Valor Probatorio del Documento Electrónico. Su autenticidad a través de la Criptología

JOSE MANUEL NUÑEZ JIMENEZ

Doctorando Curso "Valor Probatorio de los Documentos Electrónicos" dirigido por el Profesor Carrascosa López. UNED.

I. INTRODUCCIÓN

La aplicación de las nuevas tecnologías en todos los ámbitos de nuestra sociedad lleva consigo un cambio en multitud de aspectos de la vida diaria y profesional que hasta épocas recientes se habían mantenido prácticamente inalterables.

Así, con el empleo del ordenador, se hace posible recopilar una amplia información sobre cada persona, reuniendo un conjunto de datos que aisladamente nada dicen, pero que al ser presentados en forma sistematizada, pueden dar lugar a una información que el afectado no se imagina ni le agradaría ver en poder de otros. Tengamos presente que un ordenador puede clasificar y relacionar rápidamente, por ejemplo, nuestros datos laborales, económicos, legales, sanitarios, etc, construyendo un detallado perfil de cada individuo.

El desarrollo actual de la tecnología ha provocado el surgimiento de diversos instrumentos que, por sus características, se apartan de los tradicionales; así desde los más simples hasta los más sofisticados: máquina de escribir,

telégrafo, teléfono, fonógrafo, cinematógrafo, dictáfono, cinta magnetofónica, fotocopiadora, contestadores telefónicos automáticos, procesadores de textos, correo electrónico, videotex, telefax, télex, satélites de comunicación. Dentro de esta proliferación es evidente que existe una fagocitación de los medios más modernos respecto a los más antiguos, de modo que van sustituyéndose unos a otros.

La utilización de todas estas herramientas de forma cada vez más frecuente por empresas, particulares e incluso las Administraciones Públicas, plantea la necesidad de llevar a cabo un proceso de adaptación, tanto en el campo operativo de la técnica como en el conocimiento y valoración de las consecuencias de su implantación. Es en este último sector donde existe mayor número de lagunas, tomando una relevancia más destacada en el ámbito del Derecho, donde casi siempre existe un gran desajuste entre la realidad y su regulación legal.

España se incorporó a todo este panorama de forma tardía e insegura, de todas formas, actualmente se han dado pasos hacia el futuro aceptando la contratación por télex o fax, el uso de tecnologías como el sistema EDI, Internet, Infovía, etc, habiéndose manifestado, ya, la jurisprudencia acerca de su validez y aceptación.

El uso de estas tecnologías ha hecho resentirse la seguridad jurídica en el campo procesal, ya que en caso de acudir a los tribunales, surge una enorme dificultad probatoria en torno a todos estos avances.

Hasta ahora la doctrina se había ocupado de estudiar como "*nuevos campos probatorios*" la llamadas pruebas técnicas y científicas, a modo de casos de laboratorio de repercusión sectorial.

Por el contrario, con las técnicas de funcionamiento digital y enlace a distancia, con lo que se ha dado en llamar "*documento electrónico o informático*", no se está ya ante casos relativamente poco aplicables, sino que nos enfrentamos con la necesidad de tener que validar como medio probatorio una nueva forma de expresión del pensamiento y de la actividad humana.

Se trata de una nueva técnica, cada vez más potente y masiva, que en el plano social y económico va sustituyendo al papel, hasta este momento portador documental por excelencia, por lo que sobrevendrán consecuencias jurídicas de enorme calado.

Con la invención de la imprenta por Gutemberg, fue el papel, la forma más común de registrar definitivamente las actividades entre los hombres. Su empleo adquiere especial relevancia al incorporarle la firma, que denota la autoría, paternidad y veracidad del contenido, constituyéndose, así, el papel como el garante de la fehacencia y credibilidad, es decir, como válido y probatorio para la ley.

Sin embargo, en las sociedades actuales, se está pasando de esta forma tradicional de registro y comunicación, a otra que potencia el intercambio de información eliminando barreras de espacio y de tiempo.

Gran número de autores no dudan en afirmar que no hay inconveniente en considerar al **documento electrónico** como **documento escrito**, ya que, **contiene un mensaje** (texto alfanumérico o diseño gráfico) **en lenguaje convencional** (el de los bits) **sobre soporte** (cinta o disco) y **está destinado a durar en el tiempo**.

Al convertirse el ordenador en el único instrumento capaz de satisfacer las necesidades sociales, jurídicas y económicas, va a existir una gran cantidad de documentación desarrollada en forma automatizada lo que provoca el problema de su seguridad jurídica.

Así en la esfera procesal, además de otros campos de influencia, surgió un desequilibrio acerca de la aceptación del documento electrónico como mecanismo de prueba.

El problema se planteó en lo que se refiere a si los nuevos soportes electrónicos o informáticos se podían considerar enmarcados dentro de la clasificación de medios de prueba establecidos en los art. 1215 del Código Civil, art. 47 del Código de Comercio y art. 578 de la Ley de Enjuiciamiento Civil.

Evitando entrar en el farragoso debate doctrinal, la mayoría de los autores considera que los soportes utilizados en el área de la informática, no pueden calificarse de autónomos medios de prueba, sino que se engloban dentro de la prueba documental y, más concretamente, en el concepto de "*instrumentos, archivos, asientos o papeles privados*" a que se refiere el art. 1228 del Código Civil o el art. 578 de la Ley de Enjuiciamiento Civil.

Esta aceptación es, ante todo, coherente con el devenir de la humanidad, ya que negar la utilización procesal de estos nuevos instrumentos y técnicas puestos al servicio de los hombres, sería cerrar los ojos ante el mundo que nos rodea, hecho por el que la historia nos juzgaría.

Supongamos que tanto jueces como abogados no hicieran uso de estos medios. Se llegaría a tal descoordinación entre la práctica judicial y la vida social, que podría llegar a hablarse de indefensión.

Una interpretación coherente del art. 24 de la Constitución de 1978, que ponga en relación el párrafo 1, en lo relativo a la prohibición de la indefensión, y el párrafo 2, que reconoce el derecho a utilizar los medios de prueba pertinentes para la defensa, debe llegar a la conclusión de que en el proceso han de ser admisibles como prueba, todos los nuevos descubrimientos y avances técnicos; por lo tanto, su inadmisión debe abrir la posibilidad de interponer recurso de amparo ante el Tribunal Constitucional.

Diferentes sentencias del Tribunal Supremo y del Tribunal Constitucional reconocen y aceptan la utilización de estos medios, como modalidad independiente y singular de la prueba documental.[1]

II. VALOR PROBATORIO DEL DOCUMENTO ELECTRÓNICO

El documento electrónico es el documento proveniente de la elaboración electrónica. Debe tener una serie de características como, ser inalterable, legible gracias a un procedimiento adecuado, debe ser identificado respecto al lugar y al tiempo y debe ser estable.

La admisión del documento electrónico como prueba en un proceso exige reunir una serie de requisitos :

■[1] **STC 128/88 de 27 de Junio y STC 190/92, de 16 de Noviembre**: *"no cabe negar valor probatorio a las transcripciones de una cinta magnetofónica cuando, han sido incorporadas a los autos, no han sido impugnadas en todo o en parte, y se dan por reproducidas en el acto del juicio oral".*

STS de 24 de Marzo de 1994, Sala Primera : *"...el concepto de documento ofrece una mayor amplitud en cuanto referido al medio u objeto a través del cual se manifiesta un pensamiento o idea... lo que viene amparado por el art.1215 del Código Civil, al emplear el término de instrumentos en lugar del de documentos".*

a) que pueda demostrarse por quien pretende valerse del mismo, que el equipo utilizado para la creación del documento funciona correctamente.
b) que sea demostrable la bondad de los procedimientos de datos utilizados en la entrada de la información al ordenador, de modo que quede asegurada la exactitud de los registros en todo su recorrido.
c) que sean comprobables los medios de almacenaje, tratamiento y elaboración de la información y de preparación de su salida a fin de garantizar la fiabilidad del registro.
d) que sea un caso en el que el documento electrónico viene a hacer prueba en contra de su titular o propietario.
e) que la veracidad de la información pueda ser corroborada por otros medios complementarios
f) que puedan llegar a identificarse con precisión los sujetos participantes y las operaciones realizadas por cada uno de ellos en el proceso de elaboración del documento electrónico

La jurisprudencia ha abierto la mano en lo relativo a la admisibilidad probatoria de las fuentes de prueba de naturaleza electrónica. Así el Tribunal Supremo, en sentencia de la Sala 2ª, de lo Penal, de 5 de Febrero de 1988, abordando el problema del valor probatorio de la grabación telefónica, señala la legitimidad de tal prueba, afirmando que las relaciones de medios probatorios de las leyes de procedimiento no tienen el carácter de exhaustivos, por lo que las innovaciones tecnológicas deben incorporarse al acervo jurídico procesal.

Después de todo un debate sobre la naturaleza del documento electrónico como medio de prueba, la mayor parte de la doctrina considera que los soportes en el área de la informática, se enmarcan dentro de la prueba documental en el concepto "*instrumentos, archivos, asientos o papeles privados*".

Esta problemática sobre la admisión de los documentos electrónicos como medios de prueba, ha sido obviada en otros ordenamientos en los que el legislador, haciéndose eco de su realidad, ha decidido incorporarlos de modo directo al Derecho positivo.

Este es el caso del **Código Civil Italiano**, cuyo art. 2712 sí recoge, en relación al art. 261 del Código de Procedimiento Civil, tales medios de prueba.

Esta misma postura ha sido adoptada por el **Código Civil Portugués**, el cual los ha incorporado en su art. 362, que introduce un concepto jurídico de documento extraordinariamente amplio.

Respecto a la **normativa francesa**, el art. 1348 del Código Civil admite desde 1980 una vía que posibilita la admisión como prueba, en los casos en los que el original no exista, de una copia, siempre que sea definitiva y fehaciente, lo cual podría ser la impresión de un documento electrónico si se prueba que la misma es auténtica, en el sentido de que coincide con el documento electrónico y no ha existido manipulación alguna.

Si bien queda claro la admisión del documento electrónico como medio de prueba, aquél puede presentar estas manifestaciones :

a) el documento en soporte electromagnético (disco, disquete..)
b) el documento sobre papel preparado mediante ordenador, lo que conduce, bien a buscar nuevas técnicas de autenticación, bien a configurar un concepto jurídico que los acepten tal como salen del ordenador.
c) el documento transmitido de ordenador a ordenador o de terminal a terminal

El valor probatorio depende de la clase de prueba documental que el documento electrónico constituya. Si el documento se ha efectuado en presencia de un fedatario público, será documento público la transcripción por impresora o el documento transmitido.

Cuando las modalidades se han confeccionado privadamente, el problema se agudiza, pero la autenticidad del documento puede quedar establecida por su admisión por la otra parte, por su reconocimiento bajo juramento a la presencia judicial y por la prueba pericial.

El documento, electrónico o no, es un medio de prueba tasado que el juez debe valorar de acuerdo con lo establecido con las normas legales, aunque la jurisprudencia del Tribunal Supremo y la regulación del recurso de casación han hecho de esta prueba una más de valoración libre.

III GARANTÍAS DE LA AUTENTICIDAD DEL DOCUMENTO ELECTRÓNICO

III.1. Derecho Español

La utilización del documento electrónico como medio probatorio exige la necesaria y precisa adveración y certificación de autenticidad, veracidad y fidelidad que encuentra cauce procesal adecuado mediante el reconocimiento judicial, sometido a las reglas de procedimiento y valoración previstas.

La consideración como documento o no a efectos procesales es un aspecto relevante puesto que esa calificación lleva consigo la aplicación a su vez de las normas de valoración propias de los documentos, sin que en ese caso pueda tener entrada la libre apreciación del juez.

Si ambas partes reconocen el contenido de un documento electrónico como tal, éste produce prueba entre las partes, sin que en estos casos pueda el juez llevar a cabo una apreciación libre del mismo. Por el contrario, si una de las partes no reconoce la autenticidad del documento, habrá que pasar a la prueba de peritos y, si ello no fuera posible, a la de reconocimiento judicial.

Si éste es el aspecto procesal de la autenticidad del documento electrónico, su problemática mayor es la aparente facilidad con la que pueden modificarse. Es esta característica la que crea una mayor inseguridad, puesto que en muchas ocasiones dichas modificaciones no dejan rastro alguno, por lo que el poder probar que el documento objeto de litigio sigue siendo el mismo que cuando ocurrieron los hechos puede llegar a convertirse casi en una prueba diabólica y de imposible consecución.

Por ello, el objetivo de las partes debe ser acreditar que el sistema informático es seguro, de modo que sea posible seguir la pista de cualquier modificación que el documento haya sufrido. Si es posible acreditar este extremo, no hay duda de que la tarea de llevar al juez a la convicción de que aquél sigue siendo auténtico no será tan ardua.

Hoy en día existen un gran número de métodos para evitar las alteraciones que supone la ausencia de autenticación. Así podemos encontrar el doble tecleo, programas de control, la verificación del mensaje, la utilización del

testing, programas de pa idad y disparidad sobre cada carácter, y posteriormente sobre todos los bytes que tienen la misma posición dentro del carácter transmitido, controles y registros en la actividad de los posibles intervinientes, en la elaboración y transmisión de un mensaje...

Las **técnicas de autenticación** del documento electrónico son:

a) la criptografía o criptología : es objeto de análisis en el apartado IV,
b) el código secreto o de ingreso : supone una combinación determinada de números o de letras que sólo es conocida por el titular del mismo,
c) métodos basados en la biometría : se puede entender la identificación de un determinado operador a través de datos físicos o biológicos, si bien, necesitaríamos un sistema auxiliar para verificar la autenticidad del contenido del documento.

Las técnicas de autenticación y su fiabilidad determinarán la fuerza probatoria del documento electrónico, que obligará a las partes, vinculándose éstas, a la inalterabilidad del documento. Las normas deben propugnar la admisión de las formas de autenticación de los documentos electrónicos.

Estas nuevas técnicas son tan aceptables como la tradicional firma manuscrita. Al igual que con ésta, la signatura informática es un medio para identificar al titular o propietario del documento electrónico.

La **signatura electrónica** supone ser elaborada a través de procedimientos criptográficos, llevar un resumen codificado del mensaje y de la identidad del emisor y del receptor. Son características de la signatura electrónica :

- debe permitir la identificación del signatario,
- no puede ser generada más que por el emisor del documento, infalsificable,
- las informaciones que se generen a partir de la signatura electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla,
- la aposición de una signatura debe ser significativa y va unida indisociablemente al documento a que se refiere,

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

No existirá signatura sin intervención humana.

III.2. Derecho Comparado

La **normativa inglesa**[2] proporciona una regulación más detallada que la española. Establece dos criterios que confieren una valoración a la prueba aportada. El primero de ellos se centra en determinar si la información fue facilitada o archivada en el ordenador al tiempo en que los hechos ocurrían. El segundo de ellos se resume en conocer si la persona que en ese momento operaba el sistema o introducía los datos tenía algún motivo para falsear los hechos.

La mejor arma para convencer a un tribunal de la autenticidad de un documento electrónico es la posibilidad técnica de poder determinar la propia historia del documento desde su génesis, es el denominado "*audit trail*". Éste debería ser capaz de determinar cuándo el documento tuvo entrada en el ordenador, qué operador lo manejaba en ese momento, en qué ocasiones se accedió al mismo y por quién, si se modificó y qué extremos fueron modificados.

La seguridad del proceso en el Reino Unido ha hecho que se redactase por la Asociación Británica de Estándares, un catálogo de recomendaciones a seguir para aquellos que pretendan asegurar del mejor modo posible, de acuerdo con la técnica, las posibilidades de utilizar documentos electrónicos dotándoles de validez jurídica.

En el **Derecho norteamericano** son necesarios estos requisitos para considerar que un determinado sistema informático tiene implantado un proceso seguro de autenticación :

■[2] Civil Evidence Act.

- **conservación de archivos**: los documentos electrónicos deben conservarse durante, al menos, el mismo período de tiempo que si fueran documentos en papel.
- **seguridad e integridad de los datos**: se debe estar en posición de demostrar que a los documentos electrónicos no puede accederse sin control previo.
- **sistema de documentación**: el sistema de archivo electrónico debe estar debidamente documentado, incluyendo descripción física y lógica de la estructura de los programas, así como de las entradas y salidas de la información.
- **sistema de archivo de copias**: se debe tener en soporte físico aquellos documentos sobre los cuales una normativa específica obligue a ello (escrituras públicas, contratos con la Administración...).
- **accesibilidad del sistema**: los documentos electrónicos deben poder ser accesibles a través de su lectura o visualización en la pantalla del ordenador.

No obstante, el satisfacer los anteriores requisitos no constituye una garantía absoluta de autenticidad, si bien no hay duda de que puede mejorar sustancialmente la valoración que de los mismos lleve a cabo un tribunal.

IV. LA CRIPTOGRAFÍA O CRIPTOLOGÍA COMO GARANTIA DEL DOCUMENTO ELECTRÓNICO

Como he señalado anteriormente, se trata de una de las grandes categorías de las técnicas de autenticación del documento electrónico.

La protección que brinda el ordenamiento jurídico es una protección "*a posteriori*" que, por las características de la información, y la propia naturaleza de la tecnología informática, en muchos casos resulta insuficiente para el logro efectivo de la protección del derecho de secreto para los datos sensibles, por lo que, además de la protección jurídica, se requieren medidas de prevención que, "*a priori*", impidan materialmente el éxito de las amenazas contra la información almacenada, tratada o transmitida electrónicamente.

La criptología se incorpora al sistema de información una vez determinado qué ha de protegerse y con qué niveles. Se puede definir como un sistema de codificación de un texto con unas claves confidenciales y de procesos

matemáticos complejos (algoritmos) de forma que resulte incomprensible para el tercero que desconozca la clave descodificadora.

La criptología ha venido siendo utilizada tradicionalmente en los ámbitos militar, diplomático y comercial. Actualmente, se ha ampliado a otro usos mucho más próximos aunque con niveles de exigencias diferentes, entre los que son cada vez más frecuentes, las aplicaciones destinadas a la protección de los derechos y libertades.

La forma tradicional de preservar la confidencialidad de una red de comunicaciones ha sido la protección criptológica, que implica la utilización de técnicas que permiten llevar a cabo el ocultamiento de la información protegida a personas no autorizadas. Siendo esto así, la criptología se convierte en una exigencia imprescindible.

La protección criptológica presenta diversos grados de infalibilidad, según se trate de intereses de extrema importancia, o de intereses de menor relevancia, es decir, según se trate de comunicaciones públicas o privadas. Mientras que en las primeras la regla general es la transparencia, en las segundas prima el imperio del secreto profesional. Esto nos llevaría a la necesidad de protección sistemática de las comunicaciones privadas y, excepcionalmente, de las públicas.

A modo de ejemplo, **en el ámbito nacional,** la Ley 30/1992, de 26 de Noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, contribuye a la definición de ámbitos necesitados de protección. En este sector, y debido a los principios de cooperación, coordinación y colaboración entre Administraciones Públicas, se hace imprescindible la intercomunicación y la transmisión telemática de registros, lo que dificulta la protección exhaustiva de los datos asentados.

También la Ley Orgánica 5/1992 de 29 de Octubre sobre Regulación del Tratamiento Automatizado de Datos de Carácter Personal, deja cabida a la protección criptológica[3].

■[3] Art.9. *"1.- El responsable del fichero deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal.2.- No se registrarán datos de carácter personal en ficheros automatizados que no reúnan*

En el ámbito comunitario, hay referencias a la protección criptológica en la Decisión del Consejo de 31 de Marzo de 1992, relativa a la seguridad de los sistemas de información; en la Recomendación del Consejo de la OCDE de 26 de Noviembre de 1992, que contiene las líneas directrices para la Seguridad de los Sistemas de Información; en el Convenio de 28 de Enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal y en la Propuesta de Directiva del Consejo relativa a la protección de datos personales y de la intimidad, en relación con las redes públicas digitales de telecomunicación, y, en particular, la Red Digital de Servicios Integrados y las Redes Móviles Digitales Públicas.

La protección criptológica de los datos "*sensibles*", se sitúa en el contexto de la aplicación de las nuevas tecnologías de la información en el entorno social, jurídico y político de una sociedad democrática, donde encuentra su reforzamiento y legitimación, pero también sus límites. Globalmente considerada, requiere la adecuación de los niveles de protección a la naturaleza de la información protegida, de forma que haga posible el juego de los distintos derechos afectados.

Todo derecho tiene sus límites en relación a los derechos fundamentales que establece la Constitución. La protección criptológica debe respetar la Norma Suprema, evitando posibles colisiones con derechos y libertades que gozan de protección específica. Este es el caso de entrar en polémica con los derechos al honor, la intimidad y la propia imagen.

Estas garantías de no intromisión de las prácticas criptológicas en los derechos fundamentales, están reflejadas en normas internacionales (art.29.2[4] de la

las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a la de los centros de tratamiento, locales, equipos, sistemas y programas.".

Art.20.2. "*La recogida y tratamiento automatizado para fines policiales de datos de carácter personal...deberán ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.*".

■[4] "*En el ejercicio de sus derechos y en el disfrute de sus libertades toda persona estará solamente sujeta a las limitaciones establecidas por la ley, con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática*".

Declaración Universal de Derechos Humanos, art. 19.2[5] y art. 19.3[6] del Pacto Internacional de Derechos Civiles y Políticos y el art.10 del Convenio Europeo para la Protección de Derechos Humanos y Libertades Fundamentales.

Por otro lado, existen dos grandes técnicas criptológicas :

a) **sistemas simétricos** : el emisor, como el destinatario de un mensaje disponen de la misma clave para el cifrado y descifrado de aquél.
b) **sistemas asimétricos** : funcionan por la combinación de dos tipos de claves, una pública y otra secreta que se corresponden.

Uno de los grandes inconvenientes de la protección criptográfica es su coste tan elevado. Si bien, y a pesar de esto, las ventajas que supone la transmisión electrónica, aunadas con las garantías de seguridad que nos ofrece la criptología, superan con mucho el inconveniente anterior.

En los llamados "***sellos del software***", es el mismo ordenador el que asocia a cada instrucción un valor numérico, y así, si el programa se modifica, el valor de las instrucciones que lo componen se altera, y es el mismo ordenador, el que comprobando la desigualdad entre las claves y el valor numérico del programa, rechazaría la ejecución del mismo, señalando sus alteraciones.

El uso de la criptología para la codificación de la información en ordenadores y redes, al igual que los sistemas de control de accesos mediante *passwords*, suponen un obstáculo técnico para la investigación de los hechos presuntamente delictivos, pero es la única forma, también, de preservar la intimidad y propiedad de la información. Dilema, éste, que cebe ser resuelto a

■[5] "*Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*".

■[6] "*El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la Ley y ser necesarias para: a) asegurar el respeto a los derechos o a la reputación de los demás; b) la protección de la seguridad nacional, el orden público, la salud o la moral públicas*".

tenor de conceptos genéricos tales como la Justicia y la Seguridad, bajo la perspectiva de nuestra Constitución y de todo el Ordenamiento Jurídico.

Por lo tanto, es conveniente que los países vayan incluyendo en sus leyes la regulación y consecuencias de las prácticas criptológicas, ya que éstas no son inocuas. Utilizadas de forma abusiva o fraudulenta, puede, no sólo atentar contra la libertad de información, sino obstaculizar el normal desenvolvimiento de la sociedad y el Estado, a través de la creación de reductos impenetrables.

CONCLUSIONES

Partiendo del hecho de que el documento electrónico está admitido mayoritariamente en la doctrina, como otro medio de prueba más en el proceso, nos encontramos con que, a diferencia del soporte papel, aquél plantea el inconveniente de su fácil modificación, incluso en ocasiones, sin dejar rastro.

En estas situaciones, intentar probar la autenticidad de un documento se convierte en algo de imposible consecución.

El principal escollo, por tanto, será la admisión de una prueba por el juez. Para demostrar la autenticidad del documento hay que retrotraerse al origen del problema, es decir, plantear seriamente el tema de la seguridad de los datos sensibles y demás clases de datos. Su abordaje se hará, no sólo, desde una perspectiva eminentemente legislativa, sino también desde un prisma práctico de concreción de medidas.

Los esfuerzos deben ir encaminados a que todas las declaraciones de intenciones que aparecen en las leyes, se tornen en auténticas tomas de postura contra el mal empleo de los datos personales y los intentos de infringir las leyes.

La lucha contra la inseguridad informática, debe venir dada por la aportación de una serie de mecanismos capaces de impedir el falseamiento, modificación y la utilización fraudulenta de los datos contenidos en soporte electrónico.

Uno de esos mecanismos, quizá el más efectivo, es la criptología, técnica no muy desarrollada y que de generalizarse su empleo, forzaría su regulación, supliendo el vacío legal hasta hoy existente. Con las técnicas criptográficas se protegería la seguridad y autenticidad de los datos, debiendo tener en cuenta el legislador el peligro, en el ámbito delictivo de estas técnicas, ya que crean reductos impenetrables.

BIBLIOGRAFÍA

- ALMAGRO NOSETE y otros, (1990) "*Derecho procesal. Parte general, proceso civil. Tomo I, volumen I*" Editorial Tirant lo Blanch, 5ª ed., Valencia.

- CARRASCOSA LÓPEZ, Valentín (1995) "*Valor probatorio del documento electrónico*" *Informática y Derecho* nº9, 10, 11 UNED Mérida.

- DARÍO BERGEL, Salvador (1995) "*Contratos informáticos en el Derecho Privado*" Informática y Derecho nº8 UNED Mérida.

- DAVARA RODRÍGUEZ, M. A. (1992-1993) "*La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal*" Editorial Aranzadi. Encuentros sobre Informática y Derecho. Madrid.

- GALLARDO, M.A. (1993) "*Garantías criptológicas de las firmas electrónicas*". Actualidad Informática Aranzadi. Enero. Pp 5-6.

- GONZÁLEZ AGUILAR, A. y otros. (1991) "*El derecho de la prueba y la informática. Problemática y perspectivas*" Informática y Derecho nº1 UNED Mérida.

- HEREDERO HIGUERAS, M. (1996) "*La Ley Orgánica, 5/1992, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Comentario y textos*" Editorial TECNOS. Madrid.

- MOLINA MATEOS, J.M. (1996) "*Libertad informática y criptología*" Informática y Derecho nº 12, 13, 14, 15 UNED Mérida.

- PÉREZ LUÑO, A.E. (1992) "*Del habeas corpus al* habeas *data*". Informática y Derecho nº1 UNED. Mérida.

- ROUANET MOSCARDÓ, J. (1992) "*Valor probatorio Procesal del documento electrónico*" Informática y Derecho nº1 UNED Mérida.

SANCHO RODRÍGUEZ, J. y MORANT RAMÓN, J.L. (1993) "*Garantías de la firma electrónica de contratos y autentificación de las partes*". Editorial Aranzadi. Encuentros sobre informática y derecho. Madrid.