COMENTARIOS AL PROYECTO DE LEY "DE VALIDEZ JURIDICA DE LA FIRMA ELECTRÓNICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRÓNICO"

POR ABOG. LETICIA LORENA MEZA DUARTE

INTEGRANTE DE GHP Abogados

1.- INTRODUCCION

Conforme al Consejo Europeo Extraordinario de Lisboa de 2000: "La ingente cantidad de información disponible está creando notables oportunidades para su explotación gracias a la puesta a punto de nuevos productos y servicios. *La base de la nueva economía es la transformación de la información digital en valor económico y social, creando nuevas industrias, modificando otras y afectando profundamente la vida de los ciudadanos*" [i] .

En este sentido, nos encontramos inmersos en la denominada Sociedad de la Información, este concepto hace referencia a un paradigma que está produciendo profundos cambios en nuestro mundo al comienzo de este nuevo milenio. Esta transformación está impulsada principalmente por los nuevos medios disponibles para crear y divulgar información mediante tecnologías digitales. Los flujos de información, las comunicaciones y los mecanismos de coordinación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de *nuevas formas de organización social y productiva.*[ii]

En este contexto se enmarca el proyecto de ley que regula lo pertinente a la Firma Electrónica, la Firma Digital, los Mensajes de Datos y los Expedientes Electrónicos y que es objeto de análisis en este artículo.

2.- RESEÑA LEGISLATIVA.

El referido proyecto de Ley fue ingresado a la Cámara de Diputados de nuestro país bajo la denominación: "DE VALIDEZ JURÍDICA DE LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y LOS EXPEDIENTES ELECTRÓNICOS" el 21 de mayo de 2009, siendo aprobado por la referida Cámara el 16 de julio de 2009.

Posteriormente, la Comisión de Legislación, Codificación, Justicia y Trabajo de la Cámara de Senadores realizó modificaciones al proyecto inicial y el 22 de octubre de 2009 el proyecto de Ley fue resuelto con las modificaciones realizadas por el pleno de la Cámara de Senadores, llevando la denominación: "DE VALIDEZ JURIDICA DE LA FIRMA ELECTRONICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRONICO".

La entrada a la Cámara de origen con las modificaciones hechas por la Cámara revisora, se produjo el 03 de noviembre de 2009 y el 09 de noviembre de 2009 la Comisión de Legislación y Codificación de la Cámara de Diputados, se ratificó en su sanción original.

Actualmente se encuentra en estudio por parte de la Comisión de Asuntos Constitucionales y por la Comisión de Ciencia y Tecnología de la Cámara de Diputados.

Este proyecto de Ley contiene seis Títulos, algunos de ellos divididos en Secciones. El proyecto de Ley de la Cámara de Diputados consta de 45 artículos, mientras que en el de Senadores cuenta con 47 artículos.

3.- DESARROLLO

Dentro de las innumerables figuras que componen el presente proyecto de ley, resulta pertinente precisar que en esta oportunidad, por la relevancia de los mismos, se enfocarán dos títulos en particular, a saber: el Título Primero: "Disposiciones Generales"; y el Título III: "De la Firma Electrónica".

3.1. TITULO PRIMERO "Disposiciones Generales"

En el título primero de “Disposiciones Generales”, se establece el **Objeto y ámbito de aplicación,** por medio del cual esta ley *RECONOCE LA VALIDEZ JURÍDICA* de la firma electrónica, los mensajes de datos, el expediente digital y firma digital, y regula la utilización de los mismos, las empresas certificadoras, su habilitación y la prestación de los servicios de certificación. Cabe mencionar que la Comisión de Legislación de la Cámara de Senadores, introdujo una modificación al presente artículo incorporando el reconocimiento de validez jurídica al *expediente electrónico*, en reemplazo de expediente digital, empleado en el proyecto de origen.

El proyecto contiene una sección dedicada a las definiciones. En este sentido, es importante destacar que las normativas internacionales incluyen a las mismas dentro de sus respectivos cuerpos legales, de tal modo a dejar en claro el alcance de los mismos, entre las que podemos citar a la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) 2001 sobre “Firmas Electrónicas” y a la Resolución MERCOSUR N° 37/2006 “Reconocimiento de la Eficacia Jurídica del Documento Electrónico, la Firma Electrónica y la Firma Electrónica Avanzada en el ámbito del MERCOSUR”.

Por *Firma Electrónica*, este proyecto de ley establece que es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. De ello se puede colegir que la Firma Electrónica posee un grado básico en seguridad en cuanto a la identificación de un signatario en el ambiente virtual.

Con relación a la *Firma Digital*, se establece que es una firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

Resulta interesante poder determinar – a partir de la referida definición – los elementos de la Firma Digital[iii]:

a) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;

b) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;

c) ser susceptible de verificación por terceros;

d) estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable; y

e) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma.

En este sentido, es de destacar que la Firma Digital tiene la característica de tener un mayor grado de certeza con relación a la Firma Electrónica, atendiendo a los métodos de detección, verificación de identidad del titular y certificación de la integridad del documento y la autoría del mismo. En otras legislaciones, la Firma Digital también es denominada Firma Electrónica Avanzada (Resolución MERCOSUR N° 37/2006).

Mensaje de Datos, por su parte, es toda información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax, siendo esta enumeración meramente enunciativa y no limitativa.

Se puede constatar las actividades que explicita la normativa en lo relativo a Mensajes de Datos destacando el ambiente virtual en el cual se desarrollan las mismas e indicando a su vez los medios a través de los cuales se realizan. Sobre esto último, es preciso mencionar la acertada redacción con relación a la característica de la enumeración; señalando que es meramente enunciativa y no limitativa y por ende, dejando abierta la posibilidad de incorporaciones a nuevos elementos que cumplan las funciones de medios electrónicos, ópticos o similares, teniendo en cuenta el vertiginoso avance de la tecnología.

Como *Documento Digital*, el proyecto señala que es un mensaje de datos que representa actos o hechos, con independencia del soporte utilizado para su creación, fijación, almacenamiento, comunicación o archivo.

Un elemento que incluye la definición de Documento Digital que distingue a otras normativas es el de incluir -además de las funciones de fijación, almacenamiento o archivo- la función de *comunicación*[iv].

Como *Firmante*, es entendida toda persona física o jurídica titular de la firma electrónica o digital. Cuando el titular sea una persona jurídica, ésta es responsable de determinar las personas físicas a quienes se autorizará a administrar los datos de creación de la firma electrónica o digital. Al respecto, cabe señalar que la Comisión de legislación de la Cámara de Senadores, equiparó el concepto de *Firmante* al de S*uscriptor o Signatario*.

El titular de una firma electrónica o digital puede ser tanto una persona física como jurídica.

El proyecto establece una responsabilidad para las personas jurídicas titulares de una firma electrónica o de una firma digital, cual es la de determinación de *personas físicas* a quien aquélla autorizará a administrar los datos de creación de las respectivas firmas.

El *Remitente de un Mensaje de Datos*, es toda persona que haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar un mensaje de datos.

Conforme a la definición anterior de Firmante, se entiende que remitente puede ser tanto una persona física o jurídica, por cuenta propia o en cuyo nombre se haya actuado, verificando que esto último se dé en el contexto de la debida autorización en la administración de los datos de creación.

Con relación al *Certificado de Firma Digital*, el proyecto de ley establece que es todo mensaje de datos u otro registro emitido por una entidad legalmente habilitada para el efecto y que confirme la vinculación entre el titular de una firma digital y los datos de creación de la misma.

Este elemento es de suma importancia ya que confirma la vinculación entre el titular de una firma digital y los datos de creación de la misma, otorgando de esta manera certeza.

El *Prestador de Servicios de Certificación*, es la entidad prestadora de servicios de certificación de firmas electrónicas.

De manera acertada, la Comisión de Legislación de la Cámara de Senadores, modificó esta definición atendiendo a que la certificación es realizada sobre *firmas digitales* y no sobre firmas electrónicas –tal como aparece en el proyecto de origen-, puntualizando que son las firmas digitales las que están certificadas por un prestador acreditado.

Con relación al *Expediente Electrónico*, se entiende que es la serie ordenada de documentos públicos registrados por vía informática, tendientes a la formación de la voluntad administrativa en un asunto determinado. Esta definición se contextualiza en el marco del Gobierno Electrónico como política pública y con miras a la optimización de la gestión administrativa.

Para la mejor aplicación de esta ley, la misma establece algunos *Principios Generales:*

- *Neutralidad tecnológica*, entendiéndose que ninguna de las disposiciones de la presente Ley podrá ser aplicada de forma que excluya, restrinja o prive de efectos jurídicos a cualquier otro sistema o método técnico conocido o por conocerse que reúna los requisitos establecidos en la presente ley. En este sentido, se da un amplio marco para la aparición de nuevos sistemas o métodos técnicos y que la normativa pueda estar a la altura de las necesidades de la sociedad.

- *Interoperabilidad*, este principio se refiere a que las tecnologías utilizadas en la aplicación de la presente Ley se basarán en *estándares internacionales*. Este punto es de vital importancia atendiendo a la característica propia de las nuevas tecnologías: el de traspasar fronteras y por ende debe estar armonizada y en consonancia con las demás.

- *Interpretación funcional*, el último principio establece que los términos técnicos y conceptos utilizados serán interpretados en base a la *buena fe* de manera que no sean negados efectos jurídicos a un proceso o tecnología utilizado por otro Estado por el sólo hecho de que se le atribuya una nomenclatura diferente a la prevista en la presente Ley.

TITULO TERCERO: De la Firma Electrónica

Este título comprende tres secciones. La primera que trata sobre "La Firma Electrónica"; la segunda que trata sobre "La Firma Digital" y la última referida a "Los Prestadores de Servicios de Certificación".

En la primera Sección se destacan las *Obligaciones* de los titulares de una firma electrónica ya que los obliga a actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma. Al momento que se emplee un certificado para refrendar la firma electrónica, el titular debe actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su periodo de validez o que hayan de consignarse en él sean exactas y cabales.

El titular de la firma electrónica incurrirá en responsabilidad personal, solidaria e intransferible por el incumplimiento de los requisitos enunciados anteriormente.

En lo relativo a los *Efectos* del empleo de una firma electrónica; en el caso que se aplique una firma electrónica a un mensaje de datos, este proyecto establece que implica para las partes una *presunción* de que el mensaje de datos proviene del firmante; y que el firmante aprueba el contenido del mensaje de datos.

Sobre la *Validez jurídica* de la firma electrónica, en caso de desconocimiento de la misma, corresponde a quien la invoca acreditar su validez.

En lo pertinente a la *Revocación* de la firma electrónica: la misma pierde todo tipo de valor como firma en los siguientes casos: i) por extinción del plazo de vigencia de la misma; ii) a solicitud del titular de la firma; iii) por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso; iv) por resolución judicial ejecutoriada; y v) por incumplimiento de las obligaciones del usuario establecidas en la presente ley.

Seguidamente, se aborda lo referente a la *Firma Digital*, señalándose el caso en que la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia. Esta puntualización sobre la validez jurídica de una firma digital es de suma relevancia, atendiendo a que otorga los mismos efectos jurídicos que posee una firma manuscrita.

Pero, también existen algunas exclusiones con relación al uso de la firma digital, ya que se considera que las disposiciones de esta normativa no son aplicables a actos jurídicos de índole personalísimo[v]:

a. Disposiciones por causa de muerte,
b. Actos jurídicos del Derecho de Familia y
c. Actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital.

Para que una Firma Digital sea considerada válida, la misma debe cumplimentar con los siguientes requisitos:

a) Tiempo: haber sido creada durante el período de vigencia de la firma digital.

b) Verificación firmante/firma digital: haber sido debidamente verificada la relación entre el firmante y la firma digital, por la referencia a los datos indicados en el certificado digital, según el procedimiento de verificación correspondiente.

c) Emisión: Que dicho certificado haya sido emitido por una entidad prestadora de servicios de certificación autorizada por la presente ley.

d) Control: los datos de creación de la firma estaban, en el momento de la firma, bajo el control del firmante;

e) Detección en la Firma: es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

f) Detección en el Mensaje de Datos: es posible detectar cualquier alteración de la información contenida en el mensaje de datos al cual está asociada, que fuera hecha después del momento de la firma.

En lo atinente a los *Efectos* de su empleo a un mensaje de datos, implica para las partes la *presunción* de que el mensaje de datos proviene efectivamente del firmante y que el contenido del mensaje de datos no ha sido adulterado desde el momento de la firma y el firmante, a su vez, aprueba el contenido de ese mensaje de datos.

Un requisito importante para que la presunción sea efectiva, es que esa firma digital aplicada a ese mensaje de datos pueda ser efectivamente *verificada* con el certificado digital respectivo expedido por la prestadora de servicios de firma digital.

Con relación a la vigencia de los efectos mencionados anteriormente para el mensaje de datos al que fuere aplicada una firma digital, la normativa establece que es *indefinida.* Incluso, cuando con posterioridad a la aplicación de la misma, ésta fuera revocada por cualquiera de los motivos indicados en esta normativa.

Por otra parte, para que una firma digital pueda ser *Revocada* existen dos supuestos, a saber:

- Tiempo: por extinción del plazo de vigencia de la firma digital.
- Prestador de Servicio de Certificación: ya sea por solicitud del titular de la firma; por resolución judicial ejecutoriada; o por incumplimiento de las obligaciones del usuario establecidas en esta normativa.

En la Sección III se establecen pautas para el desarrollo de la actividad de los llamados "*prestadores de servicios de certificación"***.**

Los prestadores de servicios de certificación son las personas jurídicas habilitadas por la Autoridad normativa indicada en la presente Ley (*que según el proyecto de origen es el Ministerio de Industria y Comercio-MIC-, y según el proyecto de Senadores es el Instituto Nacional de Tecnología y Normalización-INTN-*), en base a las disposiciones de la presente Ley así como a las disposiciones del decreto reglamentario correspondiente.

Los requisitos básicos que deben cumplimentar los prestadores para ser habilitados son:

a) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

b) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

c) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;

d) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas;

e) utilizar sistemas y productos fiables que se requiera para prestar servicios de certificación y que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

f) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos;

g) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Ley, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, pudiendo emplearse para el efecto fianzas, avales, seguros o cualquier otro medio;

h) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

i) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de asignación de firmas electrónicas;

j) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

- sólo personas autorizadas puedan hacer anotaciones y modificaciones,

- pueda comprobarse la autenticidad de la información,

- los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y

- el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados.

k) Demostrar la honestidad de sus representantes legales, administradores y funcionarios a través de certificaciones de antecedentes policiales y judiciales.

Para que un certificado digital sea considerado *válido* deber ser emitido por una entidad prestadora de servicios de firma digital habilitada conforme a esta normativa y responder a formatos y estándares tecnológicos preestablecidos reconocidos internacionalmente, y contener como mínimo los siguientes datos:

- Identificación: entre su titular y la entidad que lo emitió.
- Verificación: respecto de su vigencia o revocación.
- Información necesaria: para la verificación de la firma.
- Política de certificación: identificar bajo cuál fue emitida, sobre todo si la misma implica limitación en los fines en que ha de utilizarse o de la responsabilidad que asume el prestador con relación al certificado emitido.

Entre las *obligaciones* más importantes que poseen los prestadores de Servicios de Certificación se puede citar a las siguientes:

- Adjudicar una firma digital a quien así lo solicite sin distinciones ni privilegios de ninguna clase, siempre y cuando el solicitante presente los recaudos establecidos al efecto.

- Actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él sean exactas y cabales;

- Además deberá informar a quien solicita la adjudicación de una firma digital con carácter previo a su emisión las condiciones precisas de utilización de la firma digital, sus características y efectos, forma que garantiza su posible responsabilidad patrimonial Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

- Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

- Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

- Publicar en Internet o cualquier otra red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de firmas digitales vigentes y revocadas, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que considere pertinente;

Con relación a la *Protección de Datos Personales*, que se erige en un elemento tutelado por distintas normas de carácter internacional en el área de nuevas tecnologías (CNUDMI-MERCOSUR), en esta sección se establece que los datos no podrán ser obtenidos o utilizados para otro fin, sin el consentimiento expreso del titular de los datos.

4.- COMENTARIOS FINALES

El proceso del uso de las Tecnologías de la Información y las Comunicaciones (TICs) para el desarrollo no se debería entender sólo como un fenómeno meramente tecnológico, sino debe analizárselo también desde su dimensión política (desarrollo e interacción igualitaria de sus habitantes). Esta dimensión contiene un componente adicional: la necesidad de expedir una normativa acorde al mencionado objetivo social y político, conjugado en correcto equilibrio con la vertiginosa evolución que es intrínseca a la tecnología.

Este proyecto de Ley de **DE VALIDEZ JURIDICA DE LA FIRMA ELECTRÓNICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRÓNICO,** viene a llenar un vacío con relación a las necesidades actuales tanto del sector privado como público, en el orden interno; como también el de acompañar los procesos de integración actuales y estar en armonía con los mismos, en el orden internacional.

Es un avance relevante que se da desde el aspecto legislativo, que deberá ser incorporado y asimilado por la ciudadanía toda como también por el sector de la administración pública para un real y concreto aprovechamiento de las innúmeras ventajas y opciones que nos brinda.

Aún sería necesaria una legislación específica sobre Comercio Electrónico, si bien es cierto que nuestro Código Civil nos brinda las bases para este relacionamiento jurídico, esta nueva

forma de Comercio, precisa de nuevos elementos normativos que le proporcionen certeza jurídica, elemento indispensable hoy en día para crear un ambiente de negocios atractivo, creíble y fiable.

---

[i] Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática. "Derecho de Internet & Telecomunicaciones". Pág. 05. Legis Editores S.A. Primera Edición 2003. Impreso en Colombia.

[ii] Documento "Los cambios hacia una Sociedad de la Información en América Latina y el Caribe" presentado por la Comisión Económica para América Latina y el Caribe (CEPAL), durante la reunión de Bávaro del 2003.

[iii] MERCOSUR/GMC EXT./RES N°37/2006, artículo 3°, inc. 2.

[iv] Como ejemplo podemos mencionar a la Ley argentina N°25.506/2001 "Ley de Firma Digital", artículo 6° y a la Resolución MERCOSUR N° 37/2006, artículo 3°, inc. 5°.

[v] Puede apreciarse también esta figura en: Ley N° 25.506/2001 "Firma Digital" de Argentina, art. 4°; y en la Ley N° 19.799/2002 "Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma" de Chile, art. 3°, inc. a), b) y c).