los Gobiernos de cada estado (Länder) a determinar el momento a partir del cual puedan ser presentados ante los Tribunales este tipo de documentos, así como la forma apropiada para ello.

<sup>47.</sup> Es decir, aquella que cuente con una firma cualificada.

sólo el valor de la firma avanzada, sino el de cualquier documento electrónico, pues siendo admisible la prueba por documentos electrónicos (por mor del R.D. de firma electrónica, del carácter abierto de los medios de prueba –arts. 299.3 LEC relac. 24.2 CE-, y de su regulación en los arts. 265.1.2º relacc.299.2 con relac tb 384 y 382.2 LEC), parece lógico pensar que sea ésta su interpretación, a falta de otra establecida por la ley (salvo para la firma cualificada, o avanzada con certificado reconocido, según la dicción de nuestras normas, para la que es precisamente esta valoración conforme a la sana crítica el que señala: 282.3 y 284.3 LEC). En definitiva: se distinguen premisas para igualar las consecuencias.

Al menos los documentos firmados con firma cualificada deberían considerarse prueba documental (del 268 LEC), aunque esta interpretación no parece muy acorde con la norma. Creo que por la vía del 268.2 LEC, aportando la firma electrónica con peritaje a efectos de probar la integridad y procedencia del documento, sería perfectamente viable evitar caer en esta incongruencia, y favorecer una interpretación más razonable.

Muchos de los supuestos que permiten el uso de la firma electrónica, encuentran un vacío normativo no justificado. Así, por ejemplo, no parece necesaria la intervención de una Autoridad de Certificación (PSC) cuando se trate de relaciones de tracto continuado (o de clientes con los que ya existe relación previa, lo cual es muy frecuente: billetes de avión, bancos, grandes almacenes); en otros muchos casos será posible probar la comunicación, o deducir su existencia por los “actos coetáneos y posteriores”, por lo que no será necesaria la autoridad de certificación y, en muchos supuestos, tampoco la firma electrónica.

Resulta incoherente que, usando una misma técnica, se pueda dotar a un documento de fe pública, pero nunca de la fuerza probatoria del documento privado. Pueden existir documentos privados electrónicos (siempre que medie un PSC), pero su fuerza probatoria sólo será la de la sana crítica. Es, en definitiva, criticable que mediante normativa menor se haya podido conseguir posibilitar jurídicamente el otorgamiento de documentos públicos, la presentación de documentos y solicitudes ante la Administración<sup>48</sup> y ante los Registros mercantiles y de la propiedad inmueble, que podrán emitir publicidad formal en forma electrónica<sup>49</sup>; y que usando la misma técnica (con la única diferencia de

<sup>48</sup>. Así la declaración del IRPF, o los nuevos servicios que promete <http://www.administracion.es/>.

<sup>49</sup>. Así lo reconoce la Res. DGRNot de 26 de abril de 2000. Un comentario de la misma puede encontrarse en MAESTRE, Javier, “El empleo de la firma electrónica en el Sistema Registral Español”, *Revista de Derecho Informático*, 24, julio de 2000, 14 (sólo disponible en formato electrónico vía web).



la no intervención del fedatario público), no se reconozcan los menores efectos de los documentos privados (sino única y exclusivamente cuando intervenga un PSC, y con los efectos probatorios limitados que hemos señalado).

Otra medidas van dirigidas a la informatización del Poder Judicial, protección de los datos personales, y cuestiones relativas a la seguridad, en línea con las Instrucciones de la DGRNot.

#### IV. CONCLUSIONES

Dejando de lado las normas que han facilitado la presentación telemática de declaraciones ante Hacienda, o las que facilitan el uso de las nuevas tecnologías por la Administración, que así y todo no han conseguido una gran aceptación práctica, dado el bajo índice de usuarios con los que cuenta; la normativa española reguladora de la firma electrónica apenas innova nada, y cuando lo hace induce a confusión<sup>50</sup>, por no integrarse armónicamente con las normas con las que está llamada a convivir. Además, desde el punto de vista del funcionamiento de la Administración Pública, no resulta razonable el optar por unas técnicas que, además de ser propietarias, pueden quedar rápidamente desfasadas (se vuelve a mostrar de gran utilidad atender a objetivos y a principios generales, más que a casuística).

##### 1. De Derecho privado

En un sistema como el español, donde prima la libertad de forma en el contrato, la regulación de determinados requisitos en el comercio electrónico no debe ser más que una exigencia de forma *ad probationem*, pero la regulación actual constituye el uso de firma cualificada (art. 3.1 RD 14/99) como un requisito de prueba tan necesario frente a los demás usos de firma electrónica, devaluados probatoriamente, que puede decirse que resulta en un cuasi-requisito formal, muy lejos de la permisividad ejemplar del § 126 BGB.

---

<sup>50</sup> En este sentido se pronuncia también SANZ VIOLA, que califica nuestro ordenamiento de insuficiente y caótico y considera que debe partirse del reconocimiento de la validez y plena eficacia de los contratos electrónicos (por tanto también los sometidos a firma electrónica), conforme a las normas generales del Derecho de la contratación, opinión con la que estoy completamente de acuerdo (SANZ VIOLA, Ana María, "Contratación electrónica", *Actualidad Civil*, nº 18, La Ley, Madrid, 2001, p. 676).

La actual regulación introduce una gran confusión al no integrarse con las normas tradicionales de nuestro ordenamiento. La forma especial (firma cualificada) no sólo no es exigible para la existencia del contrato, sino que tampoco otorga prerrogativa alguna desde el punto de vista procesal de valoración de la prueba, cuyo valor será el de la sana crítica, igual que si fuera una firma avanzada, o incluso una firma electrónica simple (únicamente no requiere acompañarla de peritaje, en muchos casos muy costoso).

Es muy recomendable una reforma que aborde la integración de toda esta problemática (junto a protección del consumidor, ventas a distancia, contratación por condiciones generales,...), evitando la práctica negativa de las leyes especiales.

No se pueden crear islas de legislación desconectadas y sin relación entre sí. El Derecho necesita reducir la complejidad de la vida a unas reglas o principios válidos para todos. Es necesario, como se está haciendo en Alemania o en Francia, introducir estas normas sobre contratación en internet dentro de la Teoría General del Contrato, dentro del Código civil. Así por ejemplo, mantener el principio de libertad de forma parece muy razonable, pero el legislador podrá modificar esta regla, lo que se le debe pedir es que lo haga de forma coherente, y no dependiendo de la forma del contrato, sino de los valores en juego en cada tipo contractual. No deben en ningún caso realizarse leyes especiales que pretendan regular materias tan amplias como forma, contenido y prueba del contrato, condiciones generales de la contratación, responsabilidad civil de quienes presten servicios a través de internet,... Éste es el camino que hoy en día se está siguiendo (así el anteproyecto de ley de comercio electrónico), y está erosionando gravemente la coherencia de nuestro ordenamiento, y, lo que es más grave, está dañando seriamente el principio de igualdad, porque gran parte de esta regulación no justifica su especialidad, tratando de forma diferente situaciones jurídicamente idénticas.

Si nuestro TS admite un reporte de actividad de un fax como prueba en juicio (sea esto razonable o no), no puede menos que aceptarse un correo electrónico, vaya éste firmado o no, y con independencia de que probemos de otro modo su autenticidad e integridad.

## **2. De Derecho constitucional**

Es necesario proteger la intimidad, como soporte de la libertad de expresión en internet. Ello tiene una repercusión inmediata en: 1) el derecho al tra-

bajo y la sindicación; 2) la inviolabilidad de las comunicaciones, y; 3) la protección del consumidor (frente a las agresivas técnicas de marketing que juegan con los datos personales de los usuarios)

Y las soluciones pasan probablemente por: 1) fomentar la libre competencia, no predefiniendo una técnica de firma digital concreta, sino en todo caso unos objetivos a cubrir por la técnica y, si se quiere, unos requisitos a modo de garantía que deben pasar por el depósito del código fuente; 2) El conocimiento del código fuente, incluso en el software propietario, requiere una solución a caballo entre el derecho de autor, claramente insuficiente para proteger los programas de ordenador, y el de patentes, aún más inadecuado dado su largo periodo de explotación frente a la breve vida útil de los programas, y; 3) Fomentar la educación del usuario, para que sepa utilizar su ordenador, en lugar de pretender garantizar con leyes sancionatorias, restrictivas de derechos, dicha seguridad, completamente inalcanzable por esta vía dada la tipología de la red<sup>51</sup>.

---

<sup>51</sup>. Véase nota 17.