SEGURIDAD DE LA FIRMA ELECTRÓNICA

Magistrada Martha Gladys Calderón Martínez
Noviembre de 2008

Conceptos

Gramatical

En el actuar cotidiano dentro del mundo del derecho se ha dado un gran peso a la firma, pues con esta se avala el contenido y voluntad con la que se quiere expresar su autor.

En efecto, en el diccionario de la lengua española,[1] se definen de la siguiente manera los términos firma y firmar (sólo se incluyen los conceptos que interesan al trabajo).

> "**FIRMA f**. Nombre apellido, o título que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido. // 5. Sello (II carácter peculiar o especial)."

> "**FIRMAR**. (Del lat. *FIRMARE* afirmar, dar fuerza). Tr. Dicho de una persona: Poner su firma. //2.- ant. Afirmar, dar firmeza y seguridad a algo."

Conceptual

Por su parte en la Enciclopedia Jurídica Omeba,[2] se define doctrinalmente de la siguiente manera:

> "El artículo 3633 del Código Civil establece que: 'En los testamentos en que la ley exige la firma del mismo testador, debe esta escribirse con todas las letras alfabéticas que componen su nombre y apellido. El testamento no se tendrá por firmado cuando sólo se ha suscrito el apellido, o con las letras iniciales, nombres y apellidos, ni cuando en lugar de suscribir el apellido propio se ha puesto el de otra familia a la cual no pertenece el testador. Sin embargo, una firma irregular e incompleta se consi-

[1] *Diccionario de la Real Academia de la Lengua Española*, Vigésima Segunda Edición, p. 790.
[2] *Enciclopedia Jurídica Omeba*, Editorial Bibliográfica Argentina. pp. 290-293.

derará suficiente cuando la persona estuviese acostumbrada a firmar de esa manera los actos públicos y privados', y ampliando el concepto se lee en la nota al artículo 3639: 'La firma no es la simple escritura que una persona hace de su nombre o apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad'. Regularmente la firma lleva el apellido de la familia; pero esto no es de rigor si el hábito constante de la persona no era firmar de esa manera. Los escritores franceses citan el testamento de un obispo, que se declaró válido, aunque la firma consistía únicamente en una cruz seguida de sus iniciales, y de la enunciación de su dignidad."

Doctrinal

La doctrina ha conceptualizado a la firma electrónica de la siguiente manera:

> "Término genérico y neutral para referirse al universo de tecnologías mediante las cuales una persona puede firmar un mensaje de datos."[3]

Por otra parte, también se señala que la firma digital es:

> "Simplemente el nombre que se le da a cierto tipo de firma electrónica basada en el uso de criptografía."[4]

Primer concepto legal en el mundo

Utah Digital Signature Act fue la primera ley en materia de firma digital en el mundo, publicada en 1995, define a la firma digital "como la transformación de un mensaje empleando un criptosistema asimétrico tal que una persona posea el mensaje inicial, la clave pública del firmante pueda determinar con certeza si la transformación, se creó usando la clave privada que corresponde a la clave pública del firmante y si el mensaje ha sido modificado desde que se efectuó la transformación."[5]

Concepto Legal en México

El artículo 89 del Código de Comercio reformado el 29 de agosto de 2003, establece:

> "Firma electrónica los datos en forma electrónica consignados en un mensaje de datos o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante a prueba la información

---

[3] TÉLLEZ VALDÉS, Julio, *Derecho Informático*, McGraw Hill, Tercera edición, 2006.
[4] Idem.
[5] Código de Utah http://www.jus.unitn.it/USERS/PASCUZZI/privcomp97-98/documento/firma/utah/udsa.html Consultada el 12 de noviembre de 2008.

contenida en el mensaje de datos y que produce los mismos efectos jurídicos que la firma autógrafa siendo admisible como en juicio."[6]

Concepto jurisprudencial

"La firma es el nombre escrito de una manera particular, según el modo habitual seguido por una persona en actos sometidos al cumplimiento de esas formalidades."[7]

Actualmente, los criterios que ha establecido el Poder Judicial respecto a la firma son en el sentido de que si el documento que se presente no está firmado debe desecharse, en virtud de que no existe constancia de la expresión de voluntad.[8]

Naturaleza Jurídica

La firma es la afirmación de la individualidad, pero sobre todo de la voluntariedad. En el primer aspecto significa que ha sido la persona firmante y no otra que ha suscrito el documento. En el segundo se acepta lo que ahí se manifiesta.

Carnelutti señala, que en la suscripción actual se ha fundido la manifestación del autor y la declaración de paternidad que originalmente eran distintos, la primera era al comenzar el texto y la otra al concluirlo, esta última es fundamentalmente el vínculo que une a la persona firmante con lo consignado en el documento.

Análisis del concepto de firma

De conformidad con las disposiciones del Código Fiscal de la Federación, la Firma Electrónica Avanzada, tendrá "el mismo valor jurídico que la firma manuscrita y será admisible como prueba en juicio".[9]

No obstante esta disposición, para que tenga valor probatorio pleno, la firma electrónica avanzada deberá cumplir con los siguientes requisitos:

- Autenticidad, el emisor del mensaje queda acreditado, y su firma electrónica avanzada tiene la misma validez que una firma autógrafa.
- Confidencialidad, la información contenida en el mensaje se encuentra en código, por lo que sólo el receptor designado puede descifrar el mensaje.
- Integridad, el mensaje original no puede ser modificado por un tercero, y
- No repudiación, el autor del mensaje no puede decir que no lo hizo.

---

[6] Código de Comercio http://www.cddhcu.gob.mx/LeyesBiblio/pdf/3.pdf. Consultada el 12 de noviembre de 2008.
[7] *Enciclopedia Omeba*, Op. Cit.
[8] Tesis del Poder Judicial relativas a la firma, Registros Núms. 921986, 171757, 265784, 812856.
[9] Código Fiscal de la Federación, http://www.cddhcu.gob.mx/LeyesBiblio/pdf. pp. 13 y 14. Consultada el 15 de noviembre de 2008.

Tecnológicamente hablando, la firma electrónica está relacionada con la infraestructura de clave pública (más conocida como Public Key Infraestructure o PKI),[10] este sistema se basa, básicamente en: la combinación de la llave pública y la privada de cada usuario. Las dos llaves son únicas y se generan mediante algoritmos matemáticos los cuales sirven para:

- Cifrar y descifrar archivos informáticos, y
- Firmar electrónicamente y verificar la firma de archivos informáticos.

Por ello, desde un punto de vista tecnológico la firma electrónica utiliza la clave privada para vincular un determinado archivo con el poseedor de la clave privada (que sólo él controla). Mientras que para verificar la firma electrónica se debe utilizar la clave pública (que puede ser conocida por cualquier persona), y así se puede comprobar que un determinado archivo informático fue firmado electrónicamente por una determinada persona.

Con el desarrollo tecnológico se dio la creación y uso de los documentos electrónicos, con lo cual se tuvo la necesidad de la creación y aceptación de la firma electrónica, la cual debe tener la misma fiabilidad que aporta la firma manuscrita o autógrafa en un documento impreso.

En efecto, la firma electrónica debe garantizar principalmente la identidad del firmante y que el documento no ha sido modificado desde su firma, es decir, debe aportar al mundo de los documentos electrónicos la misma funcionalidad que aporta la firma manuscrita a un documento impreso.

Para firmar electrónicamente documentos electrónicos es necesario disponer de un equipo físico[11] (ordenador, PDA o teléfono móvil) y esencialmente un certificado digital (que no es más que un pequeño fichero que asocia una clave a su titular para propósitos de identificación) que puede estar contenido en:

- El disco duro del ordenador.
- Una tarjeta inteligente.
- Un token de almacenamiento externo.
- La memoria de una PDA.
- La memoria de un teléfono móvil.
- Etc.

Elementos de la firma

La firma tiene que cumplir con ciertos elementos formales y otros funcionales que a saber son:

Formales:

- Signo personal

[10] Concepto de PKI, http://es.wikipedia.org/wiki/Certificaci%C3%B3n_Electr%C3%B3nica. Consultada el 15 de noviembre de 2008.

[11] GALAN, Carlos, *Seguridad y Confianza: Introducción a la Firma Electrónica*, http://www.izenpe.com/s/15-4812/es/contenidos/información/seminario_factura/es_10593/2005_FE_CG.pdf. Consultada el 15 de noviembre de 2008.

- Animus signand; (voluntad de asumir el contenido de un documento).

Funcionales:

-Identificación

-Autentificación

-Confidencialidad

-Integridad

-No repudio

Tipos de firma electrónica:

- Simple: su uso se pacta con firma autógrafa.

Autorización para tener acceso a servicios electrónicos, toda vez que la firma electrónica debe cumplir con los elementos funcionales y formales de la firma autógrafa, por lo que se han establecido diversos mecanismos para ello.

- Avanzada.

Clave de identificación electrónica confidencial (CIEC) se compone de un correo electrónico y una contraseña de acceso, asociados a un Registro Federal de Contribuyentes, su nivel de seguridad es medio, (la contraseña de acceso es conocida por el Servicio de Administración Tributaria, como por el titular de la clave).

Ahora bien, para garantizar la identidad del firmante, se usa la tecnología por medio de claves vinculadas a los datos identificatorios del titular del certificado, es decir, cuando se firma un documento se emplea un número clave, que solo pertenece al firmante y el receptor lo verifica con la clave pública y si el proceso de validación es positivo, se concluye que el firmante del documento es el titular del certificado.

Por lo que respecta a la integridad del documento, en el sentido de que no ha sido modificado tras su firma, se hace dando un código único al documento a partir de su estructura íntima en el momento de ser firmado.

Con la función hash se garantizan estas funciones, pues es una operación matemática que asocia un texto de extensión variable a un número de longitud fija (entre 128 o 160 bits) que se llama resumen. Si el documento sufre alguna alteración o modificación por mínima que sea, hash cambia reflejando que el documento ya no es el mismo.

Cabe mencionar que algunos algoritmos-hash más comunes[12] son:

- MD2 (128 bits – longitud del resumen).
- MD4 (128)
- MD5 (128)

[12] Idem.

- SHA (160)
- SHA-1 (160)
- SHA-224

En cuanto a la garantía del no repudio se ha conformado el siguiente procedimiento:

a) La clave privada que se vincula al certificado y que confiere unicidad a los documentos firmados desde el momento de generar dicha clave y vincularla a sus datos identificatorios (solo él la posee).

b) El certificado y los dispositivos de firma empleados deben basarse en tecnologías y procesos, seguros que eviten el uso o sustracción de la clave por parte de terceros y que se encuentren homologados por la autoridad de certificación emisora del certificado empleado.

c) Que el certificado esté activo en el momento de ser empleado.

d) Que los receptores de documentos firmados dispongan de un instrumento de verificación seguro que no permita suplantar identidades del firmante o de la autoridad de certificación que realiza la validación.

En estos términos, es claro que la seguridad de la firma electrónica es evidente y esta se garantiza por:

Encriptación, lo que garantiza que la comunicación a través de la red está protegida.

Autenticación, con la que se garantiza la identidad de ambos partícipes.

Confiabilidad, pues los participantes desean saber si la otra persona con la que interactúa es confiable.

No-repudio, dado que los participantes desean poder probar la transacción.

Funcionamiento de la firma electrónica avanzada

Como ya se expresó con anterioridad, se obtiene una clave privada que se le proporciona al usuario y éste, tiene la responsabilidad de protegerla y mantenerla en secreto. Asimismo se otorga una clave pública.

Ahora bien, al archivo se le aplica la clave privada lo que conlleva a que el resumen se cifre y al aplicarse la clave pública se pueda verificar el mensaje.

Para llevar a cabo lo anterior se hace uso de la criptografía la cual tiene como objetivo básico, encontrar un sistema que permita hacer llegar determinada información considerada secreta desde un lugar de origen, a otro llamado destino, de forma tan segura que si el mensaje es interceptado el atacante no pueda decodificar

el mensaje, este sistema se ha utilizado desde la época de los romanos.

Métodos Criptográficos

Cifrado simétrico o clave secreta

En 1977, se pública el Data Encryption Standard (Des) a partir de un encargo del Ministerio de Defensa Norteamericano a IBM.

Este sistema se basa en un algoritmo de sustitución y transportación de bits y puede ser utilizado en el texto cifrado y a la que inversa, por su sencillez no puede ser utilizado por un conjunto numeroso de interlocutores.

Cifrado asimétrico

En este sistema se utiliza una pareja de claves creadas mediante métodos matemáticos complejos. Una clave privada que será custodiada por su propietario y una clave pública que será conocida por todos los usuarios. Estas dos claves son complementarias entre sí, lo que cifra una sólo puede descifrarlo la otra y viceversa y segundo las ventajas del uso de ese sistema es que es más seguro, dado que suprime la necesidad del envío de la clave. Su inconveniente es la lentitud de la operación.

En la firma electrónica avanzada se usa la criptografía asimétrica (Sistema criptográfico de clave pública (RSA), es la técnica más reconocida y utilizada mundialmente. También está Rabin, El Gamal, Mc Eliece, Knapsack, Probabilística, entre otros.

A fin de poder hacer uso de la firma electrónica avanzada debe asegurarse que existan los órganos que emitan los certificados digitales correspondientes, los cuales deben ser confiables y para ello debe crearse una infraestructura para que se puedan otorgar las claves públicas (PKI).

Efectivamente, las autoridades de certificación deberán cumplir con el papel de fedatarios públicos digitales para que puedan emitir certificados acordes a su naturaleza. Cabe señalar, que el más extendido es el de la FNMT aplicado al ámbito tributario. También están VeriSign, ACE, FESTE, Camerfirma, Izenpe, etc.

La importancia de estas autoridades de certificación, radica en el hecho de que los certificados digitales son piezas de software que identifican a su propietario. Estos certificados digitales se obtienen a través de una solicitud que se hace vía Internet y posteriormente se apersona el solicitante ante una oficina de acreditación de certificación digital y después puede descargar el certificado en su ordenador para así poder entablar relaciones con terceros utilizando el Internet en forma segura.

Como ya se dijo, la clave pública del usuario firmada por una autoridad de cer-

tificación es lo que se llama Certificado Digital (acuses) y puede ser almacenado en directorios para posibilitar su consulta por múltiples usuarios.

Es necesario señalar, que hay variedad de certificados que sirven para una diversidad de actuaciones, es decir, no todos los certificados son iguales.

El formato estándar de los certificados digitales[13] es el siguiente:

1. Versión del certificado.
2. Número de serie.
3. Nombre del emisor.
4. Fecha inicio/expiración.
5. Nombre del Titular.
6. Clave pública del titular.
7. Extensiones.
8. Firma del emisor.

Como dijimos no todos los certificados son iguales[14] y cada cual posee su propia utilidad.

- Clase 0: Sin identificación.
- Clase 1: Con registro.
- Clase 2: Administración Pública.
- Clase 3: Fedatario Público.
- Clase 4: Militar.
- Clase WEB: Certificado de servidor seguro.
- De componente.

Con todos estos mecanismos se resguarda la seguridad del interactuar de las partes, que usan estos medios tecnológicos, pues se cuida:

- ✓ La privacidad.
- ✓ La autenticación.
- ✓ La autorización.
- ✓ La autoria.

No obstante este cuidado, siempre existe latente el ataque cibernético por parte de los llamados delincuentes informáticos que pueden realizar las siguientes conductas ilícitas entre otras muchas:

i. Ataque directo.
ii. Denegación de servicio.
iii. Pérdida de privacidad.
iv. Modificación de datos.
v. Suplantación, entre otras.

Países que regulan la firma electrónica avanzada

La primera ley en materia de Firma Digital en el Mundo fue la denominada "*Utah Digital Signature Act*", que fue publicada en 1995, en el Estado de UTAH.

El concepto de firma electrónica se precisó en la hoja Número dos, de este trabajo.

---

[13] Idem.
[14] Idem.

Alemania[15]

El 13 de junio de 1997, fue promulgada la *Ley sobre Firmas Digitales* y el 7 de junio del mismo año, fue publicado su Reglamento. Law Governing Frame-work Conditions for Electronic Signatures and Amending Other Regulations (Bundesgesetzblatt- BGBI. Teil I S. 876 vom 21. Mai 2001). Publicados el 16 de mayo de 2001 en la Official Journal N° 22, el 22 de mayo de 2001. In Forcé 22 May 2001).

Argentina[16]

El 17 de marzo de 1997, el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la Resolución 45/97 -firma digital en la Administración Pública. El 14/12/2001 se publicó la *Ley de Firma Digital para la República Argentina* 25/506.

Bélgica[17]

Loi fixant certaines regles relatives au cadre juridiqe pour les signatures électroniques et les services de certification (Moniteur belgue du 29 septembre 2001). Loi introduisant l'utilisation de mohines de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, 20 octobre 2000. Belgisch Staatsblad, 22/12/200. Moniteur Belge.

C.E.E.[18]

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. Decisión de la Comisión, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica (2000/709/CE).

Canadá[19]

British Columbia Bill 13-2001, The Electronic Transactions Act.

---

[15] Alemania Ley. http://www.bundesnetzagentur.de/media/archive/3612.pdf. Consultada el 18 de noviembre de 2008.

[16] Argentina Ley de Firma Digital http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm. Consultada el 18 de noviembre de 2008.

[17] Bélgica Ley http://economie.fgov.be/information_society/e-signatures/law_e_signature_002.pdf. Consultada el 18 de noviembre de 2008.

[18] Parlamento Europeo y del Consejo, 1999/93/CE, de 13 de diciembre de 1999, Diario Oficial No. L 013 de 19/01/2000 p. 0012-0020 http://www.cert.fnmt.es/legsoporte/directiva.PDF. Consultada el 18 de noviembre de 2008.

[19] Canadá The Electronic Transctions Act. http://www.qp.gov.bc.ca/statreg/stat/e/01010_01.htm. Consultada el 18 de noviembre de 2008.

Colombia[20]

Colombia (*Ley* 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación).

Chile[21]

Chile *Ley sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación* 2002.

Dinamarca[22]

Act 417 of 31 May 2000 on Electronic Signatures. Bill L 229. Execütive Order on Security Requirements etc., for Certificatión Authorities. Execütive Order N° 923 of 5 October 2000. Execütive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors. Execütive Order N° 922 of 5 October 2000.

Francia

Décreto n° 2001-272 de 30 de marzo de 2001, pris pour l'application de l 'article 1316-4 del Código Civil relativo a la firma electrónica*. Ley 2000-230* de 13 de marzo de 2000.

Irlanda

Electronic Commerce Act, 2000 (Number 27 of 2000)

Italia

El 15 de marzo de 1997, fue publicado el "*Reglamento sobre: Acto, Documento y Contrato en Forma Electrónica*" aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999, las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la ley sobre firma electrónica.

Japón

1/04/2001 *Ley sobre Firma Electrónica y Servicios de Certificación*.

Luxemburgo

Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques,

---

[20] Colombia Ley 527/1999 Diario Oficial http://www.secretariasenado.gov.co/leyes/L0527_99.HTM. Consultada el 18 de noviembre de 2008.

[21] Chile Ley sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma 19.799, Publicada en el Diario Oficial el 12 de abril de 2002, http://repositorio.idiem.cl/ley19799.pdf. Consultada el 18 de noviembre de 2008.

[22] Dinamarca Ley publicada en Boe. 21, 20 de diciembre de 2003, http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343pdf. Consultada el 18 de noviembre de 2008.

au paiment électronique et á la création du comité “commerce ” détermination d ‘un e et de la Chambre des métiers.

Panamá[23]

Ley 43 de Comercio Electrónico del 3 de agosto de 2001.

Portugal[24]

Decree-Law 290-D/99.

Reino Unido[25]

Electronic Communications Act, del 25 de mayo del 2000.

Suecia

Qualified Electronic Signatures Act (FSF 2000:832)

ONU

Cabe señalar que la Organización de las Naciones Unidas por conducto de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNDUMI, mejor conocida por sus siglas en inglés UNCITRAL), con sedes tanto en Nueva York como en Viena, se compone por 37 países. Funciona desde 1968, elaborando múltiples convenciones, además de reglas de arbitraje, modelos de contratos, de cláusulas contractuales y guías jurídicas, pero sobre todo Leyes Modelo como la de Arbitraje (adoptada por México en 1992), Comercio Electrónico (adoptada en México en el 2000) y Firma Electrónica (adoptada por nuestro país en el 2003).

En la sesión del día 12 de diciembre de 2001, fue aprobada por el pleno de la 85a Sesión Plenaria de la Asamblea General la Ley Modelo sobre las Firmas Electrónicas.

OCDE

En marzo de 1997, la Organización para la Cooperación y el Desarrollo Económico publicó su recomendación para el establecimiento de políticas sobre Criptografía, sin embargo solo establece una serie de lineamientos que se sugiere a los gobiernos adoptar al momento de legislar en materia de firma digital y de Entidades Prestadoras de Servicios de Certificación.

Ecuador

Ley del Comercio Electrónico y su reglamento de 2003.

---

[23] Panamá Ley 43, http://www.informatica-juridica.com/anexos/anexo956.asp. Consultada el 21 de noviembre de 2008.

[24] Portugal Published in the D.R. No. 178 (Series I-A), of 2 of August. http://www.icp.pt/template20.jsp?categoryId=98100&contentId=164788.

[25] Reino Unido Ley, http://www.informatica-juridica.com/anexos/anexo1437.asp. Consultada el 21 de noviembre de 2008.

En el **Perú** se ha dictado la Ley de Firmas y Certificados Digitales (Ley 27269), de fecha 26 de mayo de 2008.

Chile

El 15 de Septiembre del año 2003, el Gobierno de Chile expidió la ley 19.799, en la que se señala que los documentos serán válidos de la misma manera y producirán los mismos efectos que los expedidos en soporte de papel.

En dicha ley se señala que se usarán formatos técnicos, formato clásico PKCS#7 **XMLDsig** firma XML.

Las modalidades de la firma que regula son:

- **Firma básica.**
- **Firma fechada.**
- **Firma validada o firma completa.**

España

(Real Decreto Ley 14/1999 sobre Firmas Electrónicas. Septiembre de 1999, Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden 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. -Ley de Servicios de la Sociedad de Información-) El Proyecto de Ley de firma electrónica, de 20 de junio de 2003, ha introducido diversas modificaciones respecto del vigente Real Decreto ley 14/1999 de firma electrónica. Tras su ratificación por el Congreso de los Diputados, se acordó someterlo a una amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto, entre los puntos más importantes que considera están: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, Time stamping, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y el más debatido, Certificados para Personas Morales, un caso distinto a la firma electrónica de los representantes de las personas morales, pues se persigue dar firma a las empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados

Asimismo existe la Ley 59/2003 de firma electrónica de 19 de diciembre de 2003 y que regula la firma.

- **Simple**. Identifica al firmante.
- **Avanzada**. Garantiza la integridad PKI.
- **Reconocida**. Cualificada por Qualified.

La Ley de Firma Electrónica de España del 19 de diciembre de 2003, en su

artículo 4°, precisó el uso de la firma electrónica en el ámbito de la Administración Pública, lo que implica también a sus organismos públicos y las entidades dependientes o vinculadas a las mismas y las relaciones que mantengan aquella y éstos con los particulares.

Asimismo, estableció que los servicios de certificación, se presentarán sin que se requiera autorización previa, sino ésta se realizará en el régimen de simple competencia, asimismo prevé las causas de extinción y la suspensión de su vigencia.

México.

Código Fiscal de la Federación publicado el 5 de enero de 2004

17-D	• Aspectos generales para la presentación de documentos digitales. • Efectos de la Firma Electrónica Avanzada en documentos digitales.· • Comparecencia ante el SAT. • Prestadores de Servicios de Certificación Autorizados por el Banco de México. • Reserva de los datos de identidad. • Certificados emitidos por la Secretaría de la Función Pública y otros.
17-E	• Acreditación de documento digital mediante sello digital.
17-F	• Facultades de certificación de Firmas Electrónicas Avanzadas otorgadas por el SAT.
17-G	• Datos que deberá contener los certificados que emita el SAT.
17-H	• Casos en que los certificados quedarán sin efectos.
17-I	• Método para verificar la integridad y autoría de documentos o sellos digitales.
17-J	• Obligaciones de un titular de un certificado emitido por el SAT.

19-A	• Presentación de documentos digitales por personas morales.
31	• Sujetos obligados a tramitar el certificado digital de Firma Electrónica Avanzada.
2do. Transit. Fr.XXII	• Aprovechamiento de la infraestructura Extendida de Seguridad implementada por el Banco de México.

Reglas de la Resolución Miscelánea Fiscal, publicadas el 31 de mayo de 2004 y modificadas el 28 de diciembre de 2005

2.22.1	• Procedimiento para tramitar el certificado digital de Firma Electrónica Avanzada.
2.22.2	• Renovación de certificados digitales.
2.22.3	• Del contenido de los certificados digitales. Complemento al artículo 17-G del CFF.
2.22.4	• De los dispositivos de almacenamiento, complemento al artículo 17-H del CFF.
2.22.5	• Revocación de certificados digitales.

Código de Comercio publicado el 29 de agosto de 2003

Capítulo I	• De los mensajes de datos.
Capítulo II	• De las firmas.
Capítulo III	• De los Prestadores de Servicios de Certificación.
Capítulo IV	• Reconocimiento de certificados y firmas electrónicas de extranjeros.
Transitorios	• Disposiciones Transitorias.

Uso de la Firma Electrónica Avanzada en México

El uso de esta herramienta es muy reciente, no obstante, tenemos los siguientes:

Banco de México

Sistema de pagos.

Secretaría de la Función Pública

- Declaración patrimonial de funcionarios (DECLARANET).
- Sistema de COMPRANET

Secretaría de Economía

- Sistema de inscripciones al Registro Público de Comercio (SIPRED).
- Norma de conservación de documentos digitales (NOM-151).

Instituto Mexicano del Seguro Social

- Sistema IDSE (IMSS desde su empresa). Permite a los patrones realizar movimientos sobre la situación de sus empleados desde Internet.

Uso específico de la firma electrónica en las llamadas PDA.

En el manual del usuario de la computadora de bolsillo (www.htc.com), se observa en el capítulo 7, relativo a "Trabajar con correos corporativos electrónicos corporativos" en el punto 7.5 "Seguridad del correo electrónico" indica lo siguiente:

> Windows Mobile en su computadora de bolsillo protege los correos de Outlook a través de Secure/Multipurpose Internet Mail Extensión (S/MIME), que le permite firmar y cifrar digitalmente sus mensajes.
>
> **Requisitos**. El Cifrado S/MIME y las firmas digitales para computadora de bolsillo basados en Windows Mobile sólo están disponibles con Exchange Server 2003 SP2 o una versión posterior que soporte S/MIME. Si no utiliza uno de estos productos o no ha sincronizado aún, estas opciones no están disponibles.
>
> **Nota**. Puede cifrar un mensaje con o sin un certificado. Sin embargo, para leer un mensaje cifrado necesitará un certificado válido para descifrarlo.

Para firmar y cifrar individualmente un mensaje nuevo.

1. Haga clic en **Inicio**>**Mensajería**>**Correo de Outlook.**
2. Haga clic en **Menú**>**Nuevo** para crear un nuevo mensaje.
3. Haga clic en **Menú**>**Opciones de mensajes**.

4. En la lista **Seguridad**, seleccione si cifrar solamente, firmar el mensaje solamente o hacer ambas cosas.
5. Haga clic en **Listo**.

Para verificar la firma digital de un mensaje firmado que recibe.

1. Abra el mensaje de correo electrónico de Outlook que ha sido firmado digitalmente.
2. **En la parte superior del mensaje, haga clic en Ver estado de firma**.
3. Haga clic en Menú > Comprobar certificado.

Para ver los detalles del certificado en el mensaje, haga clic en **Menú**> **Ver certificado.**

Nota. Puede haber distintas razones por las que una firma digital no es válida. Por ejemplo, el certificado del autor del mensaje puede haber caducado, puede haber sido revocado por la autoridad del certificado o el servidor que verifica el certificado no está disponible. Contacte con el remitente para informar del problema.

Para firmar digitalmente y cifrar todos los mensajes.

Puede configurar ActiveSync para firmar y cifrar digitalmente todos los mensajes salientes. Debe obtener un certificado válido para firmar y cifrar mensajes de correo electrónico con éxito.

1. Haga clic en **Inicio**>**ActiveSync**.
2. Haga clic en **Menú**> **Opciones**.
3. Seleccione el tipo de información de **correo electrónico** y haga clic en **Configuración**. En la pantalla Opciones de sync. De correo, haga clic en **Menú**>**Avanzadas**.
4. Seleccione **cifrar mensajes** para proteger sus correos y evitar que sean leídos por receptores no deseados. Seleccione **Firmar mensajes** para que los receptores estén seguros de que los correos son enviados por usted y no han sido alterados.
5. Haga clic en **Menú** > **Elegir certificado** para seleccionar un certificado para firmar o cifrar los mensajes de correo electrónico saliente.

Punto de vista personal

Una vez hecho un análisis somero del tratamiento doctrinal y legal que se ha dado a la firma electrónica y sus usos en el contexto nacional e internacional se procederá su análisis de conformidad con la teoría de las relaciones de Khun, en la cual se analizan el choque de paradigmas y el hecho de que al final se impone la postura del grupo dominante.

Conforme a esta teoría y analizando las disposiciones que regulan las relacio-

nes de los particulares en el uso de firma electrónica de documentos, se observa que los legisladores han normado éstas, tratando de que sean lo más diáfanas posibles, pero considero que su aplicación no atiende a las circunstancias y realidad de la sociedad, porque en su mayoría, si bien tienen acceso a la educación, ésta no llega al nivel del uso y manejo de las herramientas tecnológicas como lo es el uso de una computadora para enviar documentos firmados electrónicamente o elaborar procedimientos administrativos, no obstante que la Secretaría de Hacienda y Crédito Público lo ha implementado de manera aceptable en el pago de impuestos; en consecuencia, es claro que la generalización del uso de la firma electrónica debe pasar por un largo periodo de transición para poder aceptarse y aplicarse mayoritariamente, dado que sus beneficios serían en el mejor momento de la actividad administrativa y sobre todo jurisdiccional si se pretende introducir en un tribunal como lo es el Tribunal Federal de Justicia Fiscal y Administrativa.

Por otra parte, y atendiendo a la teoría integradora de la argumentación de Mac Cormick, con la que se pretende concretar, explicar y justificar las ideas expresadas en abstracto con relación al razonamiento práctico.

En este caso, consideramos que se trata de un caso fácil o claro, el cual, según la teoría de Mac Cormick, puede resolverse aplicando las deducciones o inferencias, es decir, usando el *modus ponens,* que es el silogismo demostrativo por excelencia y se basa en la ley.

Las disposiciones que rigen a la firma electrónica y los medios por los que se cuidan sus elementos desde mi punto de vista se encuentran claramente prescritos en las normas que los rigen, en virtud de que la firma electrónica es un procedimiento reconocido legalmente y sustentado en un equipamiento informático y se usa en cualquier documento electrónico.

En este orden de ideas, es claro que el uso de la firma electrónica, en el quehacer cotidiano entre particulares y autoridades, ha evolucionado a grandes zancadas, por lo que se ha perfeccionando de tal manera, que actualmente es verdaderamente confiable su uso además que se está generalizando entre las partes, razón por la cual la implementación del juicio en línea propuesto por el Presidente del Tribunal Federal de Justicia Fiscal y Administrativa en la Décimo Séptima Reunión Nacional de Magistrados, celebrada el mes de agosto de 2008 en Acapulco, Guerrero, es totalmente viable y prometedora, no obstante debe romperse una fuerte resistencia tanto de los Juzgadores como de las partes que acuden a este Tribunal, en virtud de que ante el desconocimiento se considera que el uso de la firma electrónica por parte de todos los participantes, así como las pruebas que se lleguen a exhibir, las cuales actualmente deberán

someterse a un periodo de transición, incluyendo testimonios notariales contarán con una validez confiable, en virtud de que se podrán consultar los certificados digitales expedidos al efecto. Esto no implica que dichos certificados no se puedan desvirtuar por las partes lo que implicará un nuevo giro en la teoría de la valoración de las pruebas y su impugnación; en efecto, la certificación que se haga estará sujeta a impugnación, pues en todo momento se puede acudir al banco de almacenamiento de los certificados para verificar los datos que contienen, los cuales al ser expedidos por un tercero que es a su vez autorizado y se rige por ciertas normas, con lo que se pretende asegurar mayor certeza del autor material de los documentos y se podrán consultar y analizar más rápidamente.

Ciertamente, con los candados que técnicamente se implementan para el uso de la firma electrónica, es claro que el problema de certidumbre que se vislumbraba se desvanece y podemos con confianza lograr determinar la autoría del documento electrónico tanto por parte del actor, de las autoridades, de las partes, así como los instrumentos notariales que se exhiban en virtud de que todo aquel que firme un documento electrónico debe contar con su certificado vigente y validado. Además de que el contenido e integridad del documento también se encuentra garantizada, así como su posible manipulación posterior.

Lo que me hace vislumbrar que el uso de esta herramienta pueda aplicarse a otros aspectos del procedimiento como lo son las notificaciones por esta vía, máxime que se están implementando los mecanismos correspondientes.

Efectivamente, analizando la seguridad del correo electrónico que se está implementando, el envío de documentos firmados electrónicamente, es casi una realidad inminente en general, por lo que, en muy poco tiempo se podrán llevar a cabo las notificaciones por este medio, pues se podrá adjuntar al archivo del acuerdo, el archivo en el que se remitieron las pruebas exhibidas por cualquiera de las partes, con lo que también se supera la objeción en relación a los traslados.

Por último, considero que el uso de la informática en los procedimientos jurisdiccionales no tendrán más límite que la imaginación, tanto de los particulares como de las autoridades, aunado sobre todo al actuar innovador del juzgador, que a mi juicio es el más reacio a esta evolución, en virtud de que se tiene muy poco acceso a la informática, herramienta que nos permite soñar con lo inalcanzable, lo anterior en virtud de que no se tienen los conocimientos ni el menor interés en obtenerlos aunado al hecho de que los equipos con los que se cuenta para el desempeño del trabajo son demasiado obsoletos, además de que por el cuidado que el área de informática de este Tribunal señala debe tener, tiene relación al Sistema Integral de Control de Jui-

cios con el que monitoreamos el debido control de los documentos de nuestros expedientes, así como su ubicación, restringen el acceso a utilerías que son muy convenientes para el desempeño del trabajo, así como a los antivirus que permiten un mejor cuidado y desempeño de los equipos. No obstante es de reconocerles que el Sistema Integral de Control de Juicios que opera desde 2001, no ha tenido un ataque de virus, el cual nos paralice.

Ante este nuevo panorama tengo la plena convicción que el gran desencanto que sufrimos por el enorme cúmulo de asuntos que día con día los particulares presentan, se podrá superar, al utilizar esta herramienta dado que podrán ser estudiados más profunda y acertadamente, además de que su trámite se verá agilizado, lo que nos permitirá cumplir con el mandato constitucional que nos constriñe a impartir justicia en forma pronta, integral y expedita.

En esta medida, si tenemos bien ganada una fama de más de setenta y dos años, con esta herramienta la podremos fortalecer, pues un tribunal es más confiable y respetado en atención a los fallos que hace. No obstante debemos ser cuidadosos y no irnos con el canto de las sirenas, pues si todos los asuntos se agilizan, pronto tendremos un mayor número de asuntos íntegrados que deberán resolverse, por tal razón en este momento, creo que sería adecuado que los juzgadores hagamos uso de esa herramienta con el objeto de sistematizar nuestros criterios, cuestión que si bien actualmente se hace, se realiza en forma rudimentaria y atendiendo en muchos de los casos a la buena memoria de los Magistrados y sus colaboradores.

Por otra parte, respecto a la información que con motivo de la ley de transparencia nos es solicitada, estimo que también podrá ser proporcionada con mayor celeridad al contar con una herramienta que nos lo permita.

No obstante, debemos hacer llegar los conocimientos a las partes para que confíen en el uso de esta herramienta; en esta tesitura, la propuesta de la implementación del Juicio en Línea, cada vez se fortalece y lo hace más viable, sobre todo, porque las partes tendrán la confianza en su trámite, pues el uso de la firma electrónica de todas las partes es básico, pues es la prueba de la manifestación de su voluntad; por tal razón, al manejar las herramientas tecnológicas, podremos determinar su existencia y, por tanto, su valor en el campo del derecho.

Por último, y como conclusión final, estimo que el Tribunal Federal de Justicia Fiscal y Administrativa, si pretende estar a la vanguardia en el uso de los avances tecnológicos, debe organizar cursos de Derecho informático e informática jurídica, con los cuales aprendamos a utilizar en nuestro trabajo las herramientas que nos permitan desempeñarlo con mayor calidad

y productividad con lo que se dará dar un paso hacia la modernidad que nos ha dejado atrás desde hace un buen tiempo.

Con todo lo anterior, es claro que se pretende lograr uno de los objetivos de la sociedad de la información, que es que todos los participantes de la comunidad tengan un mayor acceso al conocimiento para la mejor toma de sus decisiones, con lo que también se fomentará la democracia, transparencia, responsabilidad y, por lo tanto, un gobierno eficaz.

Otro de los objetivos de la sociedad de la información, estimo que se lograría pues se estaría reduciendo la brecha digital que se ha creado entre sus habitantes.

Ahora bien, y analizando los beneficios que pudiera traer el uso de esta herramienta dentro de un juicio en línea ante este Tribunal, encontramos los siguientes:

- El acceso a los expedientes serían de 365 días al año.

- El procedimiento se agilizaría además de que sería igualmente seguro.

- Tal vez se podría reducir el tiempo del procedimiento a una cuarta parte del mismo.

- Con todo lo anterior se ahorraría tanto tiempo como dinero.

Respecto a la actividad del Tribunal, considero que obtendríamos los siguientes beneficios.

- Se posicionaría como uno de los Tribunales que usan tecnología de vanguardia.
- Se contaría con mecanismos eficientes de evaluación del desempeño.
- Se reduciría el tiempo de trámite administrativo e incrementaría el tiempo para el estudio y análisis jurisdiccional.
- Se podría hacer un reparto equitativo del trabajo entre todos los miembros del Tribunal sin importar su jurisdicción.
- Se facilitaría el control y acceso a la base de datos.
- Se podrían fijar y sistematizar los nuevos criterios.
- El último y el más importante es que se lograría una jornada de trabajo eficiente y mejoraría con ello la calidad de vida de sus integrantes.

Para finalizar, considero que debemos crear la confianza y seguridad en el uso de las herramientas tecnológicas que tenemos a nuestro alcance con el objeto de que nuestra vida, si bien se vuelva más fácil, también sea de mejor calidad para todos.

Recordemos que la necesidad es la mejor maestra para encontrar soluciones y alternativas, siempre y cuando queramos ser humildes aprendices.

FUENTES DE INFORMACIÓN

LEGISGRÁFICAS

- **Internacional**

Código de Utah, http://www.jus.unitn.it/USERS/PASCUZZI/privcomp97-98/documento/firma/utah/udsa.html. Consultada el 12 de noviembre de 2008.

- **Federal**

Código de Comercio, http://www.cddhcu.gob.mx/LeyesBiblio/pdf/3.pdf. Última reforma de 17/04/2008. Consultada el 12 de noviembre de 2008.

Código Fiscal de la Federación, http://www.cddhcu.gob.mx/LeyesBiblio/pdf/8.pdf. Última reforma del 01/07/2008. pp. 13 y 14 consultadas el 12 de noviembre de 2008.

Diario Oficial de la Federación 6/10/2000: Convenio de Colaboración para establecer los mecanismos de emisión y administración de los certificados digitales, que se utilizarán para acceder al Registro Público de Comercio y para realizar transacciones comerciales, que celebran la Secretaría de Comercio y Fomento Industrial y la Asociación Nacional del Notariado Mexicano A.C.

Diario Oficial de la Federación 6/10/2000: Convenio de Colaboración para establecer los mecanismos de emisión y administración de los certificados digitales, que se utilizarán para acceder al Registro Público de Comercio y para realizar transacciones comerciales, que celebran la Secretaría de Comercio y Fomento Industrial y el Colegio Nacional de Contaduría Pública Mexicana A.C.

BIBLIOGRÁFICAS

Diccionario de la Real Academia de la Lengua Española, Vigésima Segunda Edición.

Enciclopedia Jurídica Omeba, Tomo XII, Bibliográfica Argentina.

TÉLLEZ VALDÉS, Julio, *Derecho Informático*, Mc Graw Hill, Tercera Edición, 2006.

REYES KRAFFT, Alfredo Alejandro, *La Firma Electrónica y las Entidades de Certificación*, Porrúa, México 2003.

CAMPOLII, Gabriel Andrés, *La Firma Electrónica en el Régimen Comercial Mexicano*, Porrúa, México 2004.

RIOFRÍO MARTÍNEZ-VILLALBA, Juan Carlos, *La Prueba Electrónica*, Temis, Bogotá-Colombia 2004.

ACOSTA ROMERO, Miguel, *Nuevo Derecho Mercantil*, Capítulo XVIII: "La Firma en el Derecho Mercantil Mexicano", Porrúa, México, 2000.

REYES-KRAFFT, Alfredo Alejandro, *Firma Electrónica*, http://www.iupuebla.com/Doctorado/Docto_derecho/Material_profe/LA%20FIRMA%20ELECTRONICA.pdf.

CIBERGRÁFICA

IUS 2007 Tesis del Poder Judicial relativas a la firma, Registro No. 921986, 171757, 265784, 812856.

Código de Utah http://www.jus.unitn.it/USERS/PASCUZZI/privcomp97-98/documento/firma/utah/udsa.html. Consultada el 12 de noviembre de 2008.

Concepto de PKI http://es.wikipedia.org/wiki/Certificaci%C3%B3n_Electr%C3%B3nica. Consultada el 15 de noviembre de 2008.

Dr. Carlos Galán "*Seguridad y Confianza: Introducción a la Firma Electrónica*" http://www.izenpe.com/s15-4812/es/contenidos/informacion/seminario_factura/es_10593/adjuntos/2005_FE_CG.pdf. Consultada el 15 de noviembre de 2008.

Alemania, Ley http://www.bundesnetzagentur.de/media/archive/3612.pdf. Consultada el 18 de noviembre de 2008.

Argentina, Ley de firma digital http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm. Consultada el 18 de noviembre de 2008.

Bélgica, Ley http://economie.fgov.be/information_society/e-signatures/law_e_signature_002.pdf. consultada 18 de noviembre 2008.

Parlamento Europeo y del Consejo, 1999/93/CE, de 13 de diciembre de 1999, Diario Oficial N° L 013 de 19/01/2000 P. 0012-0020, http://www.cert.fnmt.es/legsoporte/directiva.PDF. Consultada el 18 de noviembre de 2008.

Canadá, The Electronic Transctions Act, http://www.qp.gov.bc.ca/statreg/stat/e/01010_01.htm. Consultada el 18 de noviembre de 2008.

Colombia, Ley 527/1999, Diario Oficial, http://www.secretariasenado.gov.co/leyes/L0527_99.HTM. Consultada 18 de noviembre de 2008.

Chile, Ley sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma 19.799, Publicada en el Diario Oficial el 12 de abril de 2002, http://repositorio.idiem.cl/ley19799.pdf. Consultada el 18 de noviembre de 2008.

Dinamarca, Ley publicada en Boe 21, 20 de diciembre de 2003, http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf. Consultada el 18 de noviembre de 2008.

Panamá, Ley 43, http://www.informatica-juridica.com/anexos/anexo956.asp. Consultada el 21 de noviembre de 2008

Portugal, Published in the D.R. No. 178 (Series I-A), of 2 of August, http://www.icp.pt/template20.jsp?categoryId=98100&contentId=164788.

Reino Unido, Ley http://www.informatica-juridica.com/anexos/anexo1437.asp. Consultada el 21 de noviembre de 2008

Jordi Albareda, de Tradise para COELCO “Todo sobre la firma electrónica y la factura telemática para su empresa”, http://www.microsoft.com/spain/empresas/tecnologia/firma_electronica.mspx?gclid=CJy3srrDi5cCFSEeDQodK2pU4g. Consultada el 18 de noviembre de 2008.