INFORME DE INVESTIGACIÓN CIJUL

TEMA: LA FIRMA DIGITAL

RESUMEN: El presente informe de investigación recopila nociones de Doctrina acerca del tema de la Firma Digital, desarollando su concepto y características principales, además se profundiza en su validez y otros temas como su autenticación.

Índice de contenido

1 DOCTRINA

a) Concepto de Firma digital

[BRIZZION][1]

“A diferencia del encriptado, la firma digital es un invento reciente, estimulado por la expansión de las comunicaciones digitales. Permite que el receptor de un mensaje pueda verificar la autenticidad de la firma que aparece en el documento digital. El sistema es útil tanto para imposibilitar la alteración de la firma como para establecer que ella pertenece efectivamente a quien aparece como firmante. "Para tener validez jurídica, las

firmas digitales deben permitir verificar tanto la identidad del autor de los datos (autenticación de autoría), como comprobar que dichos datos no han sufrido alteración desde que fueron firmados (integridad)".

En el método de criptografía tradicional, tanto quien envía el mensaje, como quien lo recibe, conocen y utilizan la misma clave. De ello resulta cierto nivel de inseguridad, pues aquélla puede ser interceptada por un tercero, quien queda así en condiciones de utilizarla para leer todos los mensajes que pretendían estar ocultos.

En la década de los años '70 se inventó la criptografía con clave pública, que funciona de este modo: el emisor del mensaje dispone de un par de claves, llamadas pública y privada; la primera se da a conocer, mientras que la segunda es mantenida en secreto. Al firmar digitalmente un mensaje, el emisor emplea un elemento que sólo él conoce (su clave privada), pero que permite al receptor establecer que el creador de la firma necesariamente dispuso de ese elemento secreto. A tal fin se emplean criptogramas de clave asimétrica, como el DSA (Digital Signature Algorithm) o el SET (Secure Electronic Transactions).

En la práctica, la denominada firma digital combina los caracteres que forman la clave privada con la totalidad de los caracteres del documento al que se le quiere adosar la firma. El destinatario recibe el documento con la firma digital y la clave pública del emisor, y que da en situación de verificar su autenticidad mediante la asociación con la clave pública del suscriptor; si la serie de caracteres que obtiene coinciden con los del documento transmitido, la firma resulta válida.

Dentro del mismo sistema, se considera digesto de mensaje seguro al que es encriptado con la clave privada del firmante, de modo que quien dispone del documento digital inicial, la transformación encrip-tada y la clave pública del firmante, pueda determinar que esa transformación fue realizada utilizando la clave privada que corresponde a la clave pública del firmante. Se trata, con palabras del artículo 2.1. de la ley alemana de firma electrónica del 13 de junio de 1997, de verificar "el propietario de la clave de firma y el carácter de no falsificada de la información".

La firma digital, por sí sola, no brinda confidencialidad a la transmisión si el documento es remitido sin encriptar.

Conforme al artículo 29 del Anteproyecto de Ley de Firma Digital de 1999, "Clave privada: es aquella que se utiliza para firmar digi-talmente, mediante un dispositivo de creación de firma

digital, en un criptosistema asimétrico seguro. Clave pública: es aquella que se utiliza para verificar una firma digital, en un criptosistema asimétrico seguro". "Dispositivo de verificación de firma digital: es un dispositivo de hardware o software técnicamente confiable que verifica una firma digital utilizando la clave pública del firmante". "Función de digesto seguro: es un algoritmo criptográfico que transforma un documento digital en un digesto de mensaje, de forma tal que se obtenga el mismo digesto de mensaje cada vez que se calcule esta función respecto del mismo documento digital y sea computacionalmente no factible tanto inferir o reconstituir un documento digital a partir de un digesto de mensaje como encontrar dos documentos digitales diferentes que produzcan el mismo digesto de mensaje". "Criptosistema asimétrico seguro: es un método criptográfico que utiliza un par de claves compuesto por una clave privada utilizada para firmar digitalmente y su correspondiente clave pública utilizada para verificar esa firma digital, de forma tal que, con las longitudes de claves utilizadas, sea computacionalmente no factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como desencriptar aquello que ha sido encriptado con una clave privada sin la utilización de la correspondiente clave pública".

El Borrador final de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre un marco común para las firmas electrónicas [digitales] del 13 de mayo de 1998 (COM [1998] 297/2) provee estas definiciones en el artículo 5°: "1. 'Firma electrónica' [digital], una firma bajo forma digital, integrada, ligada o asociada de manera lógica a los datos, utilizada por un signatario para indicar su aceptación del contenido de esos datos y que cumple con los siguientes requisitos: (a) estar vinculada únicamente al signatario; (b) permitir identificar al signatario; (c) haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control; y (d) estar vinculada a los datos a los que se relaciona de modo tal que se detecte cualquier modificación ulterior de esos datos". "3. 'Dispositivo de creación de firma', los datos únicos, tales como códigos o claves criptográficas privadas, o un dispositivo físico configurado específicamente, que el signatario utiliza para crear la firma electrónica [digital]". "4. 'Dispositivo de verificación de firma', los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico configurado específicamente, utilizado para verificar la firma electrónica [digital]".

La administración de estas claves se realiza mediante autoridades certificantes o certificadores de clave pública. Al respecto, el artículo 7° del Anteproyecto de Ley de Firma Digital de 1999 prevé

que el certificado de clave pública debe contener, entre otros, los siguientes datos: nombre de su titular; tipo y número de su documento; clave pública del titular, con identificación del algoritmo utilizado; período de vigencia del certificado; firma digital del certificador de clave pública que emite el certificado, con identificación de los algoritmos utilizados; etcétera."

b) Características de la Firma Digital

[LARGAESPADA RODRIGUEZ][2]

"La Firma Digital inserta sobre un documento electrónico, le confiere a este las siguientes presunciones iuris tantum:

1-Autoría: se presume salvo prueba en contrario; que toda Firma Digital pertenece al titular del certificado digital.

2- Integridad: si el resultado de un procedimiento de verificación de una Firma Digital es auténtico, se debe presumir salvo prueba en contrario que este documento no ha sido modificado desde el momento de su firma.

3-Atríbuibilidad: cuando un documento electrónico sea enviado y este contenga la Firma Digital del remitente, se presumirá, salvo prueba en contrario, que el documento proviene del remitente.

3-No repudiación o no rechazo en origen: implica que el emisor del mensaje no pueda negar en ningún caso que el mensaje ha sido enviado por él.

Por lo tanto, se puede afirmar con segundad, que la carga de la prueba recae sobre la persona que duda de la autenticidad o validez de la Firma Digital.

Con relación a la verificación de la firma, se debe comprobar que la firma se creó durante el Período Operacional de un Certificado Válido; además, que el mensaje no ha sido alterado.

Respecto al concepto del Período Operacional de un Certificado Válido, es importante mencionar que los certificados electrónicos tienen una vigencia determinada, por lo que éstos deben ser renovados en los períodos indicados por las respectivas Autoridades Certificantes.

Dos de las características principales de la Firma Digital son:

a- Que sólo puede ser generada por el poseedor de la clave privada; además, puede ser verificada por cualquier persona que conozca la llave pública del firmante,

b- La Firma Digital es dependiente del documento que se firmo con esta, por lo que no se podría reproducir por parte del receptor la firma digital para firmar otros documentos."

c) Firma electrónica frente a firma manuscrita; firma digital en particular en el comercio electrónico.

[MARTÍNEZ NADAL][3]

"En el comercio electrónico, el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas que pueden ser remplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica. Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

En este concepto amplio y tecnológicamente indefinido de firma [recogido en el art. 2, apartado 1, de la directiva comunitaria por la que se establece un marco comunitario para la firma electrónica y en el art. 2, apartado a) del Real Decreto-ley 14/1999, de 17 de septiembre, por el que se regula la firma electrónica en el Derecho español], tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (p. ej., la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje (exigencias éstas básicas que debe cumplir un mensaje firmado, sea o no electrónico). Tan es así que incluso podría dudarse de su condición de firma, por su nula o escasa utilidad.

Una clase particular de firma electrónica que podría ofrecer una mayor seguridad es la de las firmas digitales. Estas firmas digitales son tecnológicamente específicas, pues se crean usando un sistema de criptografía asimétrica o de clave pública (frente a las firmas electrónicas tecnológicamente indefinidas como hemos dicho, por cuanto comprenden cualquier método, incluido, pero no limitado, al de los sistemas de clave pública).

Estos criptosistemas de clave pública (basados en el uso de un par de claves asociadas: una clave privada, que se mantiene en secreto, y una clave pública, libremente accesible por cualquier persona) permiten:

— realizar firmas digitales, que pueden ser tanto o más útiles, válidas y eficaces en el comercio, y en el derecho, como la firma escrita sobre papel: aplicando la clave privada del emisor sobre el mensaje, y verificado el mismo por el destinatario con la clave pública de aquél, si el resultado es positivo, se tiene garantía de la autenticación e integridad del mensaje.

De forma que, como señalan distintas legislaciones e iniciativas legislativas en la materia (y también el art. 2 del borrador inicial de propuesta de directiva, aunque en la versión definitivamente aprobada esta definición ha desaparecido, por su tendencia cada vez más neutral desde el punto de vista tecnológico) «firma digital» es una firma electrónica que utiliza una técnica de criptografía asimétrica tal que una persona que disponga de la clave pública del firmante puede determinar si:

a) la transformación se realizó utilizando la clave privada del firmante que corresponde a la clave pública del firmante (esto es, autenticación); y

b) el mensaje de datos ha sido alterado (es decir, integridad)

— y enviar mensajes secretos a través de canales inseguros como Internet: utilizando la clave pública del destinatario, de conocimiento público, el remitente puede estar seguro de que sólo el destinatario, el tenedor de la clave privada, puede descifrar el mensaje (confidencialidad).

Por ello, las firmas basadas en la criptografía de clave pública son consideradas seguras por cuanto, como se verá a continuación con más detalle, permiten satisfacer, en principio, las exigencias de autoría e integridad necesarias para que el mensaje y su firma electrónica sean vinculantes para el firmante y exigibles ante los tribunales; e incluso es posible que determinados criptosistemas

de clave pública utilizados con función de firma digital puedan ser utilizados, si así se desea, para obtener confidencialidad.

Estas firmas digitales vendrían a ser la firmas electrónicas avanzadas definidas en el artículo 2, apartado 2 de la directiva comunitaria y el artículo 2, apartado b) del Real Decreto-ley español sobre firma electrónica. Sin embargo, la directiva comunitaria (y correlativamente el Real Decreto-ley español) regula la firma electrónica en general, y no sólo la firma digital en particular, en un intento de abarcar otras firmas electrónicas, basadas en técnicas distintas de la criptografía asimétrica (técnicas disponibles o en desarrollo que permitan cumplir algunas o todas las funciones características de las firmas manuscritas en un medio electrónico).”

Esta tendencia a la neutralidad tecnológica se ha acentuado a medida que se han ido sucediendo las distitas versiones de la directiva como pone de manifiesto el hecho de que la versión final defina única y exlusivamente la firma electrónica (ar. 2.1.), mientras e el primer borrador existía también una definición de firma digital, en el artículo 2.2; y del par de claves, pública y privada, en los artículos 2.4 y 2.5. únicamente al establecer el concepto de dato de creación de firma (definido, en el art. 2.4, como aquel dato único, como códigos o claves criptográficas privadas, usado por el firmante para crear una firma electrónica) y dato de verificación de firma (definido, en el art. 2.7, como aquel dato único, como códigos o claves criptográficas públicas usado para verificar una firma electrónica) existe una referencia a la criptografía asimétrica.”

d) Validez y reconocimiento de la firma digital en el Derecho Costarricense.

[QUIROS ROHRMOSER][4]

“Antes de que se promulgara la ley número 8454, "Ley de Certificados, firmas digitales y documentos eletrónicos, en octubre del 2005, existía un vacío legal en el ordenamiento jurídico costarricense respecto al tema en cuestión. Aunque este ley es bastante pequeña y quizás incompleta para abarcar la temática, al menos nos brinda un marco conceptual y reconoce

explícitamente los institutos de documento electrónico, firma digital o electrónica y certificados electrónicos.

El capitulo tercero de la referida ley trata el tema de la firma digital y la define en el artículo ocho como:

"Artículo 8.- Alcance del concepto. Entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico...".

Como se puede apreciar el artículo anteriormente citado, nos da

una definición legal de la firma digital, indicando asimismo sus dos funciones principales, la autoría del documento y su vinculación al documento que acompaña.

Para que la firma digital tenga utilidad, seguridad y funcionalidad, debe de tener un respaldo legal. El artículo 9 de la referida ley número 8454, le otorga el mismo valor y eficacia probatoria a la firma digital que a la firma manuscrita, toda vez que esta cumpla con los requisitos mínimos. De esta manera los usuarios de documentos electrónicos pueden estar seguros y tranquilos de que en una eventual disputa, la ley otorga el mismo valor legal a la firma digital que a la manuscrita.

Al artículo 10, último del capítulo que abarca la firma digital, establece la presunción de autoría y responsabilidad de los autores de los documentos electrónicos. Referido artículo establece que todo documento, mensaje o archivo electrónico asociado a una firma digital certificada se presumirá, de la autoría y responsabilidad del titular, salvo prueba en contrario, siempre y cuando se cumplan todas las formalidades legales requeridas para la validez.”

e) Iniciativas de la Unión Europea

[SARRA][5]

"Los lineamientos generales en torno de los cuales se enmarcan los proyectos normativos sobre firma digital, encriptación y promoción del comercio electrónico, dentro de la Unión Europea, están contenidos en diversas directivas, resoluciones y comunicaciones del Parlamento y Consejo europeos.

1) Resolución del Parlamento Europeo de 1996. El 19 de septiembre de 1996, el Parlamento Europeo, por res. A4-244/96, solicitó a la Comisión de Iniciativa Europea sobre Comercio Electrónico la preparación de lincamientos concernientes a la seguridad de la información, la confidencialidad, la firma digital y la protección de la privacidad.

Posteriormente, el 12 de abril de 1997, se elevó un reporte por medio del cual se creó un marco político coherente de fomento del comercio electrónico dentro de la Unión Europea, con el objeto de posibilitar futuras negociaciones que permitan el consenso internacional para una postura común al respecto. Los propósitos fundamentales de esta iniciativa son los que se enumeran a continuación.

a) Fomentar el desarrollo de la tecnología y la infraestructura necesarias para garantizar la competitividad europea en el comercio electrónico.

b) Aprovechar las posibilidades del mercado interno y garantizar un marco regulador coherente en Europa y en los mercados mundiales.

c) Fomentar un entorno empresarial favorable al comercio electrónico mediante la promoción del dominio de los conocimientos necesarios y la sensibilización de los consumidores y de la industria con respecto a las oportunidades que se les ofrecen.

d) Buscar consenso internacional a partir de una posición común europea para garantizar una efectiva participación en las iniciativas internacionales de cooperación y negociación.

2) Resolución del Consejo de Ministros de la Unión Europea. El 21 de noviembre de 1996, el Consejo de Ministros adoptó una serie de medidas para asegurar la integridad y autenticación de instrumentos transmitidos digitalmente, mediante res. 967 C376/01.

3) Comunicación del Comité Económico y Social y del Comité de las Regiones al Parlamento Europeo y al Consejo Europeo. En abril de 1997, en su comunicado sobre comercio electrónico COM (97) 157, la Comisión de Iniciativa Europea sobre Comercio Electrónico anunció su intención de elaborar una política encaminada a garantizar la libre circulación de las tecnologías y los productos de encriptación e instó al desarrollo de un marco político al efecto. Para cumplir con los mencionados objetivos, ha establecido pautas

generales sobre la regulación de la criptografía en orden a fomentar la utilización de la firma y la moneda digitales, pautas que se enumeran a continuación.

a) Establecer un marco jurídico-tecnológico para la firma digital dentro de la Unión Europea.

b) Asegurar el funcionamiento del mercado interno para los productos y servicios sobre criptografía (así como productos y servicios que contengan técnicas de criptografía), al tiempo de respetar la seguridad pública y contribuir a un área de seguridad homogénea en la Unión Europea, tal como había sido establecido por el Consejo Europeo de Amsterdam (Conclusiones sobre libertad, seguridad y justicia, 16 y 17 de junio de 1997).

c) Estimular la industria europea de servicios y productos de criptografía.

d) Señalar los interrogantes internacionales surgidos como consecuencia de la naturaleza global de Internet y otras redes digitales. En particular, tender a la remoción de barreras al comercio de servicios y productos de criptografía y a la obtención, en tanto sea posible, de comunicaciones seguras "punto a punto" a escala global.

e) Proveer las bases para la integración de la criptografía dentro de un marco de otras políticas europeas, como por ejemplo la de protección de la privacidad, la de protección del consumidor, la atinente a derechos de propiedad intelectual, etcétera.

f) Estimular y permitir que usuarios de todos los sectores económicos se beneficien con las oportunidades de la sociedad de la información, que sólo puede ser completamente explotada o aprovechada si se basa en un marco de seguridad y confianza.

El objetivo final de esta iniciativa es la promoción del comercio electrónico europeo, al que consideran con amplias proyecciones debido a que tendrá un importante impacto en la competitividad de Europa en los mercados mundiales. La iniciativa crea un marco político adecuado para posteriores emprendimientos globales de la Unión Europea y tiene por objeto establecer una postura común de sus países integrantes, a fin de conseguir un consenso mundial mediante negociaciones internacionales.

4) Conferencia Ministerial Europea. En su declaración de julio de 1997 de la Conferencia que tuvo lugar en Bonn, la Unión Europea enfatizó sobre la necesidad de elaborar un marco legal y técnico para la firma digital dentro del ámbito europeo. Asimismo, resaltó la importancia de un estudio respecto de la factibilidad de la utilización de tecnologías de encriptación fuerte para el

comercio electrónico.

5) Audiencia de la Unión Europea sobre firma digital y encriptación. Esta audiencia fue realizada en Copenhague el 23 y 24 de abril de 1998 y tuvo como objetivo la exploración del uso y desarrollo de la firma digital y la encriptación. Si bien la temática desarrollada fue similar a la tratada en otras oportunidades, este encuentro tuvo la particularidad de que, además de participar en él los países miembros de la Unión Europea, estuvieron presentes representantes de Australia, Canadá, Estados Unidos de América, Japón, Noruega y Suiza.

6) Propuesta para una directiva del Parlamento y Consejo europeos para un marco común para la firma digital. La propuesta COM (1998) 297 final, del 13 de mayo de 1998, fue redactada acorde con las recomendaciones de la dirección general XIII de la Comisión Europea que, a principios de 1998, había formulado el Anteproyecto de Directiva de un Marco para los Servicios de Certificación Electrónica (el que, el 2 de abril de 1998, obtuvo la aprobación por parte de todos los Estados miembros, aunque con alguna preocupación para el reconocimiento legal de la firma digital desde el derecho comunitario- puesto que los sistemas jurídicos de los distintos países europeos diferían considerablemente).

7) Resolución del Parlamento Europeo de 1998. En la res. COM (98) 297 C4-0376/98, 98/0191 (COD) del Parlamento Europeo está contenida la opinión de éste respecto de la propuesta para la directiva mencionada en el apartado anterior. Esta resolución fue publicada en el Diario C 104 del 14 de abril de 1999."

f) Firmas Digitales y Autenticación de Evidencia Electrónica

[TORRES GONZALEZ][6]

Introducción

“En los últimos años, hemos visto un crecimiento vertiginoso en la necesidad de programados (“software”) en todas las etapas de nuestras vidas. Las computadoras dejaron de ser una herramienta

opcional y pasaron a ser una necesidad, muchas veces impuesta, para el desarrollo de nuestras tareas. Más aún, no simplemente estamos aumentando la cantidad de información que guardamos en estos sistemas sino que la misma cada vez es más importante y necesaria en nuestro diario vivir por lo que se hace necesario asegurarnos que la misma se mantenga íntegra, segura y accesible.

La evidencia electrónica incluye todo aquello que sea susceptible de estar en medios electrónicos. Esto puede ser desde una grabación de video, una conversación telefónica, un documento de computadora, entre otros. Para propósitos de este trabajo, nos referiremos a la evidencia electrónica como toda aquella información que puede ser manipulada en una computadora y que sea susceptible de llegar en algún momento al tribunal.

Como discutiremos a continuación, el descubrimiento de evidencia electrónica presenta unos problemas particulares debido, principalmente, a que este tipo de evidencia puede ser fácilmente duplicada y manipulada ocasionando que la autenticación de la misma se torne más difícil en comparación con la evidencia no electrónica.

Este trabajo tiene como propósito demostrar que es necesario utilizar un estándar claro de firmas electrónicas para poder facilitar la autenticación de evidencia electrónica en los tribunales. Más aún, si estamos intentando regular para que los países se unan en un comercio a través del Internet y para facilitar las transacciones electrónicas internacionalmente, debemos crear un estándar mundial a través de tratados para que se usen los mismos sistemas de firmas electrónicas a través de la mayor parte del mundo.

II. Autenticación de Evidencia

La autenticación de evidencia significa establecer que lo que el proponente sostiene que la evidencia es, efectivamente lo es. Esto es para propósitos de cumplir con el requisito de que toda la evidencia tiene que ser pertinente para un caso en particular. Una evidencia es pertinente si tiende a “hacer la existencia de un hecho más probable o menos probable de lo que sería sin tal evidencia; dicho hecho debe a su vez, referirse a una cuestión en controversia o a la credibilidad de algún testigo o declarante”.

[v] No podemos hablar entonces de pertinencia si no tenemos claro que el objeto, material o cualquier otra evidencia que traemos a juicio se trata, en efecto, de lo que decimos que es.[vi] Pero no toda evidencia auténtica es pertinente, sino que éste es un elemento dentro de la pertinencia, por esto es que hablamos de pertinencia condicionada (a otros elementos).

Las reglas de evidencia, tanto federal como local nos presentan unas guías a la hora de autenticar la evidencia. Estas guías no son taxativas, sino que son unos ejemplos que no pueden ser interpretados como limitación a las maneras de autenticación. Entre los ejemplos que nos proponen se encuentran:

* Testimonio de Testigo de Conocimiento
* Comparación Pericial o por Juzgador
* Prueba circunstancial
* Proceso o Sistema
* Admisión de Parte
* Disposición de Ley

Como hicimos notar, las reglas de evidencia no nos crean unas pautas obligatorias a la hora de la autenticación y esto nos permite crear nuevos métodos a la hora de enfrentarnos con evidencia que no ha sido tomada en consideración hasta el momento.

La cadena de custodia es otro método de autenticación, que aunque no está contenido en las Reglas de Evidencia de Puerto Rico, ha sido reconocido por nuestra jurisprudencia. Nuestro Tribunal ha ido más lejos, y en Pueblo v. Carrasquillo, plantean situaciones donde no simplemente se puede usar como método de autenticación sino que el acusado tiene el derecho a exigirlo. Ahora bien, este método se utiliza para evidencia demostrativa que no es susceptible de ser identificada por su apariencia externa ni susceptible de ser marcada. Cuando la evidencia contiene características distintivas que la hacen fácilmente identificable, no es necesario establecer la cadena de custodia; tampoco lo es si se trata de evidencia debidamente marcada.

Este método de autenticación consiste en demostrar que no hubo ninguna alteración a la evidencia desde el momento en que la misma

se hizo relevante hasta el momento en que se trajo a juicio. La cadena está formada de eslabones que han interactuado de una forma u otra con la evidencia y para cada uno de ellos, se debe incluir el momento de la custodia, de quién se recibió la evidencia y a quién se le pasó, y las medidas tomadas para asegurar la integridad de la evidencia y evitar que se intervenga con ella o se altere.

Por la fácil manipulación de la evidencia que se encuentra en medios electrónicos, ésta también está sujeta a que se pruebe cada uno de los eslabones de la cadena de custodia para que la misma sea admisible en el juicio. Para asegurarnos de que la evidencia electrónica no ha sido alterada podemos ver, entre otras cosas, las políticas sobre el almacenamiento y las restricciones de acceso, utilizar dispositivos tecnológicos para limitar su acceso o utilizar algún tipo de codificación que indique cuando y por quién el documento ha sido accedido o si el mismo ha sido alterado. Veremos más adelante algunos de los aspectos de la evidencia electrónica que ha causado problemas en los tribunales.

Existen ciertas instancias donde las Reglas de Evidencia de Puerto Rico nos permiten presentar cierta evidencia sin que se requiera "evidencia extrínseca como condición previa a la admisibilidad". Esto por que ciertos tipos de documentos gozan de cierta confianza y se permite que se prueben a si mismos. La evidencia es la siguiente:

* Documentos Reconocidos
* Documentos públicos bajo sello oficial
* Documentos públicos suscritos por funcionarios públicos
* Documentos públicos extranjeros
* Copias certificadas de récords y documentos públicos
* Publicaciones oficiales
* Periódicos o Revistas
* Etiquetas comerciales

Una vez probamos que cierta evidencia cae dentro de uno de los renglones anteriores, es el oponente y no el proponente el que debe presentar evidencia extrínseca, en caso de que así lo desee, demostrando que la evidencia no es auténtica.

III. Problemas en la Autenticación de Evidencia Electrónica

La autenticación es una de las partes más retantes a la hora de trabajar con la evidencia electrónica.[xxiv] La información en medios electrónicos es fácil de ser manipulada y los tribunales son muy cuidadosos a la hora de tomarla en consideración y darle confiabilidad.[xxv] El tribunal se expresó en el caso de St. Clair v. Johnny's Oyster & Shrimp, Inc.,[xxvi] donde nos dicen:

"There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No Web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation... For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed. R. Evid. 807"

El e-mail es un ejemplo de evidencia electrónica. Este es un instrumento que ha cambiado de una manera asombrosa la forma en la que nos comunicamos. Para el año 2007 se espera que se estén enviando más de 2.7 trillones de e-mails. Con estos datos, podemos tener la certeza de que esta documentación electrónica es y va a seguir siendo cada día con más frecuencia, fuente de debate en los tribunales. Los e-mails, al igual que el resto de la evidencia electrónica (y no electrónica), tienen que ser autenticados para poder ser admisibles en los tribunales, pero estos, por la frecuencia en que son usados y por la facilidad con la que pueden ser manipulados, dificultan aún más el decir con certeza, quién los envió y si los mismos se mantienen íntegros desde el día que fueron enviados.[xxviii] En la actualidad, para autenticar comunicaciones electrónicas normalmente utilizamos el contenido o circunstancias extrínsecas a la comunicación.

La cadena de custodia es otro problema más a la hora de autenticar la evidencia electrónica. Aunque, como dije anteriormente, los tribunales son bastante cuidadosos a la hora de aceptar la evidencia en medios electrónicos, en algunos casos han permitido evidencia propensa a ser alterada aunque no se haya probado toda la cadena de custodia por la complejidad que tiene probar lo

contrario, que en efecto, no fue alterada. Esto realmente es un problema, pues tenemos la preocupación de que se pueda fabricar evidencia en contra de algún acusado y los tribunales, al no tener las herramientas ni la preparación para probar lo contrario, puedan estar cometiendo alguna injusticia en contra de éste.

Las páginas de Internet también son fuente de debate en los tribunales por la cantidad de información que las mismas contienen y la facilidad con la que se pueden manipular. Para autenticarlas los tratadistas recomiendan 3 pasos:

1. Tenemos que demostrar, que el documento impreso que traemos al tribunal representa una copia fiel y exacta de lo que mostraba nuestra computadora cuando estábamos viendo la página de Internet.

2. Tenemos que demostrar que lo que estábamos viendo en nuestra pantalla, en efecto, era una copia fiel y exacta de lo que realmente estaba en el servidor.

3. Cuando traemos esa prueba para probar que lo que se dice es cierto, puede levantar problemas de prueba de referencia.

Reglas de Evidencia Propuestas para Evidencia Electrónica

En Puerto Rico, el Comité Asesor Permanente de las Reglas de Evidencia de Puerto Rico se encuentra evaluando las reglas de evidencia para atender algunos de los problemas con los que se están enfrentando los tribunales, y, entre las reglas propuestas, las que atienden los asuntos de evidencia en medios electrónicos son las siguientes:

* Récord Electrónico

o Un récord electrónico podrá autenticarse mediante evidencia de la integridad del sistema en el cual o por el cual los datos fueron grabados o almacenados. La integridad del sistema se demuestra a través de evidencia que sustente la determinación de que en todo momento pertinente el sistema de computadoras o dispositivo similar estaba operando correctamente o en caso contrario, el hecho de que su no operación correcta no afectó la integridad del récord electrónico.

* Correo Electrónico

o Un correo electrónico podrá autenticarse mediante evidencia de la integridad del sistema en el cual o por el cual fue creado, enviado o recibido.

* Se presumirá la integridad del récord si:

o (1) se establece mediante declaración jurada que fue grabado o almacenado por una parte adversa a la que lo propone, o

o (2) se establece mediante declaración jurada que fue grabado o almacenado en el curso usual y ordinario de negocios por una persona que no es parte en los procedimientos y quien no lo ha grabado o almacenado bajo el control de la que lo propone.

Aunque estas reglas propuestas atienden una parte de la problemática existente, es necesario que las mismas abarquen todo tipo de evidencia electrónica y que atiendan las diversas situaciones que pueden ocurrir con esta evidencia para asegurar su autenticidad e integridad.

IV. Firmas Digitales

¿Que es una firma digital?

En términos generales, una firma digital es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La tecnología para producir este resultado es lo que se conoce como cifrado asimétrico o cifrado de llave pública (Public Key Encryption). En términos más específicos, para generar una firma digital, necesitamos:

1. Un código de autenticación del mensaje (Message Autentication Code o MAC). Esto es una serie de dígitos derivados del propio mensaje, para asegurar su integridad.

2. Un algoritmo matemático, para producir un resultado ilegible de la combinación entre MAC y la llave privada (explicada a continuación), excepto con el uso la llave pública que le pertenece al mismo usuario. A esto le llamamos la Firma Digital.

3. Dos llaves específicas para un usuario, una privada (que va a mantener solamente en su posesión) y una pública (que la va a compartir con las demás personas). Cada llave se trata de una serie de dígitos y letras que son específicas para ese usuario. Las llaves se miden por bits y cuánto más alto sea este número, más segura es la llave.

Ahora bien, no estamos hablando de encriptación de documentos para que no sean visibles por nadie. Lo que estamos haciendo aquí es adjuntar al documento una serie de información que sale como resultado de utilizar el algoritmo matemático, junto con la llave privada de forma que, teniendo la llave pública de esa persona, podamos certificar que él produjo esa firma y que el documento está inalterado.

El resumen de todo lo anterior significa que, aplicando el algoritmo matemático se produce una mezcla entre la información electrónica y la llave privada a la que llamamos Firma Digital. Esa Firma Digital es un resultado único para esos dos elementos. Ahora bien, esa Firma Digital junto con la llave pública produce el mismo documento original.

El funcionamiento del algoritmo para producir las llaves privadas y públicas, al igual que el algoritmo matemático para el cifrado exceden el alcance de este artículo, pero voy a discutir un poco de cuan seguro es este sistema. No hay forma matemática de crear la llave privada, ni con la llave pública ni con la firma digital. Pero existe un método que se conoce como el ataque de fuerza bruta (Brute Force Attack). Para esto, lo que se hace es probar cada una de las alternativas, usando computadoras potentes, para intentar recrear la llave privada. Uno por uno, se coge el mensaje y una llave al azar y se prueba a ver si usando el algoritmo matemático se genera la misma Firma Digital que produjo la persona que firmó. Si lo consigo, ya tengo la llave privada y podría firmar documentos haciéndome pasar por la persona a la cual pertenece. La realidad es que este método es prácticamente imposible de realizar con éxito. Una llave normal (o mas bajo de lo normal se podría decir) cuenta con 128 bits, lo que significa que hay 2128 posibles llaves que tendría que tratar. Una computadora que pudiera verificar un billón de billones (1018) llaves por segundo, tardaría 10,790,283,070,806 años[xliv] en tratarlas todas.

Firmas Digitales v.s Firmas Electrónicas

Las firmas electrónicas se tratan de un concepto más amplio. Nos referimos a un "conjunto de datos, en forma electrónica, anejados a otros datos electrónicos o asociados funcionalmente a ellos con la intención de firmarlo". La firma electrónica puede ser un nombre al final de un e-mail o documento, un "acepto" al final de la contratación cuando compra un artículo por Internet, un número de identificación personal para obtener dinero de un cajero automático, una representación digital de la firma a manuscrito como la que utilizamos cuando firmamos para la tarjeta de crédito, una firma digital, en fin, cualquier dato, puesto de forma electrónica, que tenga la intención de firmar un documento. Cuando hablamos entonces de una firma electrónica, no hablamos de una tecnología en específico, sino de una intención de, por medio de un dato electrónico, firmar un documento.

Podríamos decir, entonces, que una Firma Digital, es un tipo Firma Electrónica que consiste de un cifrado asimétrico que nos permite, además de probar la autoría del documento, asegurarnos de la integridad del mismo. Por esta razón es que también se podría decir que supera la firma a manuscrito, pues ésta no asegura que el documento no ha sido alterado desde que ha sido firmado.

Legislación Vigente sobre Firmas Electrónicas y Digitales

Actualmente, en el ámbito de Firmas Electrónicas, Puerto Rico cuenta con la Ley de Firmas Electrónicas, que derogó la Ley de Firmas Digitales que existía anteriormente. Esto surgió a raíz de la aprobación federal del Electronic Signatures in Global and National Commerce Act (E-Sign) la cual no permite que se favorezca ningún tipo de tecnología sobre otra. Con esto, Puerto Rico se separó de la vertiente civilista de adoptar la Firma Digital sobre cualquier otro método de firma electrónica y se acercó más a la vertiente del "common law" donde probar la forma y el peso de la evidencia es más importante que el tipo de firma electrónica que se utilizó.

Este movimiento de Puerto Rico al adoptar una ley de Firmas Electrónicas que sea tecnológicamente neutral responde a que E-Sign ocupa el campo y no permite que ningún estado tenga ninguna ley que favorezca un método sobre otro. Al igual que Puerto Rico,

los demás estados de la unión aprobaron legislaciones que cumplieran con ese requisito.

Aunque nuestra ley se modificó para atemperarla con E-Sign federal, añadió, como parte de los requisitos para ser una firma electrónica válida y a su vez tener el mismo efecto legal que una firma a puño y letra, que dicha firma asegure la integridad tanto de la firma como del documento que está firmando. Además, nuestra ley de Firmas Electrónicas, a diferencia de E-Sign, crea unas presunciones a la hora de utilizar firmas electrónicas:

* Existe una presunción controvertible de que el documento no ha sido modificado desde el momento de su firma, si es posible utilizar un dispositivo de verificación de la firma electrónica y del contenido de un documento electrónico que permita corroborar con éxito la firma y el contenido del mismo.

* Existe una presunción controvertible de que la firma electrónica pertenece al signatario titular del certificado de firma electrónica que contiene los datos de verificación de firma correspondientes.

* Existe una presunción controvertible de que la firma electrónica fue añadida por el signatario a un documento electrónico con la intención de firmarlo.

* Existe una presunción controvertible de que la información contenida en un certificado de firma electrónica vigente es correcta.

Estas presunciones, heredadas de la ley anterior de Firmas Digitales, además de lo dicho anteriormente, nos hacen pensar que en realidad no se le está dando el mismo peso a cualquier firma electrónica sino que se favorece una que asegure la integridad del documento como lo sería la Firma Digital lo cual iría en contra de lo que establece E-Sign en el sentido de no darle mayor peso a una tecnología que a otra.

El movimiento internacional es aceptar todas las firmas electrónicas pero reconocer la Firma Digital (o aquella que asegure el contenido del documento) para propósitos de autenticar los documentos. Lo que significa esto es que no se le va a negar validez legal a una firma electrónica sin importar el método que se utilice, pero, si la misma va a ser usada con el propósito de asegurar la integridad del documento, tiene que usarse una firma electrónica que así lo permita (por ejemplo, una firma digital).

V. Firmas Digitales y Autenticación de Evidencia Electrónica

El uso de Firmas Digitales en la autenticación de evidencia electrónica es evidente. Nuestra propia ley, como vimos en la sección anterior, establece presunciones que harían más fácil la presentación de evidencia en nuestros tribunales. Estas presunciones obedecen a que, utilizando este método, se asegura tanto la integridad como la autoría de cualquier dato en medios electrónicos de forma que un tribunal puede entender, prima facie, que se trata de unos datos verdaderos. El uso, sin embargo, que se le está dando a esta tecnología no es muy amplio. Los tribunales, como vimos en las secciones anteriores, siguen enfrentándose con el dilema de autenticación haciendo de estos procesos unos extremadamente onerosos.

Firmas Digitales y Autoría

Como vimos, las firmas digitales, nos aseguran, por definición, la identificación del firmante, esto por que la llave privada se mantiene únicamente en su posesión y la ley crea una presunción de que eso es así. El signatario, a su vez, tiene la responsabilidad de mantener su llave privada en secreto y no compartirla con terceros y de no hacerlo podría responder por su negligencia.

Para asegurarnos de que la Firma en realidad pertenece a una persona en particular, descansamos en un tercer ente, conocido como una Autoridad Certificadora (CA por sus siglas en inglés) que así lo certifica. Esta entidad se encarga de mantener un registro de Firmas Digitales conocido como “Public Key Infrastructure” donde mantiene una relación entre las firmas digitales y la identidad de los firmantes. A esta relación la llamamos certificado. Estos certificados se tienen que mantener vigentes y el CA tiene que asegurarse de que, en caso de que alguna llave privada haya sido comprometida (que haya caído en manos de otras personas además del firmante) el certificado sea revocado. De esta manera nos aseguramos de que las personas que vayan a verificar las Firmas Digitales sepan desde que fecha el documento pudo haber sido firmado por otra persona que no haya sido la que aparece en el certificado. A su vez, los CA tienen que certificarse con otro CA, esto por que cada firma digital que ellos emiten tiene que estar a su vez firmada por ellos mismos y

esta firma tener su propio certificado. De esa manera se crea una estructura de certificados y ciertos tratadistas entienden que debe ser el gobierno el CA de última instancia.

Podemos entonces concluir que, teniendo un certificado válido, la firma digital de cierta información en medios electrónicos fue hecha por la persona indicada en el certificado. Además, como vimos, la complejidad para poder adivinar la llave privada de alguien es prácticamente imposible. Estas razones son las que hacen que las Firmas Digitales avaladas por un certificado válido se consideren como "Non – repudiable". Este término se refiere a que una vez se pruebe la identidad de la persona en el certificado y que la firma pertenece a ese certificado, la persona no puede decir que eso no fue firmado por él.

Firmas Digitales e Integridad

Por integridad nos referimos a que la información electrónica no ha sido alterada (se mantiene íntegra) desde el momento en que se firmó hasta el momento en que se trae al tribunal. Cualquier alteración, sea o no sustancial, cambiaría la evidencia y afectaría su autenticación, pues en efecto, no se trataría de lo que proponemos que es.

Como parte del algoritmo matemático para crear la Firma Digital, se utiliza lo que se conoce como el MAC o el Código de Autenticación del Mensaje.[lxxiii] Este código es único para cada mensaje y cualquier alteración al mensaje, produciría un código distinto. Este código se mezcla con la llave privada a través del algoritmo y nos produce la firma. Esta firma, es entonces verificada con la llave pública (o certificado) y nos da, con toda certeza, no simplemente el autor del documento, sino el MAC con el que podemos verificar que el mensaje no ha sido alterado.

La integridad del documento, o probar que el documento no ha sido modificado, se logra mediante el uso de una Firma Digital. No todas las firmas electrónicas proveen el mecanismo para verificar la integridad del documento, parte esencial en la autenticación de evidencia electrónica.

Los movimientos hacia crear una uniformidad en las firmas

electrónicas a nivel internacional incluyen dentro de sus definiciones que, para ser considerada una firma electrónica válida, debe hacer detectable cualquier alteración del documento posterior a su firma cuando esta sea una de sus finalidades. Más aún, como vimos, la legislación vigente en Puerto Rico, aunque quiere darle cabida a cualquier firma electrónica, mantienen el requisito de poder detectar un cambio dentro del mensaje que se está firmando para hacer válida ciertas presunciones.

Debemos recordar que toda la información susceptible a estar en medios electrónicos puede ser firmada para garantizar su integridad. Normalmente pensamos que se trata únicamente de documentos escritos, pues son los que solemos firmar cuando se trata de firmas a manuscrito. Pero en este caso, podemos firmar cualquier tipo de evidencia electrónica, como lo serían, fotos, películas, hojas de cálculo, imágenes de discos duros enteros, entre otras.

VI. Sugerencias

Como vimos, muchos de los problemas que tenemos a la hora de autenticar la evidencia electrónica[lxxvii] pueden ser resueltos mediante el uso de Firmas Digitales. Para esto, debemos adoptar unas normativas a la hora de trabajar con la evidencia electrónica:

* Debe implantarse una política de firmas digitales en los documentos o escritos puestos en Internet para ciertas industrias, por ejemplo, la prensa.

  o Esto, nos aseguraría la integridad y la fuente de dicho escrito.

* En ciertas industrias reguladas, debe implantarse el uso de firmas digitales en el envío de comunicaciones electrónicas tanto internas como externas:

  o Un ejemplo de esto serían los avisos del banco enviados por e-mail.

* Para toda incautación de evidencia por parte del estado, se debe dar una copia de la firma digital expedida por una agencia de

certificados al acusado. Esto evitaría los problemas que confrontamos con las cadenas de custodia ya que estaríamos marcando la evidencia.

* En ciertas industrias reguladas, la información almacenada deberá contener la firma de la persona que la creó.

o Un ejemplo de esto sería en la industria de salud, cada médico que escribe en un récord, debe poner su firma electrónica en lo que escribe asegurando así su autoría e integridad.

* En todo descubrimiento de prueba, todo documento electrónico debe ser firmado por la parte que provee la información y dicha firma debe ser presentada en la corte a la vez que se presenta el documento. Con esto, no necesitamos la cadena de custodia ya que tenemos la presunción de que los documentos no fueron modificados desde que fueron firmados.

* Bajo la Regla 79 de las Reglas de Evidencia de Puerto Rico, la cual establece la Autenticación Prima Facie, se debería enmendar para añadir:

o Documentos Electrónicos con Firmas Digitales expedidas por una Autoridad Certificadora.

* Debemos también crear un estándar en el que podamos confiar a la hora de validar una firma electrónica. No podemos crear unas presunciones en el vacío que sean neutrales a la tecnología. El estándar que propongo es uno de Firmas Digitales, tal y como se presenta en este artículo.

* Los programas que interactúen con las firmas electrónicas deben estar regulados también por el estado. De nada vale que se mantenga la llave privada de forma que nadie la pueda ver, si el programa que uso para firmar no tiene los estándares de seguridad adecuados.

VII. Conclusión

Una tecnología como la Firma Digital, con tanta aceptación y que está siendo usada por distintas industrias, permitiría una manera más rápida y sencilla de autenticar la evidencia electrónica en los tribunales.

Los tratadistas se han expresado sobre la dificultad que están enfrentando los tribunales al tratar de autenticar evidencia electrónica donde las legislaciones obligan a tratar todas las firmas electrónicas de la misma manera, sin poderle dar un mayor peso probatorio a una que a otra:

Critics of E-SIGN point out that the U.S. legislature failed to specify a technology that would provide legally adequate security and, thus, has pushed the responsibility of providing adequate legal certainty onto future lawmakers, judges, and juries. This uncertainty could create evidentiary presumption problems for judges and juries to solve. Under this scenario, judges and juries will likely have difficulty distinguishing between each new technology's level of security, even with the help of lawyers and experts, especially when the technology is in its infancy. The legislature is better suited to the task of gathering the sophisticated expertise required to create appropriate presumptions about the security of electronic signature technologies.

Las legislaciones vigentes en Estados Unidos y a su vez en Puerto Rico con respecto a las firmas electrónicas fallan al no establecer estándares firmes a la hora de proveer medidas para asegurar la autoría y la integridad de la información que se guarda en medios electrónicos. El propósito de su creación es permitir la participación de nuestro país en el comercio internacional, pero la falta de estándares está creando un caos en los tribunales. Las presunciones creadas por la ley no pueden trabajar en un vacío de una tecnología neutral sino que tienen que basarse en tecnologías seguras, que están funcionando y que proveen la alternativa de permitirnos autenticar la evidencia de una manera más certera.

Existen iniciativas por parte de la American Bar Association de crear estándares a la hora de autenticar evidencia electrónica y su enfoque mayor está siendo el uso de firmas digitales e infraestructuras de llaves públicas. También hay intentos de crear una nueva categoría de Cibernotarios cuyas funciones van a ser

similares a la de los notarios como los conocemos ahora pero a través del Internet. Dentro de las normativas que proponen para estos funcionarios se encuentra el registro de las llaves públicas.

Queda mucho por hacer y muchos retos contra los que enfrentarnos, pero los abogados tenemos que tener una participación activa a la hora de encontrar maneras que ayuden a la economía procesal y a la rapidez con la que se llevan a cabo los procedimientos judiciales. Asegurándonos en etapas tempranas de seguir ciertas normas que nos ayuden a mantener la integridad de los documentos en medios electrónicos y aplicando una tecnología en específico, facilitaríamos mucho la tarea de autenticación de evidencia en los tribunales. La jurisprudencia cada día reconoce una mayor responsabilidad en los abogados de ser diligentes a la hora de trabajar con la evidencia electrónica. Esta tecnología se encuentra disponible y se llama Fir.”

FUENTES CITADAS

1 BRIZZIO, Claudia. La informática en el nuevo derecho. Buenos Aires, Argentina. 1° edic. Editorial Abeledo-Perrot. 2000. pp 89-92.
2 LARGAESPADA RODRIGUEZ, Adriana. La seguridad jurídica del documento electrónico en el Derecho Positivo Costarricense. Tesis para optar por el grado de licenciatura en Derecho. Ciudad Universitaria Rodrigo Facio, U.C.R. pp 20047
3 MARTÍNEZ NADAL, Apol.lónia. Comercio electrónico, firma digital y autoridades de certificación. Madrid, España, 3° edic. Editorial Civitas. 2001. pp 41-44.
4 QUIROS ROHRMOSER, Manrique. La figura de la factura electrónica, su análisis en el Derecho comparado y la necesidad de su regulación en el ordenamiento jurídico costarricense. Tesis para optar por el grado de licenciatura en Derecho. Ciudad Universitaria Rodrigo Facio, U.C.R. 2007. 47-49.
5 SARRA, Andrea Viviana. Comercio electrónico y derecho. Buenos Aires, Argentina. 1° Edic. Editorial Astrea. 2001. pp 372-347.
6 Base de datos de la página ALFAREDI. [en línea]. Torres Gonzalez, Julio. Firmas Digitales y Autenticación de Evidencia Electrónica. Página visitada el 02-12-08. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=9897