C-57

Panamá, 14 de marzo de 2001.

Honorable Legislador
Eddy E. Londoño G.
Presidente de Comisión de Comercio,
Industrias y Asuntos Económicos
Asamblea Legislativa.
E S. D.-

Honorable Legislador:

Me refiero a su Nota fechada 27 de diciembre del 2000, recibida en este despacho el 16 de enero del presente año en torno al anteproyecto de Ley 98 "Por medio de la cual se adopta la normativa aplicable a la firma Digital".

En virtud de su solicitud, le hacemos llegar algunas consideraciones sobre este instrumento legal, las cuales esperamos coadyuven y enriquezcan el contenido de dicho anteproyecto.

Comentarios respecto del proyecto de ley por medio del cual se adopta la normativa aplicable a la Firma Electrónica o Digital.

Introducción.

Creo que para poder intentar una aproximación al estudio de este proyecto de Ley por medio del cual se adopta la normativa aplicable a la firma digital, es importante tener por base una introducción preliminar, respecto de este sistema de comunicación y descripción electrónica de datos. Para ello nos haremos asistir, en términos generales por el estudio de la profesora Titular de Derecho

Mercantil de la Universidad de Palma (Baleares)[1], la doctora la Apolónia Martínez Nadal, de su trabajo Firma Electrónica, Valor Jurídico y Seguridad.

En efecto, en el comercio electrónico, el clásico documento de papel es sustituido por el novedoso documento electrónico. Y por ello, desaparecen las tradicionales firmas manuscritas y las funciones que ellas desempeñan. Desde el punto de vista técnico, se ofrece la firma digital, basada en la criptografía asimétrica, como técnica sustitutiva que puede desempeñar iguales o incluso superiores funciones.

Los criptosistemas de clave asimétrica o pública están en el uso de un par de claves asociadas: una clave privada, conocida sólo por su titular, que debe mantenerla en secreto (e incluso, puede ocurrir que ni siquiera el titular conozca la clave privada, que probablemente se mantenga en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal, o, en la situación ideal, mediante un dispositivo de identificación biométrica, p. ej., a través del reconocimiento de una huella digital o la lectura láser del iris de los ojos), y una clave pública, relacionada matemáticamente con ella, y que puede ser accesible para cualesquiera (e incluso debe serlo, a través, p.ej., de directorios públicos de fácil acceso). Si bien las dos claves están matemáticamente relacionadas entre sí, el diseño y la ejecución en forma segura de una criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan derivar de ella la clave privada (inderivabilidad).

Este sistema de criptografía asimétrica permite realizar firmas digitales, que proporcionan autenticidad, integridad y no rechazo de origen, y que pueden resultar tanto o más útiles, válidas y eficaces en el comercio y en los procedimientos legales como la firma escrita sobre papel- El procedimiento básico para ello es el siguiente:

a) El emisor de una mensaje (cifrado o no a efectos de confidencialidad) lo cifra digitalmente utilizando su clave privada, y su receptor podrá descifrarlo utilizando la clave pública del suscriptor, de forma tal que si el mensaje, conteniendo información textual, es legible, tiene la seguridad de que el

[1] Universitat de les Illes Baleares. Carretera de Validemossa, km 7'5. CP 07003 Palma (Baleareas)

mensaje ha sido enviado por el titular de la clave privada correspondiente a la clave pública que él utiliza (autenticación); además, el mensaje no ha sido modificado (integridad), y que, finalmente, el emisor del mensaje no puede negar ser el autor de ese mensaje con un determinado contenido (no repudiación de origen). Cualquiera que tenga la clave pública del usuario puede verificar la integridad del mensaje: si el mensaje ha sido modificado, el criptograma no se descifrará de forma adecuada, mostrando que ha sido alterado o sustituido.

b) No obstante, el procedimiento es algo más complicado porque debe añadirse un nuevo elemento: la función de hash, algoritmo que transforma una secuencia de bits en otra menor, y que se aplica para la creación como para la verificación de la firma digital. Debido a que la aplicación de criptografía asimétrica sobre la totalidad del mensaje, puede resultar costosa, especialmente si éste es muy extenso, se aplica sobre el mensaje inicial el algorismo con función de hash, y se obtiene un resumen del mismo (denominado compendio del mensaje o huella digital), caracterizado por su irreversibilidad (esto es, a partir del resumen no puede obtenerse el mensaje completo inicial), y por ser único del mensaje (es decir, es computacionalmente imposible obtener un segundo mensaje que produzca el mismo resumen o hash), de forma que cualquier cambio en el mensaje produciría un resumen o hash diferente. A continuación, el resumen o hash, de menor extensión, es cifrado con la clave privada de criptografía asimétrica del firmante (que proporciona, como veremos, integridad, autenticidad y no rechazo de origen). Y, finalmente, ambos mensajes, el mensaje inicial, total, y en claro, y la firma digital (el hash o resumen cifrado), son remitidos conjuntamente al destinatario.

c) Finalmente, el receptor, que cuenta con dos elementos (el mensaje inicial y la firma final del hash) debe proceder a la verificación de la firma. La verificación de la firmas digital es el proceso de comprobación de esa firma por referencia al mensaje original y a una clave pública dada, determinando de esta forma si la firma digital fue creada para este mismo mensaje utilizando la clave privada que corresponde a la clave pública referida. Para ello, el verificador realizará dos operaciones; descifrará el

hash firmado con la clave privada del emisor aplicando la clave pública del mismo; y aplicará la función de hash sobre el mensaje completo que ha obtenido (pues no es posible realizar lo contrario: 'desresumir' el hash que ha recibido, dada la irreversibilidad ya mencionada de esta función). Si el hash recibido y descifrado y el segundo hash obtenido coinciden, el destinatario tiene la seguridad de que el mensaje recibido ha sido firmado por el emisor con ese contenido. Por el contrario, si uno u otro de los dos elementos ha sido alterado en algún momento, no habrá coincidencia de los dos resúmenes, con lo que el receptor no podrá ni debería llegar a la misma conclusión. Y todo ello, que aparenta ser un complicado proceso matemático, se produce en cuestión de segundos con la ayuda de ordenadores.

De esta forma, la firma digital puede definirse, pues, como la transformación de un mensaje utilizando una función de hash y un criptosistema asimétrico, de forma que una persona que tenga el mensaje inicial y la clave pública del firmante puede determinar de forma segura:

a) Si la transformación fue realizada usando la clave privada de un sujeto, sólo puede ser verificado por el receptor utilizando la clave pública de ese mismo sujeto.

b) Si el mensaje inicial ha sido alterado desde la transformación; y se satisface así la exigencia de integridad, pues, si el mensaje ha sido alterado en lo más mínimo, su resumen no coincidirá con el resumen firmado del mismo descifrado, aplicando la clave pública de su emisor; y si el mensaje firmado ha sido alterado no coincidirá con el resumen del mensaje en claro.

La firma digital consigue, así, iguales, si no superiores efectos, que la firma manuscrita pues da integridad, autenticidad, y, en definitiva, no rechazo de origen.

En este sentido, la iniciativa legislativa que estudiamos hoy en día sobre la firma digital realiza un reconocimiento de los efectos de la misma equiparándola, con más o menos exigencias, a la firma

manuscrita, y estableciendo, incluso, determinadas presunciones o reglas de atribución a su favor.

En cualquier caso, ha de tenerse en cuenta que estas presunciones legales y reglas de atribución serán ciertas siempre y cuando tengan un fundamento técnico adecuado. Es decir, para que se atribuya un mensaje firmado con una clave privada determinada al titular de esa clave, es necesario que el par de claves en cuestión *cumpla una serie de características y requisitos, que implican una mínima calidad de las claves y mínimas garantías* del procedimiento de generación de las mismas que esta tecnología requiere, y que deberá estar definido en la Ley.

Análisis General del General del proyecto ley.

El proyecto de ley que se nos presenta para su estudio, va de la mano con la actual doctrina de los Tribunales Constitucionales y Corte Supremas de países como Alemania, España, Colombia, en donde sostienen que la firma autógrafa no es la única manera de signar, pues hay otros mecanismos que, sin ser firma autógrafa, constituyen trazados gráficos, que asimismo conceden autoría y obligan.

Así, las claves, los códigos, los signos y, en casos, los sellos son firmas en el sentido indicado. Y, por otra parte, la firma es un elemento muy importante del documento, pero, a veces, no esencial, en cuanto existen documentos sin firma que tienen valor probatorio (como son los asientos, registros, papeles domésticos y libros de los comerciantes).

En consecuencia, aunque, al igual que en el caso de los documentos comunes, puede haber documentos electrónicos sin firma, el documento electrónico (y, en especial, el documento electrónico con función de giro mercantil) es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido.

Por lo tanto, si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos de los ordenadores, procesadores o computadoras y se garantiza, con las pruebas periciales en su caso, la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil en soporte informático, con función de giro, debe gozar de plena virtualidad operativa.

Por esta razón impulsar un proyecto de ley como el que hoy día estudiamos, sobre la firma electrónica, es propiciar una norma que va a impulsar de forma decisiva la Sociedad de la Información en Panamá y que garantiza la seguridad de las comunicaciones que realicen las empresas y los ciudadanos a través de la red y, en especial, el comercio electrónico.

El proyecto de ley se resguarda en afirmar que la firma electrónica es un código de autenticación que identifica formalmente a los autores de un documento. Y que tendrá el mismo valor jurídico que la firma manuscrita y será admisible como prueba en juicio.

En nuestra opinión, el presente proyecto de ley comporta un compromiso claro para que las nuevas tecnologías en las comunicaciones sean accesibles a todos. Se facilita con ello, la modernización tecnológica, no sólo en los ámbitos empresariales sino, también y especialmente, en los domicilios de los ciudadanos. Amen de que se le permite al servicio público panameño, contar con una herramienta de actualización de su gestión de por sí burocrática.

Es importante destacar la importancia que la norma tiene para el sector de las pequeñas y medianas empresas panameñas y el desarrollo y uso del comercio electrónico en Panamá, con máxima seguridad jurídica.

Las empresas nacionales podrán constituir una red virtual para la distribución de sus productos, incluso más allá de nuestras fronteras, sin necesidad de contar con una red física, con el ahorro que ello representa.

Un tema crucial del cual se cuida el proyecto de ley, es el relativo a la seguridad jurídica. Para proteger la seguridad y la integridad de

las comunicaciones, la firma electrónica tendrá que estar avalada por un certificado reconocido que permita verificar la identidad del usuario y que será expedido por el prestador de servicios de certificación.

Estas empresas o entidades de certificación, que actuarán como notarios de la red, deberán inscribirse en un registro público, en sede administrativa. Específicamente bajo la responsabilidad del Ministerio de Comercio e Industrias. Sobre esto, creo que se requiere que el esfuerzo desplegado por el Ministerio de la Presidencia, específicamente, por medio de la Secretaría Nacional de Ciencia y Tecnología (Senacyt), se coordine con el Ministerio de Comercio e Industrias, a fin de evitar la duplicación de tareas funciones.

Los puntos principales del proyecto de Ley, es el ámbito de aplicación en donde se regula el uso de la firma electrónica, el reconocimiento de su eficiencia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son aplicadas a los prestadores de servicios establecidos en Panamá.

Otro tema atinado, es el de las definiciones de las expresiones de firma electrónica y firma electrónica avanzada.

El Proyecto de Ley define a la firma electrónica como "el conjunto de datos, en forma electrónica, anejo a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o los autores del documento que la recoge".

Firma electrónica "avanzada" es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Un tema que nos parece atinado, es el de establecer los efectos jurídicos de la firma electrónica.

La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados

en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio.

Otro aspecto novedoso, es el de la creación de un Registro Público de prestadores de servicios de certificación en el Ministerio de Comercio e Industrias, que bien podría ser en el Senacyt, en el que deberán solicitar su inscripción con carácter previo al inicio de su actividad. Con el fin de garantizar su máxima eficacia jurídica, pública o privada, la firma electrónica tendrá que estar avalada por un certificado reconocido que permita verificar la identidad del usuario y que será expedido por el prestador de servicios de certificación.

Asimismo, el texto legislativo establece las obligaciones, garantías y condiciones exigibles a los prestadores de servicios de certificación.

Se crea un régimen de acreditación de los notarios de la Red o de las entidades que certificarán a los usuarios que su firma electrónica sea segura.

La acreditación de estas entidades es voluntaria, pero se configura como un sello de calidad respecto de su adecuación a la normativa vigente, y otorgará garantías a los usuarios de que la empresa con la que trabaja tiene las suficientes garantías de seguridad y confidencialidad de sus datos y de sus comunicaciones.

Se requerirá de un reglamento en donde también se regule el régimen aplicable a los dispositivos seguros de creación de la firma electrónica y a los de verificación, que también podrán obtener del Ministerio de Comercio o el de la Presidencia (Senacit), un sello de calidad que demuestre que son especialmente seguros para la prestación de servicios de firma electrónica.

Todos los certificados otorgados del mismo modo en los distintos países serán reconocidos automáticamente en Panamá, mientras que en aquellos países se dé el mismo trato de reciprocidad a los certificados panameños. Sin embargo, se hará necesaria la expedición y firma de convenios de reconocimiento mutuo.

Comentarios adicionales según algunos artículos del proyecto.

En el artículo 5, creo que se debe establecer que el instrumento legal para establecer condiciones adicionales sobre el uso de la firma digital o electrónica, debe ser un Decreto del Poder Ejecutivo, y no una Resolución de Gabinete, ya que con el Decreto se establece con claridad el necesario deslinde de responsabilidad.

En el mismo artículo 5 se podrá agregar que las condiciones adicionales deberán garantizar el cumplimiento del Código Administrativo, la **Ley 38 de 2000**, sobre procedimiento administrativo general, y la **Ley**.

En el artículo 6 se podrá establecer que uno de los órganos competentes para el ejercicio de la función de acreditación podría ser Senacyt.

En el artículo 14 se podría establecer simplemente que la responsabilidad se deriva al causar daños injustificados.

En el artículo 28 se podría tener presente, que otra norma legal a tener en cuenta es la Ley 38 del 2000.

Con la pretensión de haber colaborado con su importante función legislativa, por medio de los presentes comentarios, aprovecho la oportunidad para reiterarle mi respeto y consideración.

Atentamente,

Original Firmado — Licda. Alma Montenegro de Fletcher, Procuradora de la Administración

Alma Montenegro de Fletcher
Procuradora de la Administración.

AMdeF/15/hf.