FIRMA DIGITAL

CONSIDERACIONES JURÍDICAS

Mirna Lubet Valenzuela Rivera *

Informática Jurídica y Derecho Informático

A. Informática Jurídica:

Informática, es la automatización de la información. A fin de establecer una definición clara de Informática Jurídica, se exponen las siguientes: Para Enrique Pérez Luño citado por Mirna Valenzuela, la informática es la "Ciencia que estudia el tratamiento automático de la información".

Es la utilización de las computadoras en el ámbito jurídico.

Ciencia y conjunto de técnicas de tratamiento lógico y automático de la información jurídica. Para Fernando Jordán, es la utilización de los diferentes conceptos, categorías, métodos y técnicas propios de la informática en el ámbito jurídico.

La definición más amplia es la de Edgar Salazar Cano, quien la define como: Ciencia del tratamiento racional y

automático de la información de contenido jurídico. A su vez explica: Tratamiento racional: Porque pone de relieve los caracteres de análisis, método y clasificación como condiciones necesarias para que se pueda hablar de información propiamente dicha.

Tratamiento automático: Supone la actividad instrumental que se desarrolla mediante el uso de las máquinas o computadoras. A través de los programas se desarrollarán las diversas tareas de procesamiento automático de la información.

Y el contenido jurídico: La informática jurídica se ocupa del tratamiento y análisis de la información de contenido jurídico.

Clases de informática jurídica:

La informática jurídica se divide en tres subsistemas:

Documental o informática de documentación: Es la que almacena y clasifica los datos jurídicos para su

recuperación rápida y oportuna. Se subclasifica en legislativa, judicial o jurisprudencial, doctrinaria, bibliográfica y de documentos legales.

De gestión: Es la que se utiliza en el trámite diario de la gestión de trabajo de estudios jurídicos, notaría, tribunales, registros, legislatura. Entre sus principales usos están el control, planeación y toma de decisiones en la oficina jurídica. Se subclasifica en: registral, notarial, judicial, parlamentaria, de estudios jurídicos y operacionales.

La firma digital es una serie de caracteres - letras, números, signos - generados por un programa informático con el fin de que a través de ello podamos "firmar" un documento electrónico

Decisoria: Es la que propone y adopta soluciones para casos concretos que se le plantean, en base a criterios que previamente se le han provisto, se le compara con un silogismo.

B. Derecho informático:

Para la Abogada Argentina Bibiana Luz Clara, es: "Conjunto de

normas y principios que tienen por objeto, reglar, definir, interpretar y estudiar, los aspectos en que la tecnología informática se relaciona con las distintas instituciones jurídicas".

El Internet y los juristas

Internet es un sistema maestro de diversas redes de computación que posee 2 funciones básicas a saber:

Medio de comunicación: Internet ofrece una amplia gama de canales de enlace, entre ellos comunicación escrita, (el e-mail), la comunicación verbal (contacto por teléfono) y comunicación visual (teleconferencia en Internet).

Medio de información: En esta función Internet se puede comparar con una biblioteca a cuya sala de lectura se puede conectar desde cualquier

computadora que esté conectada al sistema. A diferencia de la biblioteca que sólo la autoridad puede introducir libros o documentos, el sistema de Internet permite que los usuarios agreguen información, lo que contribuye al mayor crecimiento de la información.

Características de Internet:

La estructura de Internet se caracteriza por su organización no jerárquica. Todas las computadoras y sistemas de redes enlazadas poseen la misma capacidad de acceso a la información y demás servicios. Es un sistema de autorregulación propio. Internet no cuenta con un órgano de control que regule su funcionamiento.

Nombre de dominio en Internet:

Un aspecto importante para los juristas es el sistema de domain-name (nombre de dominio) en Internet, el cual se utiliza en dos sentidos: En relación con las direcciones de servicios de información que pertenecen a Internet y por la otra se emplea para direcciones de e-mail. Los servicios de información a que se acceden por Internet tienen su propia dirección para requerir dicho servicio. A las secciones especiales de cada dirección se les denomina domains (dominio). La mayor parte de servicios informativos para los juristas se encuentran en Internet denominado World Wide Web (www), ejemplo: HYPERLINK "http://www.umg.edu.gt" www.umg.edu.gt

El nivel más elevado constituye el campo a que se encuentra subordinado el dominio. Los niveles más elevados que se asignan a las organizaciones inscritas en Estados Unidos son: **.com** organizaciones comerciales, **.edu** universidades y otras instituciones de enseñanza, **.gob** organizaciones estatales, **.net** sistema de la red y sistema de la administración de Internet, **.org** otras organizaciones diversas.

Para los servicios que se introdujeron fuera de Estados Unidos de América, se utilizan códigos que hacen alusión al país en que se llevó a cabo la introducción a Internet, entre otros: **gt**-Guatemala, **br**-Brasil, **es**-España, **fr**-Francia, **it**-Italia, **mx**-México, **us**-Estados Unidos.

Las direcciones de e-mail, por su parte, constan de las siguientes secciones:

Usuario@ servicio.dominio.nivel más elevado.dominio.país de introducción Ejemplos:

HYPERLINK "mailto:mvalenzuela@umg.edu.gt" mvalenzuela@umg.edu.gt

HYPERLINK "mailto:mvalenzuela@rgp.org.gt" mvalenzuela@rgp.org.gt

HYPERLINK "mailto:mirnavalen@hotmail.com" mirnavalen@hotmail.com

HYPERLINK "mailto:mirnavalen@gmail.com" mirnavalen@gmail.com

En primer lugar el nombre del usuario, que le asignó el prestador del servicio o él mismo seleccionó, luego se agrega el símbolo @ que en inglés significa "at" (en), después sigue el nombre del servidor, el dominio y el nivel más elevado y el país de introducción.

Riesgos y medidas de seguridad en Internet:

El jurista debe estar consciente que Internet se concibió y desarrolló con la idea de proporcionar un acceso fácil a la información y servir como medio de comunicación rápido y efectivo. En el logro de este objetivo fundamental, la seguridad se relegó a segundo plano. Por lo anterior los juristas deben tener en cuenta los riesgos de seguridad por el ejercicio de sus profesión, entre otros: Una persona que conoce bien el sistema le es posible interceptar la información enviada, leerla e incluso alterarla. Sería perjudicial para un Abogado y Notario por la obligación de conservar el secreto profesional; por ello abstenerse de transmitir por Internet información confidencial a menos que se tomen las medidas de seguridad como el encriptar, instalar firewalls u otros. Los virus que pueden infectar la información que conserva el jurista en su computadora. Podrá contratar programas antivirus.

Pérdida de información de sus clientes. Obtener copias periódicas de respaldo de la información, dentro y fuera del bufete.

Las claves y autenticación de acceso. Llevar control de las claves y asegurarse que no se trasladen sin consentimiento o bien utilizar dispositivos de huella digital o biométrica, para garantizarse la autenticación de quién accesa al sistema.

Uso de intranet. Una red interna evita el uso de Internet y los mencionados riesgos.

Usos de Internet para los juristas:

Entre los usos y beneficios que proporciona el Internet para los juristas están:

Internet como medio de comunicación: Uso del e-mail debido a que éste es un servicio de mensajería electrónica que funciona en la red Internet. Además el uso del e-mail ofrece muchas ventajas de comunicación.

Foros de discusión y grupos listserv: Es uno de los servicios de mayor utilidad para los juristas debido a la profundidad de los temas que se tratan. Los foros de discusión y los listserv surgen de la necesidad de intercambiar información entre personas que pertenecen a comunidades interesadas por un mismo tema de reflexión.

Acceso a fuentes de información: Internet brinda la posibilidad de consultar sentencias, fallos, legislación, artículos, noticias, etc. de interés jurídico. Ofrecer y contratar servicios para el bufete.

El Internet como objeto de estudio del derecho:

A su vez el Internet en su aplicación deriva situaciones y conductas que ameritan ser estudiadas por los juristas. En algunos países existen propuestas de legislación para regular el uso de Internet, los tribunales, autoridades que aplicaran dicha normativa, el derecho aplicable, la competencia internacional, etc.

Asimismo se hace necesario contar con jurisprudencia y bibliografía especializada para el estudio del Internet desde el ámbito jurídico. Los juristas cada día se enfrentarán a más problemas legales derivados del uso de Internet y derechos asociados.

Cibertribunales o justicia electrónica

De la aplicación de la firma digital, uso de Internet y demás tecnología asociada, se derivan consecuencias jurídicas que deben ser dilucidadas por un órgano jurisdiccional competente, especializado en temas tecnológicos e informáticos, que den solución a conflictos planteados ante el.

Para ello en algunos países se han instituido los llamados Cibertribunales, que son órganos jurisdiccionales que resuelven conflictos y controversias por el uso de Internet. Es un tribunal especializado en temas como comercio electrónico,

contratación electrónica, contratos informáticos, actos de competencia desleal en la red, teletrabajo, publicidad y marketing en Internet, protección de la intimidad, responsabilidad legal, Propiedad Intelectual (derecho de Autor, nombres de dominio en la red, etc.)

Por la agilidad que caracteriza a la sociedad y economía digital es necesario que los conflictos planteados ante estos tribunales sean resueltos de igual forma, para evitar daños irreparables o que se emita resolución cuando la situación ha perdido vigencia.

Para el óptimo funcionamiento de estos tribunales es menester la capacitación inicial y continua de los jueces y personal, tanto el ámbito jurídico como en el tecnológico.

En la determinación de la jurisdicción y competencia se presenta uno de los mayores problemas: Establecer en un caso concreto, la ley aplicable, lugar de juzgamiento, aportación de pruebas, ejecución de disposiciones contractuales, interpretación de contratos.

Comentario a la iniciativa de ley para el reconocimiento de las comunicaciones y firmas electrónicas de Guatemala

En la legislación vigente se requiere, para la validez, de actos o contratos, de la firma ológrafa o manuscrita, lo que imposibilita transacciones electrónicas y la mejora de los procesos de gestión pública. Asimismo obliga a continuar conservando documentos en soporte papel, almacenarlos en espacios físicos, que además de ser onerosos, dificultan la búsqueda y consulta de los mismos.

La iniciativa de ley propone un articulado que permitirá colocar a Guatemala, en el contexto internacional, competitivo en las transacciones electrónicas mejorará la situación económica y las relaciones comerciales internas e internacionales.

Se presentó al Congreso de la República de Guatemala, un anteproyecto de ley para la regulación del comercio electrónico. La iniciativa se denomina LEY PARA EL RECONOCIMIENTO DE LAS COMUNICACIONES Y FIRMAS ELECTRONICAS, que conoció el pleno del Congreso el 17 de agosto de 2006, como iniciativa 3515 y tiene como objetivo regular el comercio electrónico

De la aplicación de la firma digital, uso de Internet y demás tecnología asociada, se derivan consecuencias jurídicas que deben ser dilucidadas por un órganos jurisdiccional competente

de Guatemala.

La primera iniciativa de este tema se presentó al Congreso en enero de 2001, Ley de Promoción del Comercio Electrónico y Promoción de la Firma Digital en Guatemala, Iniciativa 2400.

Estas iniciativas de ley responden a la necesidad de regulación legal del comercio electrónico en Guatemala y resulta necesaria como marco legal para el mismo. Está ley beneficiará tanto al sector privado como al sector público, registros públicos, Superintendencia de Administración Tributaria, etc. La vigencia del DR-CAFTA presume un crecimiento del comercio por la vía electrónica y consecuentemente la presión de aprobación de la ley.

Regulación legal de relaciones informáticas

La mayoría de leyes actuales fueron concebidas sin prever relaciones informáticas dentro de la llamada sociedad de la información, pero el cambio es real y constante, el Derecho debe adaptarse; los legisladores deben promulgar leyes acordes a los cambios actuales y con visión de futuro.

El Derecho deberá estudiar en sus distintas ramas, temas, entre otros:

Derecho Civil y Mercantil: Firma digital en contratos, validez de la firma digital, desmaterialización de títulos, contratos informáticos, contratos electrónicos por y para la red, correo electrónico para la comunicación legal, sistemas de autenticación y acceso a los sistemas, autoridades de certificación o entes certificadores, marcas y patentes, instrumentos de pago electrónico.

Propiedad Intelectual: Plagios, derecho de autor o industriales, piratería informática.

Derecho Penal: Delito Informático, delito cibernético, tipificación de nuevos delitos por el uso de la red, "hackers", delitos por la red y mediante la red, persecución, condena y cumplimiento de penas, ubicar a los responsables.

Derecho Constitucional: La protección de los derechos humanos en la red. Agencias de protección de datos, derecho a la privacidad y a la intimidad. Aplicar recursos como el "Habeas Data". Derecho tributario y derecho procesal.

Derecho Laboral: En la necesidad de permitir el "teletrabajo" (Trabajo desde una computadora personal en el lugar que el trabajador elija, en su oficina, casa u otro, modifica la forma tradicional en cuanto al horario, desplazamiento, supervisión física, falta de identidad con el empleador, etc.) se crea una situación especial que amerita regulación específica.

Derecho Notarial y Registral: Notariado digital, protocolo notarial digital, firma notarial electrónica, firma digital, notarios o escribanos como entes certificadores, documento electrónico notarial, escritura pública digital, digitalización de documentos públicos, títulos electrónicos registrales.

Firma digital

La firma digital es una serie de caracteres - letras, números, signos - generados por un programa informático con el fin de que a través de ello podamos "firmar" un documento electrónico - un simple e-mail, un libro en formato digital, o una grabación sonora digital también son documentos electrónicos -, y podamos de esa forma acreditar la identidad del firmante.

Firma digital también se define como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) a un mensaje determinado, de cifrado asimétricos o de clave pública, y que equivale a la firma autógrafa para la identificación del autor del mensaje.

Con el uso del Internet se da la posibilidad de intercambiar entre personas distantes geográficamente mensajes de todo tipo, incluidos los mensajes contractuales; consecuentemente se presenta el problema de acreditar la autenticidad y la autoría de los mismos. Los mecanismos de firma electrónica, basados en los llamados certificados digitales, sirven para cifrar, esto es, poner en clave un documento, de modo y manera que si alguien lo intercepta o abre, no lo pueda entender. Por lo anterior un concepto importante en la firma digital es el de clave.

En el sistema de firma - llamado asimétrico - hay dos claves, una llamada pública (no es secreta) y otra denominada privada (es que la que hemos de conservar con el mayor celo sin mostrársela a nadie). En otro sistema de firma, llamado simétrico, sólo hay una clave, que es privada, y ha de ser guardada con la mayor de las diligencias y cuidados.

Digamos, que el uso de la criptografía - en ella se basa la firma electrónica - posee otras utilidades a través de la firma electrónica, como es comprobar la identidad del firmante, saber a qué hora exacta y en qué fecha firmó el documento; detectar posibles intentos de modificación del mismo no autorizados, y también poner en clave información confidencial. Desde el punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

Los mensajes con firma digital deben cumplir los requisitos siguientes:

1º.- Identidad, atribuir de forma indubitada un mensaje electrónico a una determinada persona como autora del mismo.

2º.- Integridad, es la certeza de que un mensaje recibido por B (receptor) es exactamente el mismo mensaje emitido por A (emisor), sin que haya sufrido alteración alguna durante el proceso de transmisión de A hacia B.

3º.- No repudiación o no rechazo en origen, que implica que el emisor del mensaje (A) no pueda negar en ningún caso que el mensaje ha sido enviado por él. Pues bien, la firma digital es un procedimiento técnico que basándose en técnicas criptográficas trata de dar respuesta a esa triple necesidad apuntada anteriormente, a fin de posibilitar el tráfico comercial electrónico.

4º. Confidencialidad, que no es un requisito esencial

de la firma digital sino accesorio de la misma. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

La criptografía como base de la firma digital:

Para claridad en la exposición, se presenta de la siguiente forma:

“La firma digital se basa en la utilización combinada de dos técnicas distintas, que son la criptografía asimétrica o de clave pública para cifrar mensajes y el uso de las llamadas funciones hash o funciones resumen.

La criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes. El diccionario de la Real Academia Española de la Lengua define la criptografía como “el arte de escribir con clave secreta o de forma enigmática”.

La criptografía ha venido siendo utilizada desde tiempo antiguo, fundamentalmente con fines militares. Tradicionalmente se ha hablado de dos tipos de sistemas criptográficos: a) Los simétricos o de clave privada y b) Los asimétricos o de clave pública.

a) Los sistemas criptográficos simétricos: son aquellos en los que dos personas (A y B), que van a intercambiarse mensajes entre sí, utilizan ambos la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje (A), lo cifra utilizando una determinada clave, y una vez cifrado, lo envía a B. Recibido el mensaje, B lo descifra utilizando la misma clave que usó A para cifrarlo. Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales inconvenientes del sistema simétrico son los siguientes:

- La necesidad de que A (emisor) y B (receptor) se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.

- La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Las dos dificultades apuntadas determinan que los sistemas de cifrado simétricos no sean aptos para ser utilizados en redes abiertas como Internet, en las que

confluyen una pluralidad indeterminada de personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

b) Los sistemas criptográficos asimétricos o de clave pública: se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes (privada y pública), de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

- Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes. La segunda clave, la pública, es o puede ser conocida por cualquiera.

- Ambas claves, privadas y públicas, sirven tanto para cifrar como para descifrar mensajes.

- A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni

obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, que es conocida por cualquier persona, se pudiese obtener la clave privada, el sistema carecería de seguridad dado que cualquier podría utilizar la clave privada atribuida a otra

persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

La utilización del par de claves (privada y pública) implica que A (emisor) cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía a B (receptor). B descifra el mensaje recibido utilizando la clave pública de A. Si el mensaje descifrado es legible e inteligible significa necesariamente que ese mensaje ha sido cifrado con la clave privada de A (es decir, que proviene de A) y que no ha sufrido ninguna alteración durante la transmisión de A hacia B, porque si hubiera sido alterado por un tercero, el mensaje descifrado por B con la clave pública de A no sería legible ni inteligible. Así se cumplen dos de los requisitos anteriormente apuntados, que son la integridad (certeza de que el mensaje no ha sido alterado) y no repudiación en origen (imposibilidad de que A niegue que el mensaje recibido por B ha sido cifrado por A con la clave privada de éste). El tercer requisito (identidad del emisor del mensaje) se obtiene mediante la utilización de los certificados digitales, que se analizan en otro apartado.

La mayoría de leyes actuales fueron concebidas sin prever relaciones informáticas dentro de la llamada sociedad de la información

Las funciones hash:

Junto a la criptografía asimétrica se utilizan en la firma digital las llamadas funciones hash o funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, hecho éste que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

Los sellos temporales:

En el proceso de intercambio de mensajes electrónicos es importante que, pueda conocerse y establecerse con certeza la fecha exacta en la que los mensajes han sido enviados, esto se obtiene mediante los llamados sellos temporales o "time stamping", que es aquella función atribuida generalmente a los Prestadores de Servicios de Certificación mediante la cual se fija la fecha de los mensajes electrónicos firmados digitalmente.

Certificados digitales:

La utilización del par de claves (privada y pública) para cifrar y descifrar los mensajes permite tener la certeza de que el mensaje que B recibe de A y que descifra con la clave pública de A, no ha sido alterado y proviene necesariamente de A.

Para lograr la identidad de A (emisor) es necesario la intervención de un tercero, que son los llamados Prestadores de Servicios de Certificación, cuya misión es la de emitir los llamados certificados digitales o certificados de clave pública.

Un certificado digital es un archivo electrónico que tiene un tamaño máximo de 2 Kilobytes y que contiene los datos de identificación personal de A (emisor de los mensajes), la clave pública de A y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta.

Los certificados digitales tienen una duración determinada, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

Por el certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal, y si sabemos que el

mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quién es la persona titular de esa clave privada.

El proceso de obtención de los elementos para firmar digitalmente los mensajes (par de claves y certificado digital)

es el siguiente: Solicitar personalmente o por medio de Internet, por la página web, a una empresa o entidad Prestadora de Servicios de Certificación el par de claves y el certificado digital correspondiente a las mismas.

El prestador de Servicios de Certificación comprobará la identidad del solicitante, a través del documento oficial de identificación, bien directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro). En caso se trate de representantes de entidades deberá adjuntar la documentación pertinente.

El prestador de Servicios de Certificación crea con los dispositivos técnicos adecuados, el par de claves pública y privada, y genera el certificado digital correspondiente a esas claves.

El prestador de Servicios de Certificación entrega una tarjeta similar a una tarjeta de crédito que tiene una banda magnética en la que están gravados tanto el par de claves como el certificado digital. El acceso al par de claves y a los certificados digitales gravados en la tarjeta está protegido mediante una clave como las que se utilizan en las tarjetas de crédito o en las tarjetas de cajero automático. En otras ocasiones, en lugar de la tarjeta el Prestador de Servicios de Certificación deja almacenado el certificado digital en su propia página Web, a fin de que el destinatario copie el archivo y lo instale en su computadora.

Con esa tarjeta magnética y un lector de bandas magnéticas adecuado conectado a la computadora, se podrá leer y utilizar la información gravada en la tarjeta para firmar digitalmente los mensajes electrónicos que se envíen a otras personas.

Firma electrónica notarial**Usos de la firma electrónica avanzada en el ámbito notarial:**

Los notarios podrán remitir documentos públicos notariales, comunicaciones, partes, declaraciones y autoliquidaciones tributarias, solicitudes o certificaciones vía electrónica a otro notario o registrador, a la administración pública u órganos jurisdiccionales. Asimismo podrán remitir copias simples electrónicas a las entidades y personas interesadas, cuando su identidad e interés legítimo le consten al notario.

El envío a particulares de documentos e información con el valor, efectos y requisitos legales, también es permitido.

Firma electrónica en el contexto internacional:

En cada país que se ha implementado el uso de la firma digital en el ámbito notarial, se han establecido las disposiciones legales que lo regulan, los mecanismos de aplicación, medidas de seguridad e infraestructura aplicable; varía en algunos aspectos, pero en general se trata de prestar un mejor servicio notarial con seguridad y certeza jurídica, aplicando la tecnología.

En España a partir de la promulgación de las Disposiciones Generales sobre la Incorporación al Notariado de las Nuevas Tecnologías, Real Decreto/Ley 14/1999, se emiten disposiciones para los notarios, tales como: Disponer de manera obligatoria de sistemas telemáticos para la emisión, transmisión, comunicación y recepción de información.

Dentro de los 9 meses siguientes a la vigencia de la Ley, los notarios deberán obtener los servicios de certificación de firma electrónica avanzada, y adquirir el dispositivo seguro de creación de firma. La firma electrónica notarial, entre los datos de verificación estarán los de identidad del titular, su condición de notario activo, su sede notarial.

El uso de la firma digital avanzada estará destinada exclusivamente a la suscripción de documentos públicos u oficiales propios de su oficio. No podrá utilizarse para asuntos personales o profesionales que no sean notariales.

La firma electrónica avanzada la obtendrá al tomar posesión de la notaría, se extinguirá con el cese de su función y se suspenderá conforme el ejercicio de su cargo como notario. Deberá tener vigente el certificado.

Los prestadores de servicios de certificación en ningún caso podrán almacenar ni copiar los datos de creación de firma.

Obligación de custodia personal y denuncia por pérdida u otro:

Los notarios estarán obligados a custodiar personalmente adoptando las medidas de seguridad adecuadas los datos de creación de firma electrónica que les correspondan. No podrán ceder su uso a ninguna otra persona en el supuesto. Deberán denunciar inmediatamente al colegio respectivo su pérdida, extravío o cualquier situación acaecimiento que pueda poner en peligro el secreto o la unidad del mecanismo para que lo comunique al prestador de servicio de certificado que hubiera expedido el certificado o a quien le hubiera sido transferido para que proceda inmediatamente a su suspensión o revocación.

La obligación de custodia establecida en amplios términos en que su incumplimiento por el notario constituye infracción disciplinaria muy grave. En el ámbito del Derecho notarial la firma digital no tiene el carácter de firma sino de sello.

En Guatemala, en el ámbito notarial se presentó al Congreso de la República, en el mes de septiembre de 2004, iniciativa de una NUEVA LEY DE NOTARIADO, en donde se incorpora el llamado Notariado Digital, Protocolo Notarial Digital, Documento Electrónico y se dispone que al contar con la infraestructura necesaria e idónea la Corte Suprema de Justicia de Guatemala, establecerá la normativa aplicable.

En el ámbito registral, el Registro General de la Propiedad, presentó al Congreso de la República, iniciativa para reformar el Código Civil en el sentido de autorizar la firma electrónica registral, para uso de los Registradores de la Propiedad.

Firma electrónica registral

La legislación vigente en Guatemala, establece la formalidad de incluir la firma del Registrador en los asientos como requisito para su validez, no obstante el volumen de los mismos ha requerido que la Registradora General de la Propiedad nombre varios Registradores Auxiliares para que entre otras funciones firmen los asientos.

En la exposición de motivos a las reformas del Código Civil, presentada por la Comisión Nacional Registral, se describe de manera clara y explícita la razón de dichas reformas, así: El Registro de Propiedad de la Zona Central ha implementado el proceso de modernización aplicando paulatinamente, en la mayor parte de sus operaciones, los avances de la tecnología electrónica, dentro del marco legal que le brindaba el segundo párrafo del artículo 1221 del Código Civil, que dice: "Queda facultado (el registrador) para innovar progresivamente el actual sistema, adoptando la microfilmación de los documentos, la computarización y teleproceso, de acuerdo con las posibilidades económicas del Registro".

**Los notarios estarán
obligados a custodiar
personalmente adoptando las
medidas de seguridad
adecuadas los datos de
creación de firma electrónica
que les correspondan**

Si bien esa norma permitió la implementación del proceso de modernización, actualmente se considera insuficiente para los programas, sistemas y nuevas

tecnologías que se han establecido en diversos servicios y operaciones registrales y también para las que se ha planificado incorporar en el futuro, como se hace ver al explicar la razón de ser de cada una de las reformas que se proponen en la iniciativa de ley. La Comisión Nacional Registral, creada por Acuerdo Gubernativo número 30-2005, del Presidente de la República tiene entre sus atribuciones la de promover y dirigir el proceso de modernización del Registro de la Propiedad, para lo cual cuenta con un porcentaje equivalente al 20% de los ingresos que en concepto de honorarios perciba el Registro. En diciembre del año pasado, dicha Comisión aprobó que se emprendiera la modernización del Segundo Registro de la Propiedad, con sede en la ciudad de Quetzaltenango, con lo que se beneficiará a la población de ocho departamentos del sur y occidente de la República. Este proceso ya está en marcha.

Por otra parte se ha estructurado y puesto en vigencia una política de descentralización. Están funcionando sedes regionales en Petén, Zacapa, Escuintla y Cobán, que estarán conectadas en línea con el Registro General y, cuando concluya su modernización, con el Segundo Registro. De esa cuenta, se ampliará para todos los usuarios la cobertura que ahora presta la Institución, puesto que podrán realizar sus gestiones sin necesidad de acudir a las sedes de los Registros.

En ese contexto, se ha considerado indispensable proponer al honorable Congreso de la República, que considere la conveniencia de introducir cambios

puntuales a cuatro artículos del Código Civil, para adecuarlos a los métodos tecnológicos que ya se están aplicando y se prevea de una vez algunas otras que se implementarán en el futuro. Algo similar hizo en su oportunidad ese Organismo cuando se reformaron las normas que regulaban en dicho cuerpo legal las operaciones del Registro Civil, con la finalidad de eficientar sus operaciones. Con ese objetivo, las reformas que contiene la iniciativa de ley, son las siguientes: Modificar el inciso 8º del artículo 1131, reformado a su vez por el artículo 5º del Decreto Ley 124-85, en el sentido de que además de la firma autógrafa del registrador que autorice la operación, podrá emplearse en su sustitución firma digital, electrónica, digitalizada o impresa por cualquier medio electrónico del mismo funcionario. La reforma

tiene como propósito que estas últimas formas de firma, universalmente reconocidas, dos de las cuales ya se utilizan en el Registro General, produzcan los mismos efectos jurídicos que la firma autógrafa, que era el medio tradicional de autorizar las inscripciones. Como cualquier otra institución que recurra a esos sistemas tecnológicos, se prevé que el Registro, con la asesoría profesional y técnica correspondiente, que ya está contratada, tome todas las medidas pertinentes para garantizar mediante controles biométricos o de similar naturaleza la autoría de las nuevas modalidades de la firma. A eso obedece la última frase de la reforma propuesta.

Como resultado de la puesta en funcionamiento de nuevas técnicas, las razones que el Registro asienta en los títulos sujetos a inscripción que devuelve a los usuarios, ya no solamente consistirán en un resumen elaborado por el operador (método todavía aplicado por el Segundo Registro) sino en una transcripción de la respectiva operación, (razón registral transcrita). Con ello se fortalecerá considerablemente la seguridad y certezas jurídicas y evitará que entre la inscripción y la razón del título puedan existir divergencias. Esta nueva modalidad también posibilitará que el notario pueda verificar sin necesidad de ir al Registro si existe

o no plena concordancia entre el título y su inscripción. Con esa finalidad, que se considera de evidente beneficio para el tráfico jurídico inmobiliario y de otros bienes inscribibles, se propone adicionar un tercer párrafo al artículo 1132 del Código Civil.

Las certificaciones del Registro, como las de los Registros Civil y Mercantil General de la República, podrán extenderse por nuevos medios que no están

expresamente contemplados en la actual legislación. Para cubrir este aspecto, la iniciativa de ley amplía los sistemas de reproducción que regula el artículo 1183 del Código Civil y dispone, como consecuencia de la introducción de nuevos métodos de firma, que en las certificaciones ésta pueda hacerse constar por los medios y con los mismos efectos jurídicos previstos en el nuevo inciso 8º. del artículo 1131 del mismo instrumento legal. Es un hecho reconocido que uno de los cambios más significativos en la modernización del Registro, ha sido que las operaciones se asientan en libros electrónicos. En consecuencia, se propone la reforma del artículo 1221 del C. Civil en el sentido que los libros del Registro podrán ser electrónicos y físicos. Actualmente solo se contempla los segundos. También se considera necesario ampliar la norma del

En cada país que se ha implementado el uso de la firma digital en el ámbito notarial, se han establecido las disposiciones legales que lo regulan

segundo párrafo de dicho artículo, para que el Registro pueda en el futuro ir introduciendo progresivamente los controles y sistemas de operación que le permitan contar siempre, sin necesidad de recurrir a nuevas reformas legales, con tecnología de punta, con los mejores y más eficientes programas, técnicas y sistemas, de acuerdo a las posibilidades económicas de cada institución y conforme a las normas comunes de seguridad correspondientes.

La propuesta en este aspecto, consiste en una norma más específica que la actual que es la que ha permitido, como se dijo al principio, que el Registro no sea una institución estática, sino que se haya adaptado progresivamente a los sistemas electrónicos con que operan casi todas las instituciones públicas de índole similar, no solo en el istmo centroamericano, sino que prácticamente en todo el mundo. Esta es la finalidad de la ampliación que contiene la iniciativa. Finalmente, en vista que es un hecho notorio que algunos de esos procesos ya están en funcionamiento en el Registro, se propone que el decreto entre en vigencia al día siguiente de su publicación, por cuanto no se requiere de ningún tiempo para su implementación y los usuarios ya están familiarizados con ellos.

La iniciativa pretende, por lo mismo, dotar al Registro de la Propiedad de un marco jurídico idóneo, funcional, efectivo, que responda a las necesidades actuales y posibilite, por otro lado, la permanente actualización de los sistemas digitales y electrónicos que promuevan y garanticen la seguridad y certeza jurídicas de sus operaciones, en beneficio del estado de derecho y de la paz social.

Documentos electrónicos a los registros públicos:

En España, es permisible la remisión y presentación por vía electrónica de títulos y documentos susceptibles de inscripción a los Registros Públicos, de la Propiedad, Mercantiles o de Bienes Muebles, expedidos con la firma electrónica avanzada, por el notario autorizante o responsable del protocolo. Esta nueva aplicación de la firma electrónica, en la presentación de documentos a los registros públicos, constituye un avance para el Derecho notarial y para el Derecho Registral.

Bibliografía y portales de información:

- Cabanellas Guillermo y Palazzi Pablo. Derecho de Internet Editorial Heliasta S.R.L., Argentina, 2004.
- Comisión Nacional Registral de Guatemala. Exposición de Motivos de Reformas al Código Civil, Decreto Ley 106. Guatemala, 2005.
- Luz Clara, Bibiana. Manual de Derecho Informático Editorial Jurídica Nova Tesis, Argentina, 2001.
- Rodríguez Adrados, Antonio. Incidencias en la Seguridad Jurídica Preventiva de la Ley 24/2001. Edita: Consejo General del Notariado. España. 2004.
- Rojas Amandi, Víctor Manuel. El Uso de Internet en el Derecho. Oxford University Press México, S.A. de C.V. México. 2000.
- Valenzuela Rivera, Mirna Lubet. La Informática en la Función Notarial. Tesis de grado, Universidad de San Carlos de Guatemala. 1990.
- HYPERLINK "<http://www.opinionvirtual.com>"
www.opinionvirtual.com
- HYPERLINK "<http://www.canallegal.com>"
www.canallegal.com
- HYPERLINK "<http://www.congreso.gob.gt>"
www.congreso.gob.gt
- HYPERLINK "<http://www.sat.gob.gt>"
www.sat.gob.gt
- Artículo del Abogado Javier Hernández Martínez, del Bufete opinión virtual.com
- Documento presentado por el Lic. Fernando Quezada Toruño a la Comisión Nacional Registral.

* *Abogada y Notaria, Universidad de San Carlos de Guatemala, Magíster Artium en Derecho Notarial, Universidad Mariano Gálvez de Guatemala, Directora General de Maestrías, Universidad Mariano Gálvez de Guatemala. Docente Universitaria de pregrado y posgrado. Consultora del Despacho de la Registradora General de la Propiedad de Guatemala.*