INFORME DE INVESTIGACIÓN CIJUL

TEMA: JURISPRUDENCIA SOBRE COMERCIO ELECTRÓNICO

RESUMEN: El presente informe aborda el tema " Jurisprudencia sobre comercio electrónico", desarrollando entre otros temas: competencia desleal, en uso de marca internacional inscrita por otra empresa en dirección de internet, la firma electrónica como herramienta en la seguridad del comercio electrónico, impuesto de ventas sobre el comercio electrónico, además se incluye un anexo de votos de la Comisión Nacional del Consumidor por denuncias contra aerocasillas en compras por internet.

Índice de contenido

1 JURISPRUDENCIA

A.Competencia desleal Uso de marca internacional inscrita por otra empresa en dirección de internet

[TRIBUNAL PRIMERO CIVIL][1]

"V.- De los autos se tiene por demostrado que la actora presentó para su inscripción su marca “TRAVELWEB” en Canadá el 25 de marzo de 1996, inscrita el 12 de abril de ese año. Se dispuso que el uso en ese país data al menos desde octubre de 1994 (traducción de folios 16 a 19). Con esas mismas fechas, se pidió la inscripción en la Comunidad Europea en clase 42, para suministrar información sobre viajes, alojamiento y turismo de reservación por medio de comunicaciones públicas en línea por computadora (folios 20 a 30). Igualmente se solicitó la inscripción en la Oficina de Patentes y Marcas Comerciales de los Estados Unidos y, como fecha de uso, se indica 1º de octubre de 1994. La fecha de presentación fue el 9 de marzo de 1995 y se inscribió el 28 de marzo de 1996 (folios 67 y 81). También hay varias solicitudes en esa misma oficina de los Estados Unidos por la misma marca, pero por diversas clases entre ellas 35, 39, 41, 42. En Costa Rica, la marca de comentario se encuentra inscrita a nombre de la actora a partir del 29 de setiembre de 1997, como se concluye de las certificaciones de folios 325, 372 y 415. Por su lado, la demandada inscribió el dominio en la Academia Nacional de Ciencias el 25 de noviembre de 1997: travelweb.co.cr. Esa inscripción se realizó tres días antes de presentarse la demanda el 28 de noviembre de 1997. Como prueba documental marcada 6, folios 262 y siguientes, se acredita que la demandada utiliza TRAVELWEB para ofrecer servicios de turismo en Costa Rica. Por último, con la prueba siete, se demuestra el uso de la marca por la actora en internet, con la gran cantidad de de usuarios que ingresan a esa página. A folio 379 se agrega traducción de un documento que contiene los datos de los servicios que presta la marca de la accionante a nivel de hotelería en el mundo. VI.- Con ese cuadro fáctico, debidamente demostrado con prueba documental, el fallo estimatorio es correcto y debe mantenerse, desde luego en lo que es motivo de inconformidad. Resulta innecesario reiterar, pues sería odioso hacerlo, el apoyo normativo que contiene la sentencia. Los fundamentos de derecho son incuestionables, pero para efectos de esta confirmatoria singular relevancia tiene lo dispuesto en el numeral 17 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. En su enunciado, se prohíben los actos de competencia contrarios a las normas de corrección y buenos usos mercantiles, generalmente

aceptados en el sistema de mercado, que causen daño efectivo o amenza de daño comprobados. De seguido el legislador enumera algunos supuestos propios de competencia desleal, entre ellos se destacan los incisos a) y d). En el primero se prohibe actos que generan confusión , por cualquier medio, respecto del establecimiento comercial, los productos o la actividad económica de uno o varios competidores. En el segundo, se trata de impedir el uso , imitación, reproducción, sustitución o enajenación indebida de marcas , nombres comerciales, denominaciones de origen, expresiones de propaganda, inscripciones, envolturas, etiquetas, envases o cualquier otro medio de identificación, correspondiente a bienes o servicios propiedad de terceros. En autos se demuestra que la marca de servicio “TRAVELWEB” pertenece a la actora, inscrita en Costa Rica en el Registro de la Propiedad Industrial desde el 29 de setiembre de 1997. No obstante, su uso a nivel de mercado internacional en internet data del 1º de octubre de 1994, pero su inscripción en diversos países se produjo en los primeros meses de 1996 (Canadá, Comunidad Europea y Estados Unidos). También se acredita que la demandada utiliza ese vocablo al menos en dos direcciones en el campo informático con la finalidad de promocionar servicios de hotelería y turismo en general. Ella misma lo admite al contestar la demanda. Es indudable que ese proceder causa confusión en el consumidor, quien fácilmente puede estar negociando con una empresa distinta. El hecho generador afecta la actividad económica de la empresa que tiene inscrita la marca con anterioridad. El Tribunal no cuestiona la libertad mercantil y ofrecer al consumidor buenos y mejores servicios, pues esa competencia justa y de buena fe conlleva grandes beneficios. En aras de conservar ese marco de lealtad, el derecho internacional y las normas internas de cada país, reprochan cualquier conducta que ponga en peligro ese objetivo. VII.- En este asunto, el punto debatido no es simplemente el uso de una marca en los términos comunes. Por ejemplo, el empleo de una marca visible en vasos, refrescos, comida enlatada, entre otros. La cuestión de autos reviste una particularidad: es una marca de servicios inscrita en el Registro, pero ser utiliza para ofrecer servicios por medio de internet. No es la tradicional violación de actos en el mercado cotidiano como se ha concebido. El avance en la tecnología permite ahora adquirir bienes y servicios sin salir del hogar o de la oficina, para ello basta una computadora y tener acceso a internet. Este nuevo panorama económico, donde por ese medio se realizan numerosos negocios cada minuto y se mueven impensables sumas de dinero, exigen normas de protección para evitar engaños o confusiones a la gran cantidad de usuarios de ese sistema. La red internet pertenece a la categoría de las redes WAN (redes grandes de cobertura mundial) y esta

integrada por el conjunto de redes interconectadas más grande, con máquinas localizadas alrededor del mundo. Internet comprende el gobierno, al comercio y a las organizaciones educativas de todo el planeta. Es una biblioteca digital global, intensa sobre una tecnología de comunicación flexible. Esta biblioteca digital ofrece diferentes servicios que se utilizan para crear, explotar, accesar, buscar, ver y comunicar información sobre un conjunto de diversos temas. La información está organizada en menús, almacenada en documentos hipermedios, documentos de texto. La información puede ser audio, vídeo comunicados utilizando el correo electrónico o manteniendo conversaciones interactivas de computador a computador. Los servicios básicos de internet son: 1) correo electrónico (e-mail). 2) chatting o conversar con otras personas usando el teclado de la PC. 3) FTP (file transfer protocol) protocolo de transferencia de archivos, permite transferir archivos de texto, gráficos, de sonido de una computadora a la nuestra. 4) Word Wide Web (www) organiza la información por medio de hipermedios (cada documento puede contener referencias incorporadas a imágenes, audio, sonido, texto en otros documentos). Cada miembro de esta gran red debe tener un nombre que permita identificarlo, lo que se denomina “dominio”. Como parte de su organización, internet ha definido un conjunto de categorías o dominios que permiten agrupar los diferentes tipos de redes o computadores conectados a la red. Dentro de estas categorías o dominios, en Costa Rica se pueden mencionar las de carácter académico (ac), gubernamental (go), comercial (co), organización (or), salud (sa) y financiero (fi). Finalmente, la dirección de internet se compone del nombre del computador, el sitio al que pertenece, el dominio organizativo y el dominio geográfico. Por razones obvias, las direcciones no pueden ser exactamente iguales y por ende hay que desechar la idea de que, para que haya competencia desleal, la similitud debe ser idéntica. La dirección de la actora contiene la marca registrada “TravelWeb” y la demandada la incluye en sus diversas páginas de internet. Carece de importancia, por lo tanto, si se trata o no de palabras de fantasía o genéricas. Lo que se protege es su inscripción con anterioridad a favor de la actora, sin que la accionada pueda utilizarla de alguna manera dentro de los mismos servicios que brinda internet. Incluso, la inscripción del dominio en la Academia Nacional de Ciencias no le concede a la accionada ningún derecho frente a la demandante. En primer lugar, la inscripción se realiza en una institución distinta al Registro la Propiedad Intelectual, además se hace con posterioridad y apenas unos días antes de presentarse esta demanda. La Ley de Creación de la Academia Nacional de Ciencias, número 7544 publicada en el Diario La Gaceta número 217 de 15 de noviembre de 1995, no exige dentro

de su articulado la obligación de inscribir los dominios y, menos aún, contiene derechos expresos a favor de quien lo hace. Es una institución de derecho público no estatal y dentro de sus objetivos, entre otros, debe promover la investigación científica y el desarrollo tecnológico del país (inciso a. Del artículo 3º). No es un instituto registral que supere o deje sin efecto al Registro de la Propiedad Intelectual, sino que tiende a promover y ordenar el quehacer tecnológico. Lo conveniente es que ambas instituciones mantengan una estrecha coordinación cuando se trata de inscribir marcas o reservar dominios que puedan causar confusión y discusiones en el campo de la competencia desleal. Por lo pronto, la actora inscribió en el Registro de la Propiedad Intelectual y en otros países, lo que no sucede con la demandada a pesar de ocurrido en la Academia Nacional de Ciencias. En cuanto a la existencia de un daño efectivo o amenaza de daño comprobado, estima el Tribunal que es inherente a los actos prohibidos que se han acreditado, es especial es razonable la amenaza que se produce ante la complejidad de los servicios de internet. El sistema es visitado por millones de personas y los servicios de turismo llaman la atención a los viajeros por la facilidad de encontrar valiosa información. Ahora bien, es cierto que el a-quo rechazo el extremo petitorio de condenar a la parte demandada, pero ese pronunciamiento no implica que no se haya incurrido en actos prohibidos. De todos modos, el Tribunal no puede abordar ese punto porque su denegatoria beneficia a demandada como única apelante y la actora se conformo con lo resuelto."

2 PROCURADURÍA GENERAL DE LA REPÚBLICA DE COSTA RICA

A.Firma electrónica herramienta de seguridad en el comercio electrónico

[PROCURADURÍA GENERAL DE LA REPÚBLICA DE COSTA RICA][2]

Como es harto conocido, el desarrollo de las comunicaciones, merced al uso generalizado de la computación e informática en toda actividad humana, ha revolucionado favorablemente la vida de todos los ciudadanos. Hoy en día difícilmente existe persona que a diario no tenga contacto con las computadoras, de manera directa o indirecta. Además, el impulso que en materia educativa han tenido las nuevas generaciones, aunado al enorme mercado que representa

esta nueva disciplina y la constancia demostrada por los profesionales en la materia, han llevado a nuestro país a una situación realmente ventajosa en materia informática, siendo por ello muy común que prácticamente cualquier persona, con un buen nivel de conocimiento en el campo computacional, esté en posibilidad de accesar las bases de datos disponibles. No es casualidad que nuestro país tenga uno de los porcentajes más altos en cuanto a cantidad de microcomputadoras por habitante en toda América Latina. Igualmente, el acceso tanto a redes locales como a la red internacional Internet está bastante generalizado y es mucho mayor del que indican las cifras oficiales.

Ese acceso constante a la conexión "en línea", aunado al giro evidente que han tomado las relaciones comerciales en la llamada "nueva economía" mediante el intenso comercio electrónico, la apertura de mayores y más variados mercados y la confirmación realista de que día a día se producen contratos informáticos, provoca que muchas personas y entidades requieran de una herramienta confiable para llevar a cabo sus transacciones comerciales con seguridad jurídica y certeza personal. Se trata, pues, de imprimir un grado mayor de seguridad no sólo en las relaciones comerciales cotidianas, sino también, y mayormente, en las relaciones jurídicas de los ciudadanos donde se requiera contar con elementos de confianza que permitan llevar a cabo actos personales con efectos jurídicos válidos. A fin de cuentas, de lo que se trata es de que la firma electrónica y los documentos que certifica tengan validez legal y surtan efectos probatorios ante las autoridades e instituciones públicas o en estrados judiciales. Por supuesto, el principal beneficiado será el ciudadano común, quien podría contar con estos nuevos instrumentos de seguridad y ya de uso general.

Unas de las características de los elementos electromagnéticos es su fragilidad. Los datos guardados y las transacciones que sobre ellos se realizan, en tanto registros magnéticos u ópticos sobre superficies metálicas o vinílicas, son sumamente frágiles y de fácil manipulación o incluso anulación, lo que implica que cualquier particular que tenga acceso a ellos podría dañarlos o hacerlos desaparecer sin dejar el menor rastro y sin la menor posibilidad de recuperación. Además, debemos adicionar que las telecomunicaciones son harto falibles, susceptibles de ser intervenidas, interrumpidas o desviadas sin que el ciudadano tenga el menor conocimiento de ello. Esta circunstancia en particular se produce debido a que las tecnologías computacionales y su

consecuente rasgo de procurar las comunicaciones telemáticas, han aprovechado intensamente la infraestructura telefónica instalada. De esta forma, el acceso a los sistemas de información mediante líneas de cobre se convirtió en la manera más utilizada de conexión remota, circunstancia que no podía ser de otra forma, pues era el medio que mejor se adaptaba a las necesidades de comunicación existentes. El mismo argumento puede aplicarse a otros métodos de comunicación utilizados en la actualidad, como los cables coaxiales y las transmisiones inalámbricas.

Con la creación de un mecanismo tan necesario como la firma electrónica, no sólo el comercio electrónico se vería beneficiado y estimulado, sino actividades tan importantes como las investigaciones, la seguridad, la salud pública, los procesos judiciales o profesiones liberales como el notariado, pues la firma electrónica iría de la mano de institutos tan novedosos como el protocolo electrónico, el expediente electrónico, etc. los cuales ya no tendrían barreras para una cabal existencia y aplicación en nuestro país.

II.-

"Firma electrónica" y "firma electrónica avanzada".-

El proyecto de ley habla de "firma digital", expresión que no consideramos la más feliz. La razón por la cual adversamos de la utilización del término "firma digital" es porque hemos considerado que puede traer confusión con el concepto y práctica de la "firma digitalizada", es decir, la firma manuscrita que es recuperada en formato digital mediante la utilización de un lector óptico ("scanner"), el cual recoge elementos cualesquiera del exterior para convertirlas en imágenes visibles dentro de un sistema de cómputo e imprimibles adjuntas con documentos.

La noción de "firma electrónica" es bastante más precisa y atañe más a la estructura física y naturaleza tecnológica de la herramienta que se utiliza para ese propósito. Lo propio puede verse en concepciones temáticas como "correo electrónico", "expediente electrónico", "comercio electrónico" o "documento electrónico". Este concepto es más utilizado en la legislación

europea, donde ha tenido un desarrollo legislativo importante desde hace varios años. Sin embargo, en América Latina ha calado más la utilización del término "firma digital", lo que no deja de producir confusiones como las expresadas y otras más. (1)

_____

(1) Si bien algún autor se esfuerza por diferenciar entre el concepto de "firma electrónica" y "firma digital" (tomando ésta como un elemento superior y continente de la firma electrónica avanzada), para efectos prácticos, hemos decidido respetar en lo posible la terminología utilizada en el proyecto de ley, entendiendo una y otra expresión como sinónimos. No obstante, nuestra inquietud y propuesta queda planteada en este acto.

El novedoso instituto de la firma electrónica, término correcto a nuestro parecer según explicamos supra, lo definimos como el sistema tecnológico cierto que tiene la función de identificar de manera única y lógica al remitente de un mensaje en conjunto con los documentos electrónicos que desee adjuntar, expresando así su conocimiento y voluntad de ejecutar una conducta y ser destinatario de los efectos jurídicos de ella, mediante la utilización de programas de cómputo y herramientas de comunicación jurídicamente aprobados y técnicamente confiables. Es decir, la firma digital estará llamada a individualizar y vincular, de manera cierta y unívoca, el mensaje y los documentos enviados por la persona titular de una cuenta electrónica personal.

No se trata, pues, de una simple firma manuscrita que se digitaliza y luego puede reproducirse como una imagen e insertarse dentro de un texto, como es usualmente la creencia popular.

La firma digital constituye la expresión de una manifestación de voluntad que se da a conocer por un medio distinto del manuscrito, esto es, a través de una herramienta tecnológica que es puede ser manipulada únicamente por el titular del derecho para declarar su voluntad de una manera y en un sitio distinto del que físicamente podría encontrarse ubicado aquél.

Se trata sobre todo de un instrumento electrónico elaborado mediante tecnología segura y no susceptible de manipulación externa cuya función es primordialmente identificadora de la persona que utiliza un sistema de comunicación remoto y desea certificar que es ella, y no otra persona, quien está enviando un

mensaje o documentos ciertos, o bien, que desea manifestar su voluntad y obligarse en cierta relación contractual. Tal es la analogía con la noción de "firma" manuscrita, dado que ésta cumple precisamente la función de identificar a la persona que la imprime en un documento que tendrá efectos legales relevantes. Es el único contexto donde ambos conceptos tienen similitud. Por demás, los procedimientos para hacer valer una u otra son diametralmente distintos.

Ahora, con miras a asegurar aún más los efectos jurídicos de la firma electrónica, se creó la noción de "firma electrónica avanzada", concepto un tanto innecesario si se piensa que este instituto jurídico-tecnológico fue ideado precisamente con el deseo de que tuviese la naturaleza de instrumento identificador sin reparos que expresamos en los párrafos anteriores. Es decir, no tiene sentido que exista un sistema de firma digital de mayor o menor confianza, sino que debería ser una herramienta única, de iguales características.

La firma digital avanzada, de acuerdo con los conceptos generalmente aceptados, debe tener al menos cuatro características:

1.

estar vinculada de manera única al firmante;

2.

permitir la identificación del firmante;

3.

haber sido creada utilizando medios que el firmante pueda mantener bajo su exclusivo control; y

4.

estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior en éstos sea detectable. (2)

---

(2) Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, artículo 2, definición de "Firma electrónica avanzada". Publicado en el Diario Oficial de las Comunidades Europeas de 19 de enero de 2000.

Cabe aclarar que ese concepto no es propio de la legislación del Viejo Mundo, sino que es constante en la doctrina iusinformática. En este caso, la normativa europea no ha hecho sino recoger el concepto técnico ya existente y reconocido por los especialistas en la materia. En el mismo sentido, véase el Proyecto de guía para la incorporación al Derecho Interno de la Ley Modelo de la CNUDMI para las Firmas Electrónicas, elaborado por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (Grupo de trabajo sobre Comercio Electrónico). New York, 23-30 marzo de 2001, documento a/cn.9/wg.IV/wp.88.

Para efectos del presente proyecto de ley, creemos conveniente mencionar en qué consisten cada uno de los elementos de la firma electrónica avanzada, de manera que el legislador los tenga en cuenta a la hora de completar y sancionar en definitiva el contenido de las normas que regirán la materia. Todas ellas guardan una muy estrecha relación entre sí, pero se hace necesario individualizarlas en aras de una mejor comprensión de su contenido.

a) Vinculación de la firma electrónica de manera única con el firmante.-

El primer requisito que se exige de la firma electrónica avanzada es que debe estar vinculada de manera única con el firmante del mensaje y de los datos que se anexen, si éstos existen. El remitente actúa y se obliga, en principio, en su nombre o como representante de una persona moral sobre la que ejerza la representación judicial o extrajudicial, o como apoderado de un tercero.

Ahora bien, dicha vinculación se verá cristalizada en la persona que tenga la facultad de contar con el medio capaz de

creación de firmas electrónicas. Es decir, el remitente debe contar con un medio tecnológico (programa de cómputo creado al efecto o algún otro dispositivo de seguridad para identificación personal, o bien, la palabra de paso o clave privada) que le permita el envío de correspondencia y documentos por vía remota y por tanto la posibilidad de ser identificado sin lugar a dudas.

El objetivo es este último, es decir, poder individualizar al remitente de un mensaje, ya sea para una obligación comercial, algún trámite formal, escritura pública, etc. Técnicamente, la forma como puede llevarse a cabo este proceso de reconocimiento personal sería a través de un certificado digital debidamente acreditado y emitido por una autoridad certificadora de servicios de esta naturaleza.

Resulta conveniente explicar brevemente en qué consiste el certificado digital, tanto desde el punto de vista formal como material. Formalmente, el certificado digital sería simplemente la constancia formal emitida por la autoridad certificadora donde se indiquen los datos precisos de la persona que vaya a hacer uso de una firma electrónica, incluyendo algún procedimiento mediante el cual éste pueda elaborar una firma personalísima y sólo conocida por él. No parece posible ni recomendable que corresponda a la entidad certificadora de datos el otorgar una clave secreta o llave de paso para uso del firmante, sino que es éste, y no otro, quien debe crearla.

Desde el punto de vista técnico, el certificado digital consiste en una estructura algorítmica de datos, única e irrepetible, que sirve para vincular una firma electrónica a un firmante, no sólo para el uso de la llave secreta que puede utilizar para el cifrado de documentos y envío de mensajes, sino también para ser aplicada a los destinatarios que deseen decodificar la información remitida por el firmante a ellos.(3)

(3) Obsérvese la alusión directa al sistema de llave pública y llave privada, pues es el sistema más utilizado y confiable para la aplicación efectiva de la firma electrónica. Si bien el proyecto de ley no lo menciona (pues existen posiciones en el sentido de que se trataría de una violación al principio de neutralidad tecnológica) es lo cierto que las legislaciones que regulan la firma electrónica incluyen la infraestructura de llave pública como requisito fundamental para el instituto de la firma

digital.

a. Identificación del firmante.-

Se busca identificar de manera unívoca a la persona que se obliga en una relación jurídica. Este es, si se quiere, la razón de ser, por antonomasia, de la firma electrónica en general, pues tanto la firma común como la avanzada lo establecen en su definición.

Ahora, es importante es que el destinatario conozca la manera de descifrar el mensaje, no sólo por la obvia razón de poder conocer su contenido, sino además para asegurarse de que el remitente es quien dice su firma que es. En este punto es cuando se cumple plenamente el requisito de individualización del remitente, es decir, cuando el destinatario constata que efectivamente el mensaje llegado a su cuenta electrónica ha podido ser abierto, descifrado y constatado que el origen de los datos es un sujeto cierto con capacidad de actuar.

No obstante tan lógica posición, es necesario contar con un sistema de identificación personal, único y seguro. En este caso, pensamos en un estado anterior al de la creación de la firma electrónica, pues ésta sería ya una consecuencia de la existencia de un elemento o varios que funcionen como identificadores personales. En este caso, pensamos en instrumentos electrónicos de medición biométrica, como las huellas digitales, huellas de la palma de la mano, iris del ojo, timbre de voz, etc., es decir, componentes que son absolutamente individuales en una persona y, por ello, irrepetibles y físicamente irreproducibles.

Igualmente podría ser algún otro elemento menos sofisticado, como una tarjeta con un chip de información incorporado o una simple banda magnética que se deslice entre una ranura para decodificar su contenido, o bien, una palabra clave, un número personal de identificación o una llave privada, siempre con los mismos propósitos de reconocimiento personal. Estas son las formas actuales en que puede llevarse a cabo la cabal identificación de una persona, ya no sólo para los propósitos de la firma electrónica, sino en general, en el ámbito cotidiano. No

obstante, el cumplimiento de este requisito no basta para afirmar que nos encontramos ante la posibilidad de aplicar a plenitud el concepto de firma electrónica avanzada.

c) Creación de la firma utilizando medios que el firmante pueda mantener bajo su exclusivo control.-

Como tercer requisito, se espera que el firmante utilice medios de creación de firmas que sólo él haya operado o que le pertenezcan intrínsecamente, es decir, que le puedan ser propios.

Dichos medios pueden ser de creación lógica o captación biométrica, de acuerdo con lo mencionado antes. En ambos casos, pensamos en un dispositivo de captura o programa de cómputo particular con la facultad no sólo de crear y certificar la validez de una firma, sino también de brindarle al usuario la posibilidad de crearla y certificar que él es efectivamente el remitente quien dice su firma electrónica que es.

En la primera alternativa, el programa de cómputo dará como producto la posibilidad de crear un algoritmo prácticamente irrepetible, unido a un individuo en particular y elaborado por éste. En este caso, el remitente deberá poder crear y enviar sus mensajes y documentos anejos con la garantía de que el programa utilizado para crear y registrar su firma ha realizado una secuencia lógica de instrucciones que garanticen al destinatario la integridad de los mensajes y documentos que reciba, así como la identificación del remitente.

Se trata, pues, de que no sea un tercero (autoridad certificadora o alguna otra entidad) quien tenga la posibilidad de crear la firma para el usuario, ni tampoco tener dominio o control sobre la forma en que el interesado pueda identificarse, enviar documentos o remitirlos. En este caso, se hace necesario que el usuario tenga bajo su poder algún dispositivo personal de seguridad para asegurar el envío e identificación cierta del mensaje.

Dicho dispositivo no puede ser otro, de acuerdo con el

estado actual de la tecnología, que alguna palabra de paso o clave de llave privada permita el envío efectivo de mensajes y documentos debidamente identificados.

Una segunda alternativa de identificación puede ser la de tipo biométrico (4), según se indicó antes, es decir, dispositivos electrónicos que tengan la capacidad de captar e individualizar a sujetos según sus características corporales, tales como huellas digitales, iris oculares, facciones del rostro, timbre de voz, etc. En este caso, sólo la persona que efectivamente tenga el perfil físico predeterminado por los registros magnéticos del programa podrá enviar mensajes y documentos firmados electrónicamente a nombre personal.

_____

(4) Hemos visto que la posibilidad de utilizar tecnología biométrica está mencionada en el proyecto de ley, lo cual le brinda una mayor gama de posibilidades de identificación personal al usuario final.

Se busca, entonces, que esa palabra clave, llave privada o identificador personalísimo sean creados por y estén a disposición del usuario del servicio, no por un tercero. Necesariamente, sin este requisito, no podríamos estar frente a una firma electrónica confiable, pues perfectamente el titular de ella argüiría que su llave privada no está totalmente en sus manos, sino que existen terceros con la facultad de crearla o disponer de ella sin su consentimiento. Sería, pues, una causal de extinción de la responsabilidad del remitente, pues éste bien puede alegar que no ha sido él el verdadero firmante.

d) Detección posterior de cambios en el mensaje o en los datos adjuntos.-

Esta última exigencia es harto indispensable. El objetivo final consiste en proteger la integridad del mensaje y los documentos incluidos en él. Una forma de lograrlo es mediante la detección de algún cambio en su contenido. Así, en caso de intercepción del mensaje entre el remitente y el destinatario, debe ser posible la detección de cualquier modificación en él, de manera que el firmante pueda mantener su compromiso y que se mantenga su vinculación con el mensaje. Si existieren modificaciones, el documento ya no sería íntegro y tal panorama relevaría automáticamente al remitente de cualquier

responsabilidad jurídica sobre él, en virtud de que el contenido del mensaje podría ya no representar la voluntad del sujeto. Ahora bien, la forma como técnicamente puede detectarse un cambio en el mensaje o documentos enviados dependerá de la tecnología programática que se utilice para ello, ya sea en la confrontación de la clave privada, algún resumen algorítmico particular elaborado por el mismo programa o alguna otra alternativa que garantice este resultado, derivada de la experiencia o la visión de los estrategas expertos en seguridad y comunicaciones, pero necesariamente existente en el programa.

III.-

Conveniencia de incorporar la firma electrónica avanzada.-

Obsérvese que la llamada "firma digital avanzada" contiene en su conceptualización los elementos de control indispensables por parte del titular del derecho para la creación de la firma, el contenido del mensaje y de los datos que desee transmitir. La identificación del firmante es consecuencia obligada de los otros tres requisitos.

Tal concepto de firma electrónica avanzada, pues, incorpora importantes elementos seguridad personal que son notorios al momento de creación de la propia firma. El primer requisito es, entonces, efecto del tercero, es decir, el firmante, al crear su firma virtual de identificación, no puede depender de terceros para su validación técnica, sino que se trata de un proceso que dependerá de la voluntad de usuario para crearlo, utilizando medios tecnológicos adecuados y confiables para ese fin. Si se quiere, este punto es el más importante, pues inicia con la noción de la voluntad del firmante como centro obligado sobre el que giran los otros factores: creación de la firma, vinculación de datos, control del proceso, liga directa con el sujeto, posibilidad de detección de cambios, etc. El firmante es el elemento principal en la firma digital avanzada.

Confróntese con la definición acartonada y convencional que usualmente se maneja de "firma digital", la cual simplemente hace referencia al anexo de datos dentro de un mensaje y la

identificación del usuario. Nada más. No parece existir el control deseable o esperado por parte del firmante, ni se hace depender la existencia o no de una firma de la voluntad de él, en los términos que considere apropiados. De allí que resulte riesgoso utilizar ese concepto limitativo sin tener claras las consecuencias que puede traer: la firma digital como tal no puede tener los efectos jurídicos que sí posee la "firma digital avanzada", a menos que, por convención legislativa, se le otorgue a aquélla el mismo contenido, la misma protección técnica y los mismos efectos jurídicos que a ésta.

Ahora, ¿significa esto que la firma digital avanzada es más segura, en términos técnicos, que la firma digital común? En realidad, desde el punto de vista tecnológico y según las herramientas computacionales que se utilicen, ambas podrían tener el mismo nivel de seguridad. La diferencia entre una y otra dependerá básicamente del grado de intervención que pueda tener el usuario en su creación y el respaldo formal que las autoridades acreditadoras establezcan para ello.

Precisamente, el primer punto que llama la atención en el proyecto de ley es que se echa de menos la utilización de los términos "firma digital", pura y simple, y "firma digital avanzada". De hecho, esta última ni siguiera se menciona (como sí ocurría en el proyecto original, aunque de manera muy confusa).

En cambio, en este nuevo proyecto de ley se nos presenta un concepto de naturaleza eminentemente formal, bastante novedoso, denominado "firma digital acreditada", que resulta insuficiente y no llega a llenar el vacío conceptual presente en el proyecto de ley. Esto debe corregirse para que se muestre siempre una terminología uniforme y unívoca.

Nuestra siguiente recomendación es, pues, que el texto del proyecto de ley se ajuste en su concepción y contenido al concepto de "firma digital avanzada", con los efectos técnicos que dicha definición implica. Si bien dentro de los principios de Derecho Informático se habla de la necesidad de que las normas jurídicas sean "tecnológicamente neutras", es este caso la aplicación de aquélla noción no compromete el texto del proyecto ni lo limita o lo condiciona a la existencia de cierta tecnología en particular. (5)

(5) Resulta saludable a todas luces la aplicación del principio de neutralidad tecnológica en la redacción de los proyectos de ley de cualquier naturaleza. Las razones son bastantes variadas. Entre ellas, podemos anotar la importancia de no favorecer a un proveedor de servicios en particular o la característica esencial de la tecnología, que siempre está en perenne innovación, no así la legislación, la cual usualmente requiere de largos y tediosos trámites para su aprobación. En ese sentido, cualquier modificación en el acervo o en la mecánica tecnológica convertiría una norma en inaplicable. Ejemplo de ello puede ser el tipo penal que protege las comunicaciones telegráficas, ya casi en desuso. En cambio, leyes esenciales de protección tecnológica, como la aprobación de normas que sancionaren los delitos informáticos, a pesar de la necesidad manifiesta desde años atrás, o bien, los tratados internacionales de telecomunicaciones, usualmente tardan años antes de ser siquiera conocidas por el legislador. De esta manera, los términos de la norma son suficientemente amplios para que, independientemente de la tecnología que se aplique, puedan ser aplicables en cualquier supuesto de hecho. De allí la práctica de dejar la materia técnica como delegación para el Poder Ejecutivo en el reglamento de la norma, el cual usualmente recoge la letra menuda de la materia que se quiera regular. Por demás, la aprobación de reglamento es más ágil y su nivel de tecnicidad escapa de las decisiones no estructuradas que corresponden al legislador.

En la misma línea de pensamiento, es aconsejable que la expresión "firma digital", mencionada en el artículo primero del proyecto, se utilice en el texto como sinónimo de "firma digital avanzada", con todos los efectos que la propia ley le otorgaría. Esta disposición podría estar inserta dentro del artículo primero o algún otro numeral inicial que pretenda tener efectos aclaratorios o restrictivos, de manera que pueda salvarse cualquier omisión o que pueda ocurrir algún error de interpretación a la hora de aplicar la norma.

IV.-

La firma electrónica y el documento electrónico.-

El concepto y aplicación de la firma electrónica va unido necesariamente al documento electrónico. Es decir, la firma electrónica puede llegar a carecer de sentido si no va unida a un documento, tal y como ocurre en la realidad con la firma manuscrita y el documento de papel. Una y otra mantienen una relación natural que le da sentido lógico. Más aún, el propio concepto que se utiliza en el artículo 2 del proyecto señala que la firma digital funciona como "un conjunto de datos asociados funcionalmente a un documento electrónico". En el artículo 2 del proyecto de ley se da una definición de "documento electrónico", señalado como "toda representación electrónica de actos, hechos, datos o descripciones, y que se puede recuperar o reproducir en una forma perceptible e inteligible."

Concordamos en que se trata de una buena definición, pues contiene los elementos básicos del concepto. No obstante, puede ser insuficiente si la comparamos con otras leyes que figuran y están vigentes en el ordenamiento jurídico nacional. Existen diversas normas jurídicas que hacen referencia al "documento" en sentido amplio, abarcando también los diferentes soportes en que puede contenerlo. Es decir, el documento no es sólo el contenido de datos e información, sino también el elemento material sobre el que se transporta, sea este de tipo magnético, óptico o electrónico, etc.

Nos hemos permitido citar las normas que tratan sobre el documento en general, con miras a que se tengan como fundamento jurídicos y concordancia para la definición que se acompaña en el proyecto de ley en análisis. Advertimos que no se trata de un análisis de su contenido, sino tan sólo una referencia que consideramos obligatoria con miras a lograr una armonización de los conceptos que se plasman en diferentes cuerpos normativos. Este proyecto de ley no puede ser la excepción.

Por su importancia procesal, citaremos primeramente la Ley Orgánica del Poder Judicial No.7333 de 5 de mayo de 1993, artículo 6 bis, que contiene una serie de disposiciones muy avanzadas en materia de documentos electrónicos y utilización de ellos como medio de prueba:

"Artículo 6 bis.-

Tendrán la validez y eficacia de un documento físico original, los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos o producidos por nuevas tecnologías, destinados a la tramitación judicial, ya sea que contengan actos o resoluciones judiciales. Lo anterior siempre que cumplan con los procedimientos establecidos para garantizar su autenticidad, integridad y seguridad.

Las alteraciones que afecten la autenticidad o integridad de dichos soportes los harán perder el valor jurídico que se les otorga en el párrafo anterior.

Cuando un juez utilice los medios indicados en el primer párrafo de este artículo, para consignar sus actos o resoluciones, los medios de protección del sistema resultan suficientes para acreditar la autenticidad, aunque no se impriman en papel ni sean firmados.

Las autoridades judiciales podrán utilizar los medios referidos para comunicarse oficialmente entre sí, remitiéndose informes, comisiones y cualquier otra documentación. Las partes también podrán utilizar esos medios para presentar sus solicitudes y recursos a los tribunales, siempre que remitan el documento original dentro de los tres días siguientes, en cuyo caso la presentación de la petición o recurso se tendrá como realizada en el momento de recibida la primera comunicación.

La Corte Suprema de Justicia dictará los reglamentos necesarios para normar el envío, recepción, trámite y almacenamiento de los citados medios; para garantizar su seguridad y conservación; así como para determinar el acceso del público a la información contenida en las bases de datos, conforme a la ley."

(Así adicionado este artículo por el numeral 9 de la Ley de Reorganización Judicial Nº 7728 de 15 de diciembre de 1997. Los subrayados no son del original)

Otras normas de importancia se encuentran contenidas en el Código Procesal Civil No.7130 de 16 de agosto de 1989. Al respecto, recomendamos la lectura de los artículos 368 y siguientes, que contienen regulaciones atinentes a tema de los documentos y su aplicación procesal. Concretamente, el numeral 368

indica:

"ARTICULO 368.-

Distintas clases de documentos.

Son documentos los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y, en general, todo objeto mueble que tenga carácter representativo o declarativo."

Otra norma de gran relevancia en el tema de los documentos es la Ley de registro, secuestro y examen de documentos privados e intervención de las comunicaciones No.7425 de 9 de agosto de 1994. Esta ley es de referencia obligatoria pues, en su artículo primero concibe al documento con carácter amplio. Allí, se consideran documentos privados "la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los vídeos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo".

"ARTICULO 1.-

Competencia.

Los Tribunales de Justicia podrán autorizar el registro, el secuestro o el examen de cualquier documento privado, cuando sea absolutamente indispensable para esclarecer asuntos penales sometidos a su conocimiento. Para los efectos de esta ley, se consideran documentos privados: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representantivo o declarativo, para ilustrar o comprobar algo."

Este concepto amplio de "documento" tendrá sentido para esta visión de los nuevos instrumentos de seguridad en las comunicaciones siempre y cuando se trate de elementos no materiales, es decir, que dichos "documentos" se encuentren registrados en soportes magnéticos u ópticos susceptibles de ser almacenados, enviados o recibidos por usuarios remotos. Conviene que se haga constar esta circunstancia limitativa en los términos finales de aprobación.

De acuerdo con las normas citadas, y en aras de lograr uniformidad y concordancia con la legislación vigente, sugerimos que se tome en cuenta los conceptos que sobre documento recoge la legislación costarricense.

En otro orden de cosas, existe un tipo de documento electrónico que no se menciona en la legislación, pero que es de los más utilizados por la ciudadanía. En efecto, dentro de los documentos y formas de comunicación con que cuenta el ciudadano, requiere particular mención el correo electrónico, el cual constituye en la actualidad una de las principales formas de comunicación privada. Su costo ínfimo, la facilidad de uso y aprendizaje para enviar y recibir mensajes, la existencia de servicios de correo electrónico gratuitos, la enorme extensión territorial que abarca (pues puede ser consultado desde casi cualquier punto del planeta donde exista una línea telefónica), así como el abanico de posibilidades presentes y futuras, hacen de este servicio de comunicación el sustento de un bien jurídico de urgente protección.

Ahora bien, como todo correo electrónico utiliza, en principio, cables de cobre o coaxiales (de fácil intercepción) y su protección lógica suele ser simplemente un nombre de usuario y una palabra de acceso, la posibilidad de vulnerar este servicio de comunicación puede ser sumamente alta. Igualmente, se ha utilizado exitosamente para difundir "virus" informáticos que han ocasionado cuantiosos daños a muchas microcomputadoras y servidores alrededor del mundo.

No se requiere de grandes conocimientos técnicos para lograr un resultado exitoso, sino tan sólo conseguir el nombre de usuario y palabra clave de la víctima. Más aún, la interceptación de los

mensajes de correo electrónico no necesariamente debe darse en el transcurso de la comunicación, sino directamente en su fuente (el servidor de correo), pues los programas utilizados dan la posibilidad de extraer directamente la información, dejando una copia del correo en el servidor, con lo que el ofendido jamás se enteraría de que sus mensajes o documentos anejos a éste están siendo captados o difundidos sin su consentimiento. (6)

_____

(6) En este sentido, véase la opinión jurídica No.154-2001 de 22 de octubre de 2001, referente al proyecto de ley sobre delitos informáticos.

La utilización de la firma electrónica en los mensajes de correo sería una garantía, tanto para el remitente como para el destinatario, de que la información que se esté enviando o recibiendo por ese medio es confiable y ha sido efectivamente enviado por el firmante del documento y no por un tercero interceptor del correo. No cabe duda de que, con el estado actual de la tecnología, los programas y usuarios correos electrónicos serían los principales beneficiados con la implantación de un sistema de firmas electrónicas debidamente acreditadas.

V.-

Necesidad de proteger los documentos electrónicos.-

En general, es necesario que los usuarios de servicios de comunicación electrónicos, sean estos particulares o entidades comerciales, mantengan una comunicación fluida entre sí y también con personas jurídicas particulares u órganos públicos. Parece lógico pensar que, en las ocasiones en que ello sea necesario y atendiendo a las especiales características personales u organizativas y de la naturaleza de la información que se desee enviar, se requiera de especial reserva para las comunicaciones, especialmente las que se efectúen por medios remotos. Pensamos en información particularmente delicada, como serían las transacciones financieras, palabras claves, nombres de usuarios, información de cierto rango jerárquico, datos concernientes a las características personales, etc. Se busca que, sin menoscabar la agilidad de las comunicaciones del usuario, éste pueda

garantizarse un nivel alto de seguridad al momento de efectuarlas o recibirlas. Por ello, parece factible que el interesado pueda valerse de métodos manuales o automatizados para lograr el fin que se propone, además del uso normal de la firma electrónica.

Para aplicar esta plataforma de seguridad, el firmante dispone de variados métodos que deben estar sustentados e incluidos en un sistema de firma electrónica moderno, automático, donde la intervención humana sea mínima, de manera que la garantía de seguridad sea muchísimo más elevada.

Por otra parte, y a modo meramente ilustrativo, deseamos exponer brevemente una forma en que la entidad podría lograr un nivel bastante alto de seguridad y privacidad. Nos referimos a la utilización de lenguaje secreto o encriptado, que consideramos de suma utilidad en transmisiones que utilicen líneas de cobre u ondas expansivas en sus comunicaciones, además de la posibilidad del uso de cifras, claves, etc. para lograr absoluta reserva en el transporte resguardo de información confidencial previamente digitada en un procesador de textos u algún otro programa de cómputo diseñado al efecto. Para ello, debemos remitirnos a los sistemas informáticos por medio de los cuales el interesado puede realizar la conversión de documentos confidenciales. Dicha conversión puede tener al menos dos formas: a la primera se le llama comprensión y consiste en comprimir la información de un documento, en forma tal que éste se reduzca al mínimo posible de su volumen real y añadiendo una palabra clave para su descompresión. Ello hace posible el transporte de una gran cantidad de información en espacios pequeños o a velocidades superiores que el envío del documento en su tamaño original. Tiene la ventaja adicional que sólo descomprimiéndolo podrá verse cuál es la información que contiene y, para ello, el interesado deberá saber cuál es la palabra clave para hacerlo. Es poco lo que hay que decir para justificar y darse cuenta de las grandes ventajas que posee una aplicación programática como la descrita dentro de la firma digital, tanto para el usuario que necesite almacenar grandes cantidades de datos en espacios pequeños como para quien busque resguardar o transportar información confidencial de forma que sólo ella o las personas a las que designe puedan recuperar y aprovechar esas comunicaciones.

El segundo proceso que puede darse con una información para ocultar su contenido se llama encriptación y consiste en transformar los caracteres de un texto electrónico a un "lenguaje"

ilegible o incomprensible para el ojo humano, mediante la utilización de un programa de cómputo creado al efecto. El procedimiento es bastante simple y creemos necesario que esté incluido en las aplicaciones de manejo de firma electrónica como garantía adicional de seguridad e integridad del mensaje en su recorrido al destinatario.

Una ventaja adicional que poseen estos programas de comprensión y encriptación es que, al no ser excluyentes entre sí, pueden ser utilizados simultáneamente.

Este procedimiento viene ya incorporado en los principales programas que utilicen la firma electrónica, en la denominada clave privada, por lo que, al hablar del uso de la firma electrónica, se está incluyendo la utilización de algoritmos de encriptación tanto para el mensaje como para los documentos anejos.

VI.-

Comentarios al proyecto de ley de firma electrónica.-

Si bien hemos efectuado algunas observaciones generales y recomendaciones al proyecto de ley, creemos pertinente hacer una serie de observaciones más puntuales, tomando como base el articulado del texto. Advertimos que los errores filológicos, referentes a la sintaxis, gramaticales, mal uso de preposiciones, etc., no serán mencionados, pues corresponderá al departamento legislativo pertinente ocuparse de ellos.

1.-

Necesidad de utilizar descriptores temáticos.-

En general, la estructura del proyecto de Ley de Firma Digital, el cual se encuentra dividido en Capítulos, resulta

adecuada, pues se trata de un grupo pequeño de artículos, ahora con menos de treinta numerales, tomando en cuenta que podrían eliminarse algunos y es posible que se agreguen o desaparezcan otros más. No es necesario crear Títulos, pues no se trata de un Código u otro cuerpo normativo voluminoso y con temáticas diversas, sino que este proyecto trata, a lo sumo, de dos temas nada más (firma electrónica y certificados digitales) que se hayan tan correlacionadas que no amerita esta división. Este era el caso del proyecto de ley anterior, y observamos con agrado que se ha simplificado bastante.

Nuestra recomendación es, pues, mantener al máximo una estructura formal simplificada del proyecto, dándole mayor énfasis a la existencia de descriptores temáticos que indique el contenido de cada numeral, como una especie de epígrafe al inicio de cada artículo. Ejemplo de ello puede verse en el Código Penal o en las leyes aprobadas después de 1996, todas las cuales llevan en sus numerales algún descriptor inicial y orientador para el consultante del contenido del numeral. Esta recomendación va en concordancia con las tendencias actuales en materia de ordenación de los datos e información y el uso extensivo de tesauros en muchas disciplinas, especialmente en la emisión de normas jurídicas.

2.-

Comentario al artículo 1.-

En el artículo 1 se menciona, con buen tino, la posibilidad de autorizar al Estado para la utilización de la firma electrónica. Nos obstante, resulta conveniente hacer una remisión directa al artículo 6 del proyecto de ley, para que se entienda que el término "Estado" se está utilizando de manera amplia, no sólo al Estado central o en el sentido que normalmente se utiliza en la Ley General de Administración Pública o en la Ley de la Jurisdicción Contencioso-Administrativa. Podría ser una redacción de la forma que sigue, al final del articulo: "...de acuerdo con los alcances que se indican en el artículo 6 de esta ley.". Otra opción podría ser eliminar su mención en el artículo 1 y desarrollarlo más en el artículo 6.

3.-

Comentario al artículo 2.-

Parece existir una tendencia generalizada, aunque relativamente reciente, que se inclina a incluir conceptos y definiciones en las leyes. En el caso de los proyectos y leyes modelos de firma digital, hemos notado que siguen esa práctica, antes desconocida en nuestro medio, aunque justificable para ellos, pues se trata de presentar al interesado un panorama lo más completo posible sobre una materia en particular.

No obstante, consideramos que el texto de una ley común no es el apropiado para incluir conceptos, pues se trata de materia reglamentaria, más propia de la labor del Poder Ejecutivo. Por ello, recomendamos que el contenido del artículo 2 sea trasladado directamente al reglamento de la ley que elaborará el Poder Ejecutivo.

4.-

Conceptos incluidos en el artículo 2.-

En todo caso, deseamos plantear una serie de inquietudes sobre los conceptos incluidos en el artículo 2, pues en general no se limitan a la emisión de los alcances de los términos legislativos, sino que también incluyen regulaciones comunes, las cuales deberían estar en un numeral aparte, debidamente desarrollado.

- Acreditación:

En primer lugar, se habla del la "acreditación", haciendo depender su aplicación "de acuerdo a (sic) normas nacionales e internacionales". Infortunadamente, no se indican cuáles son esas normas nacionales o internacionales que podrían ser aplicables en nuestro país. Ahora, si se trata de leyes nacionales, deben indicarse exactamente cuáles son. En particular, debe tomarse en cuenta la Ley del sistema para la calidad No.8279 de 2 de mayo de 2002, según veremos, en lo que resulte pertinente.

En el caso de las normas internacionales, podríamos encontrarnos ante el curioso caso de reglas no aprobadas formalmente por la Asamblea Legislativa, pero con eventual fuerza de ley en el territorio. Creemos que ello no es posible: no puede inhibirse la labor del ente legislativo con la aplicación de tratados o normas de rango discutible. Si se trata de reglas técnicas o conceptos científicos aceptados internacionalmente, debería indicarse de esa manera.

- Acreditación "voluntaria":

Llama poderosamente la atención el uso del término "acreditación voluntaria", pues parece dar a entender que las entidades que se dediquen a la prestación de servicios de certificación tienen la potestad de acreditarse o no, es decir, la acreditación por parte de la Autoridad de Acreditación no sería requisito indispensable para el funcionamiento de ellas. Ignoramos si se trata de un error o un resabio del proyecto anterior pero, en todo caso, la palabra "voluntaria" debería ser eliminada, pues la acreditación debería ser siempre obligatoria.

- Datos de creación de firma:

Interesa aquí la segunda parte del párrafo, la cual indica que esos datos quedarán en entredicho si no han estado en control exclusivo del usuario. Este tipo de regulación no debe ir dentro de la parte de definiciones, sino en una artículo aparte, donde no sólo mencione la parte fundamental de la norma, sino además sus consecuencias.

- Documento "digital":

La definición "documento digital" que se utiliza, como sinónimo de documento electrónico con contenido codificado, es confusa. "Codificado" puede tener varios significados, y bien podría tomarse simplemente como equivalente a "magnético" o también como "encriptado", según vimos antes. Si es esta última definición, no nos explicamos de qué manera puede utilizarse. Ya indicamos antes que el procedimiento de encriptación de documentos viene ya incorporado en los principales programas que utilicen la firma electrónica, en la denominada clave privada, por lo que, al

hablar del uso de la firma electrónica, se está incluyendo la utilización de algoritmos de encriptación tanto para el mensaje como para los documentos que se adjunten.

La confusión se incrementa cuando de seguido se dice que, en general, "se utilizará el término digital entendido como cualquier información codificada en dígitos binarios".

Nuestra recomendación es que se aclare o se elimine ese término, o se cambie por otro más preciso, como sería "documento encriptado" o "documento protegido", si es ese el objetivo. En otras circunstancias causará mucha confusión. De hecho, pensamos que podría ser reiterativo el término de "documento digital" si tenemos el de "documento electrónico", pues se supone que todo documento firmado electrónicamente ya estará de por sí codificado, exigiendo esta posibilidad a la firma electrónica "acreditada".

- Firma digital "acreditada":

Ya hemos indicado antes nuestras reservas sobre la creación de este concepto de firma digital "acreditada", pues se trata de un concepto de naturaleza eminentemente formal. Es decir, se hace depender la eficacia de las normas de aspectos puramente formales, no de contenido. Esos elementos formales no mencionan reglas técnicas o tecnológicas que sustenten su fundamento. Aparentemente, el único requisito para la existencia de dicha firma es su acreditación ante la instancia correspondiente y nada más. El problema radica en que, si la acreditación se traduce en menos requisitos o un sistema de acreditación menos severo, igual estaríamos ante una firma digital válida, aunque ineficaz para los propósitos de seguridad en las comunicaciones. Como se ve, podría ser un portillo jurídico que desviaría este novedoso instituto de sus verdaderos propósitos. Nuestra recomendación es utilizar un único concepto de firma electrónica con todos los requisitos de seguridad necesarios. No es necesario la existencia de una firma digital "acreditada" pues, por su naturaleza, la firma electrónica siempre deberá estar acreditada ante una autoridad certificadora.

Parte de la gravedad de la orientación que se le da a esta normativa radica en la existencia de dos firmas: una acreditada y otra sin acreditar. Ello es contradictorio, pues ambas deberían estar sujetas a la misma regulación y a los mismos requisitos.

Sólo debería existir un tipo de firma electrónica, no una ordinaria, otra avanzada y otra más, acreditada. Esta posición que sustentamos ya la hemos señalado líneas atrás, al criticar la expresión "acreditación voluntaria". Véase además nuestro comentario sobre el artículo noveno del proyecto de comentario.

5.-

Comentario al artículo 3.-

Se menciona el principio de neutralidad tecnológica, de manera que los métodos de creación de firmas digitales, presentes y futuros, puedan estar incluidos en el sistema de acreditación nacional. Sólo restan dos observaciones.

La primera observación está en el uso del término "aplicación". Es decir, la norma indica que "ninguna de las disposiciones de la presente Ley (sic) será aplicada...", etc. Pensamos que lo correcto sería sustituir esa palabra por "interpretada", que recoge mejor el espíritu del legislador, o mejor aún, que se redacte como "...aplicada o interpretada..."

.

La segunda observación está referida a dicho principio de neutralidad. Es cierto que la ley debe ser tecnológicamente neutra, por las razones que anotamos en páginas anteriores. Sin embargo, sí se torna necesario que el reglamento a esta ley se autorice ciertas normas tecnológicas, tales como el sistema de llave pública y llave privada, pues es el método reconocido internacionalmente que actualmente recoge la parte medular de protección y aplicación de la firma electrónica. De hecho, en toda legislación actual, en la normativa europea e inclusive en las leyes tipo sobre firma digital, se tiene incorporado el sistema de llave pública y llave privada, sin que parezca comprometerse el principio de neutralidad tecnológica, pues éstas son complementarias de aquél. La recomendación de que se regule directamente en el reglamento que emitiría el Poder Ejecutivo obedece a la naturaleza técnica y ágil que usualmente caracteriza los reglamentos.

6.-

Comentario al artículo 4.-

Parece extraerse del proyecto de ley una actitud de apertura que permite la existencia de otros sistemas de firmas electrónicas que podrían funcionar sin la acreditación de la Autoridad Certificadora. Ello se ve en las definiciones indicadas antes, tales como "acreditación voluntaria", o en el artículo 9, donde deja en libertad a las partes para elegir un sistema de firma digital de acuerdo con sus intereses, o bien, en el presente artículo 4, párrafo tercero, que señala una presunción a favor de la firma electrónica emitida por un prestador de servicios de certificación autorizado. (7)

---

(7) Contrariu sensu, esta presunción no se aplicará si se tratase de una firma electrónica emitida por una entidad certificadora no acreditada ante la Autoridad de Acreditación. Es decir, se da la posibilidad de que existan entes certificadores no acreditados ante el órgano público. Ello deja una interrogante sin resolver pues parece que la ley sólo se les aplicaría a los entes debidamente acreditados, no así a los no acreditados que, sin embargo, podrían subsistir paralelamente. No se explica qué ocurriría con estos últimos, aunque nos parece que su sola existencia, sin regulación o fuera de los alcances de la norma jurídica, resultaría a todas luces inconveniente.

Si nuestra interpretación es correcta, tendríamos dos sistemas de firmas electrónicas, según se acrediten o no ante la Autoridad de Acreditación. Es algo que sólo se extrae tácitamente, pues ningún artículo dentro del proyecto contempla tal posibilidad. Ahora, si la voluntad soberana del legislador es tal, necesario resulta que ello se consigne expresamente en un numeral donde se regule la existencia de ambos sistemas de firmas electrónicas.

Si ello se omite, o si se da una dualidad de sistemas (uno que exige acreditación y otro que no), el peligro radicaría en que nos encontraríamos ante un sistema "privado" de firmas electrónicas que no tendría regulación alguna, con la consecuente ausencia de garantías y protección para los usuarios, así como la posterior

pérdida de credibilidad ante la firma electrónica por parte del ciudadano. Obsérvese que, en los términos actuales del proyecto de ley, no habría forma de obligar a alguna entidad certificadora a acreditarse ante la autoridad correspondiente, pues la acreditación parece ser voluntaria y en ninguna parte del texto se habla de que la Autoridad de Acreditación pueda condicionar el funcionamiento de un ente certificador a que sea supervisado o controlado por ella o a cumplir los requisitos señalados en el proyecto de ley. Se trata de una situación que es necesario corregir no sólo para mantener una estructura lógica constante dentro del proyecto de ley, sino también para garantizar una protección real a las comunicaciones públicas y privadas. La aplicación del término "acreditado", en el sentido visto, debería eliminarse.

7.-

Comentario al artículo 5.-

Desde un punto de vista estrictamente lógico, el artículo 5 debería ser el número 6 y éste pasar a ser el quinto. Obsérvese que en el actual numeral 5 se indica que un funcionario público tendría la posibilidad de utilizar una firma electrónica para algún tipo de certificación. Sin embargo, ello no sería posible si no existe una norma previa que expresamente lo autorice a ello, en virtud del respeto que debe guardarse del principio de legalidad administrativa. Dicha autorización al Estado y sus funcionarios se encuentra en el numeral siguiente, el 6, por lo que recomendamos el cambio de numeración ya indicado.

8.-

Comentario al artículo 6.-

Este numeral resulta fundamental, pues se trata de la autorización para que el Estado y sus entes puedan utilizar la firma electrónica en sus labores cotidianas. Con ello, se aplica el principio de legalidad para la administración pública. Igualmente, autorizan a los entes públicos a fungir como entidades certificadoras de firmas electrónicas. Ello es de suma conveniencia, pues permitirá que organismos como la Dirección

General de Notariado, los Registros Nacionales, Poder Judicial, etc., puedan brindar una gama más amplia de servicios para el público en general y llevar a cabo proyectos como el expediente electrónico o la notificación por correo electrónico con un alto nivel de seguridad.

Sobre este último punto, y dadas nuestras reservas sobre la posible existencia de empresas certificadoras no registradas, recomendamos que toda entidad pública, en los términos amplios de este numeral, deba estar obligatoriamente avalada y registrada en la Autoridad de Acreditación. No sería posible que organismos públicos que desearen actuar como entidades certificadoras de firmas tuvieran la alternativa de estar acreditados o no. En todo caso, si esta es la intención del legislador, debe expresarla con toda claridad en el mismo artículo. Si ello no se consigna, podría ser violatorio del principio de legalidad.

Más aún, es menester un regulación precisa y detallada en el texto de la propia ley, mediante un apartado particular, que se refiera exclusivamente a las autorizaciones y posibilidades particulares para el sector público, en especial los órganos que eventualmente puedan fungir como organismos de certificación de firmas electrónicas. No se trata de otorgar privilegios o dispensas particulares al sector público, sino tener en cuenta que el principio de legalidad administrativa debe ser tenido en cuenta y respetado para no imponer restricciones innecesarias y omisiones, con lagunas jurídicas que bien pueden solventarse o preverse desde ahora. De otra forma, podría tornarse imposible la aplicación de esta normativa al Estado. No basta siquiera con remitir al reglamento para su ordenación, sino que en la propia ley, por su rango, debe haber regulación más amplia para estos órganos.

9.-

Comentario al artículo 7.-

En general, los requisitos establecidos para la creación de firmas electrónicas son concordantes con nuestra posición sustentada antes, sobre la necesidad de orientar en lo posible el proyecto de ley hacia los términos de la firma digital avanzada.

No obstante, es necesario que se ordene que en el reglamento se desarrollen las reglas técnicas que en este artículo sólo se enuncian. Nótese que ello traerá una responsabilidad importante para el Poder Ejecutivo, pues el marco tecnológico donde recomendamos se fijen estas garantías es el Reglamento, y por ello es necesario que este esclarezca los procedimientos técnicos que serán aplicables para lograr los resultados que previene la ley. De poco o nada serviría un reglamento que sólo se limite a repetir o agregar algunos puntos adicionales a los que de por sí contiene la ley, sin practicar un verdadero ejercicio jurídico y tecnológico que sustente los objetivos perseguidos por la norma de mayor rango. Es aquí donde debe explicarse y recomendarse la utilización de la infraestructura de llave pública y llave privada, como forma de lograr la seguridad real en los envíos y recepciones de los mensajes firmados.

Además, debería modificarse la redacción en cuanto a al uso de la palabra "razonable" o "razonablemente", utilizadas en los párrafos 1 y 2, pues se trata de voces que siempre están sujetas a interpretación y, por tanto, tienen un carácter subjetivo. Eliminando dichos términos se estaría otorgando una garantía mayor de seguridad, cuya elaboración no dependería de la interpretación o la actuación de un tercero, sino del propio texto de la ley. Si se insiste en dejar esas palabras, convendría que el legislador diera una interpretación auténtica, dentro del propio texto de la ley, sobre lo que debe entenderse por "razonable".

10.-

Comentario al artículo 8.-

Siendo consecuentes con nuestra posición ante la firma digital "acreditada", pensamos que los requisitos que se mencionan deben ser aplicados a todo tipo de firma, independientemente de si está acreditada o no. Esta posición se sustenta mejor en los comentarios a los artículos 4 y en el artículo 2, cuando se menciona la palabra "acreditada", así como en el artículo 9. De hecho, dicho término debería eliminarse de todo el texto del proyecto de ley.

En el párrafo 4, al final de la frase, debe agregarse la palabra "digital", pues se trata de un certificado de esa naturaleza.

11.-

Comentario al artículo 9.-

En este numeral se consagra la libertad para el ciudadano de poder utilizar sistemas de firma electrónica distintos de los autorizados, de acuerdo con su leal saber y entender. La intención es que el usuario de firmas electrónicas no quede obligado o restringido a un sistema en particular, sino que tenga la libertad de escoger algún otro sistema electrónico de dar a conocer su voluntad y manifestarla. En este caso, las partes podrían elaborar un "contrato" que contenga, entre otras cosas, las "condiciones técnicas" para suponer que se está ante un verdadero sistema de firma electrónica.

Se supone que un instrumento tecnológico que se crea y se pone a disposición de los ciudadanos debe contener un mínimo de requisitos para su cabal funcionamiento. Tomando en cuenta que sistemas como el de la firma electrónica son elaborados para consolidar un método seguro de comunicación remota de la voluntad particular, resulta lógico esperar sea funcional y tan seguro como los sistemas que estén debidamente acreditados.

Es importante señalar que, independientemente de si un usuario desea utilizar un sistema de firma electrónica particular con sus contrapartes, distinta de las emitidas por las autoridades certificadoras (según se pretende en el artículo 9), tal sistema privado igual deberá respetar los lineamientos de esta ley para la creación de sus firmas. Con ello se evita la existencia de firmas de mayor o menor seguridad, pues todas estarían sometidas a los requerimientos tecnológicos que se señalen en la ley o en el reglamento respectivo. En forma alguna se está menoscabando la libertad del particular que no desee utilizar los sistemas acreditados. De hecho, se estaría reforzando la seguridad en las comunicaciones y respetando la capacidad volitiva del ciudadano.

Así las cosas, si se mantienen los términos de este numeral,

deberá exigirse que en la propia ley o al menos en el Reglamento (que no sería lo deseable), se indiquen con claridad los requisitos mínimos que deberá contener el "contrato" en que las partes se obligarán, los cuales no deberán ser menores que lo que la propia ley señala. Si el usuario desea incluir requisitos superiores o tecnología más segura, podrá hacerlo sin problema. Pero si lo que desea es utilizar un sistema que no reúne siquiera las condiciones mínimas de seguridad, estaríamos ante cualquier cosa pero no ante un sistema de firma electrónica. Resultaría absurdo que el Estado permitiese la existencia de sistemas de firmas electrónicas con características menores o menos seguras que las que señala la propia ley, el sentido común y la experiencia.

12.-

Comentarios a los artículos 10 y 11.-

Resulta lógico que sea el Ministerio de Ciencia y Tecnología el que funja como órgano rector de todo lo concerniente a firmas y certificados digitales, pues su naturaleza así lo demanda. No obstante, y de acuerdo con la Ley del Sistema para la Calidad No.8279 de 2 de mayo de 2002, artículo 19 y siguientes, ya existe un órgano encargado de llevar a cabo acreditaciones de todo tipo. Se trata del Ente Costarricense de Acreditación (ECA), conformado por una serie de jerarcas de Ministerios, entre los que se incluye el Ministerio de Ciencia y Tecnología.

"Artículo 21.—Funciones. El ECA será el único competente para realizar los procedimientos de acreditación en lo que respecta a laboratorios de ensayo y calibración, entes de inspección y control, entes de certificación y otros afines. Tendrá las siguientes funciones:

a) Acreditar previo cumplimiento de los requisitos, conforme a las buenas prácticas internacionales.

b) Estimular la acreditación en todos los ámbitos tecnológicos y científicos del país.

c) Garantizar la competencia técnica y credibilidad de los entes acreditados. Para ello, podrá realizar las investigaciones y ordenar las medidas cautelares que considere necesarias, incluso la suspensión temporal de la acreditación.

d) Resolver, previo cumplimiento del debido proceso, las denuncias que, en materia de su competencia, se presenten contra los entes acreditados.

e) Promover la suscripción de convenios de reconocimiento mutuo y otros instrumentos de entendimiento que propicien el reconocimiento de la acreditación otorgada por él ante órganos de acreditación similares.

f) Participar en las instancias internacionales de acreditación."

(Los subrayados no son del original)

Así las cosas, la Autoridad Acreditadora debería estar subordinado ya no al Ministerio de Ciencia y Tecnología, sino directamente al Ente Costarricense de Acreditación, quizás como una de las Secretarías de Acreditación que se mencionan en el artículo 27, tomando en cuenta que se trata de una materia especial.

"Artículo 27.—Secretarías de Acreditación. Existirán secretarías de acreditación en las áreas de competencia del ECA según la estructura interna que se establezca. Serán las encargadas de dar apoyo técnico a la Comisión de Acreditación, de acuerdo con las funciones que se definan en el Reglamento de esta Ley.

Los secretarios de acreditación deberán contar con la educación, la destreza, el conocimiento técnico y la experiencia necesarios para las actividades de acreditación por desarrollar. Asimismo, estarán imposibilitados para desempeñar actividades que puedan generar conflictos de interés."

Lo importante de reseñar la existencia previa de estas normas es evitar las contradicciones legislativas y os vacíos legales. Ahora bien, no encontramos choques de normas entre las funciones que se le asignan a la Autoridad Acreditadora y las que se señalas para el ECA, siempre y cuando se tengan como incluidas o adicionales a las funciones del Ente Costarricense de Acreditación. En caso contrario, habría una importante incoherencia normativa y funcional entre entes públicos encargados de labores similares.

Nuestra recomendación, pues, es que la Autoridad Acreditadora sea una Secretaría especial del Ente Costarricense de Acreditación en los términos en que se menciona en el numeral 27 de la ley No.8279 de 2 de mayo de 2002, incluyendo el contenido del artículo 11 del proyecto de ley como una adición al literal indicado.

Siguiendo con esta línea de pensamiento, vemos que el inciso c) del artículo 11 del proyecto de ley debería eliminarse, pues el procedimiento sancionatorio ya se encuentra regulado en el numeral 32 de la ley No.8279 de 2 de mayo de 2002. Es decir, no podría la Autoridad Acreditadora imponer sanciones a las entidades de certificación, pues tal función existe en las atribuciones del ECA.

"Artículo 32.—Procedimiento Sancionatorio. De conformidad con la Ley General de la Administración Pública, la Comisión de Acreditación del ECA deberá efectuar el procedimiento sancionatorio correspondiente con el fin de verificar, de oficio o por denuncia de cualquier interesado, el incumplimiento, por parte de los entes acreditados, de los deberes referidos en el artículo 31 de esta Ley. Si como resultado de este procedimiento se comprueba que el ente investigado ha incumplido tales deberes, la Comisión de Acreditación deberá retirarle la acreditación."

En general, conviene tener en cuenta y revisar en detalle la citada normativa y ajustar los términos del proyecto de ley a las reglas ya aprobadas.

13.-

Comentario al artículo 12.-

En este numeral, al igual que en los otros que contengan disposiciones similares, es necesario señalar con toda claridad cuál es el procedimiento que la Autoridad de Acreditación utilizará para acreditar a las empresas que presten tal servicio, y no dejarlo relegado totalmente al reglamento. Es necesario que en la ley se establezcan al menos algunos requisitos mínimos y básicos, remitiendo las demás formalidades al reglamento.

El segundo párrafo deberá estar en un artículo aparte, con un epígrafe que se refiera su contenido, e incluir otras funciones adicionales para las empresas certificadoras. No es posible que sólo se indique, de manera vaga, "brindar otros servicios inherentes al propio certificado". Es necesario precisar más su contenido y concordarlo con las demás funciones que podría encargarle la ya citada ley No.8279 de 2 de mayo de 2002, en lo que resulte pertinente.

14.-

Comentario al artículo 13.-

Resulta positivo que se tomen este tipo de medidas para proteger el secreto de los datos dados a conocer y guardados por la especial naturaleza del ente acreditador. No obstante, resulta de poca o ninguna utilidad que se reseñen deberes y obligaciones a los funcionarios de alguna entidad si no lleva aparejada las sanciones del caso, tales como responsabilidad administrativa, civil y eventualmente penal. Por ello, conviene que se incluya con claridad cuáles serían los castigos que se aplicarían en caso de algún quebranto en esta obligación.

La razón de esta petición tiene asidero en la experiencia. Debe prevenirse la actuación de individuos que, por la naturaleza del trabajo que realizan, su cercanía con las bases de datos o información confidencial, y las posibilidades de acceso a ellas, deben mostrar un celo mucho mayor y plantear una política de permanente seguridad física y lógica del sistema a su cargo. Infortunadamente, la experiencia indica que las más de las veces los mismos funcionarios, los encargados de dar mantenimiento al sistema, las personas que alimentan la base de datos, o bien, los empleados que de alguna manera tienen contacto frecuente con las plataformas tecnológicas o fuentes de información confidenciales, son los que cometen hechos lesivos contra el propio ente, precisamente por esa facilidad de acceso que tienen en razón de su trabajo. Por ello, dado que los empleados cercanos a los datos deben mantener mayor responsabilidad y control sobre su accionar, al igual que quienes tengan contacto con ellos por diversos motivos, se justifica de sobremanera la necesidad de incluir sanciones.

Existe legislación penal que bien podría aplicarse al caso concreto, siempre y cuando el legislador decida vincular ambas normas y homologar las conductas para que encuadren en el mismo tipo penal. El artículo 196 bis, 217 bis y 229 bis del Código Penal, según la adición practicada por la ley No.8148 de 24 de octubre de 2001, deberían ser tomados en cuenta para la redacción de este apartado.

En tal sentido dejamos planteada nuestra recomendación.

15.-

Comentario al artículo 14.-

En este artículo se nota una vez más el deseo de mantener una posición neutral ante el cambio tecnológico. Es por ello que se habla sólo de "un sistema de acreditación", sin entrar a detallar en qué consiste. Por supuesto, la intención es loable y oportuna. Empero, creemos conveniente que dicho sistema se mencione en detalle dentro del reglamento a la ley. No parece posible ni conveniente que dichas disposiciones se dejen al arbitrio del ente de acreditación, sin que la persona que busque acreditarse no sepa con certeza cuáles son los requisitos necesarios para ello, o que las exigencias de acreditación cambien según el criterio unilateral de la autoridad de acreditación. Esta posición, que percibimos como incerteza normativa para el observador foráneo, se repite en el párrafo segundo, cuando se habla de "requisitos de normas nacionales e internacionales". No es posible, tal y como mencionamos antes, hacer depender la existencia o validez del funcionamiento de la entidades de certificación de normativa foránea no recogida en normas nacionales, ya sean estas leyes o reglamentos. Contrario a lo que se menciona en el párrafo segundo, con ello no se garantiza "seguridad y confianza" ni parece adecuado para proteger los derechos de los usuarios.

Una normativa de este tipo no puede ser tan amplia y ambigua como para dejar de mencionar aspectos capitales como los señalados.

Es necesario además reorientar la denominación y las funciones de los entes públicos que se mencionan pues, de acuerdo con el

estado actual de la legislación, los cometidos que se mencionan en el primer párrafo corresponde la Junta Directiva del Ente Costarricense de Acreditación y a una eventual secretaría de acreditación.

Igualmente, deberán respetarse las disposiciones del artículo 24 de la Ley del Sistema Nacional para la Calidad, tales como la publicación en el Diario Oficial de la lista de entidades acreditadas y las demás que señale la normativa vigente.

Los demás puntos señalados en el párrafo tercero deberán introducirse como modificaciones o adiciones a los términos que contempla la ya citada ley No.8279, especialmente en los numerales 21 y 24.

16.-

Comentario al artículo 15.-

En el inciso 2 se habla de "normas" utilizadas para la creación de las firmas. Pensamos que sería más apropiado hablar de "reglas técnicas", que da una sentido más pertinente al contenido del certificado digital. "Normas" podría interpretarse como las leyes y reglamentos jurídicos que dan sustento a la existencia del certificado, y no a las disposiciones técnicas que lo respaldan. En tal sentido, sugerimos que se explique con claridad el sentido de dicho término, o bien, se acoja la sugerencia indicada.

17.-

Comentario al artículo 18.-

Con el advenimiento de la nuevas tecnologías y las comunicaciones que permiten y promueven los contactos internacionales y especialmente el comercio electrónico, resulta lógico suponer que las firmas digitales no están diseñadas ni destinadas para tener efectos únicamente en el territorio nacional, sino que se espera que sean de común uso allende las fronteras, entre usuarios situados en diferentes partes del mundo.

Tal es la razón de la existencia de este artículo, que prevé la posibilidad de acreditar en Costa Rica firmas electrónicas provenientes de otras naciones o de otras empresas diferentes de las que se hallen autorizadas en el país.

En tal situación, resulta loable que se den las previsiones del caso, tales como la homologación por parte de una empresa acreditada, y que se cumplan con los requisitos que se señalen en las normas correspondientes. No obstante, siempre queda la duda sobre las denominadas "normas internacionales", pues no se explica si se refiere a normas jurídicas o a normas técnicas, lo que puede llevar a confusión a la persona que desee prestar su empresa para homologar firmas extranjeras, pues no sabría con certeza cuáles normas debe cumplir.

Ahora bien, si se tratase de normas jurídicas internacionales, ya hemos hecho nuestros reparos en los comentarios anteriores. Si se tratare de normas técnicas de carácter internacional, deberían estar recogidas en el reglamento respectivo que elabore el Poder Ejecutivo, pues no es posible que se apliquen en el país normas no conocidas por la ciudadanía, o que sólo obraran en poder del órgano público encargado de aplicarlas o velar por su cumplimiento. En tales casos, dado que se trata de una función exclusiva del Poder Ejecutivo, deberá elaborarse algún mecanismo cierto de actualización jurídica normativa para que, cada vez que la tecnología cambie, dichas modificaciones sean recogidas e incluidas rápidamente en el reglamento y dadas a conocer a los interesados.

Por otra parte, sí debe quedar claro que sólo los prestadores de servicios autorizados son los que pueden homologar firmas electrónicas no establecidas en el país. De otra manera, nos encontraríamos ante el grave caso de firmas electrónicas extranjeras acreditadas en Costa Rica mediante empresas que a su vez no tienen la bendición de la Autoridad Nacional de Acreditación, situación que automáticamente debería invalidar a aquéllas.

18.-

Comentario a los artículos 19 y 20.-

Quizás el principal escollo que encontramos en estos dos numerales es el uso de los términos "dilación indebida", "esforzarse", "razonable" y "razonablemente", etc., amén de las posibilidades tan amplias para cumplir ciertos requisitos de seguridad, pues son conceptos tremendamente imprecisos y supeditados a interpretaciones subjetivas de los individuos involucrados. Por ello, creemos que lo recomendable sería que la propia norma, ya sea en la ley o el reglamento, indique con claridad cuáles podrían ser las reglas que objetivamente debe cumplir el usuario para acatar con los objetivos buscados por el legislador. Estos son la creación efectiva por parte del usuario de una firma electrónica segura, la posibilidad de proteger su identidad en caso de sospechas de que ha caído en manos de terceros, etc. Consideramos, pues, inconveniente no señalar taxativamente los remedios y demás disposiciones que desea el legislador proteger, en lugar de dejarlos a la libre interpretación del usuario o de la administración. De otra manera, habría que esperar la jurisprudencia judicial para definir qué se debe entender por ellos o qué quiso decir el ente legislativo cuando creó dichas voces o su alcance exacto, situación igualmente perjudicial, pues resulta casi indeterminables las acciones por seguir.

19.-

Comentario a los artículos 20 y 21.-

Para efectos formales, conviene indicar en los párrafos 4 y 5 del artículo 20, así como en los demás párrafos pertinentes del artículo 21, que se trata de un certificado digital, dado que allí sólo se habla de "certificado", sin mayor explicación.

20.-

Comentario al artículo 22.-

En el inciso g) debe añadirse que los "otros factores pertinentes", según se cita literalmente en el artículo 22, deben constar claramente en el reglamento que se elabore para esta ley.

Además, es prudente tener en cuenta el numeral 31 de la Ley del Sistema Nacional para la Calidad No.8279 de 2 de mayo de 2002, que señala una serie de deberes para los entes acreditados, mismos que deberán entenderse como yuxtapuestos a las otras obligaciones que se mencionan en este artículo 22.

Artículo 31.—Deberes de los Entes Acreditados.

Los entes acreditados deberán:

a) Respetar y aplicar lo dispuesto en los ámbitos de la acreditación concedida, en el acta de compromiso y en el reglamento de acreditación correspondiente.

b) Facilitar las evaluaciones de seguimiento, anunciadas y no anunciadas, de la acreditación concedida.

c) Respetar los plazos y las condiciones establecidos para la expiración y la posible renovación de la acreditación.

21.-

Comentario al artículo 23.-

Aparentemente existen errores de digitación en este artículo. En el párrafo primero, línea tercera, se indica que "en el perjuicio de su actividad". Nos parece que el término correcto debería ser "en el ejercicio de su actividad".

Igualmente, en el párrafo segundo, segunda línea, parece faltar el adverbio de negación "no", pues sólo aparece una letra "n". De otra manera, se estaría tergiversando el deseo del legislador de librar de responsabilidad a las empresas prestadoras de servicios por el uso indebido por parte del usuario de un certificado de firma digital.

22.-

Comentario al artículo 25.-

Cabe recordar la necesaria confrontación que debe tener el presente proyecto con la citada ley No.8279 de 2 de mayo de 2002, en virtud de que se trata de funciones que corresponderían eventualmente al Ente Costarricense de Acreditación, en virtud de lo dispuesto en el artículo 21 de la norma citada. Por supuesto, queda a criterio del legislador efectuar los cambios que considere prudentes en esta materia, pero siempre es positivo hacer notar la existencia de alguna disposición jurídica que podría causar contradicción o dudas en la verdadera intención del Poder Legislativo en algún punto en concreto.

En especial, citamos los literales 26 y 32 de la ley, que rezan:

Artículo 26.—Funciones de la Comisión de Acreditación.

La Comisión de Acreditación tendrá las siguientes funciones:

a) Acreditar previa comprobación del cumplimiento de los requisitos correspondientes, conforme a las buenas prácticas internacionales.

b) Instruir los procedimientos de investigación y sancionar a los entes acreditados que incumplan esta Ley y su Reglamento.

Artículo 32.—Procedimiento Sancionatorio.

De conformidad con la Ley General de la Administración Pública, la Comisión de Acreditación del ECA deberá efectuar el procedimiento sancionatorio correspondiente con el fin de verificar, de oficio o por denuncia de cualquier interesado, el incumplimiento, por parte de los entes acreditados, de los deberes referidos en el artículo 31 de esta Ley. Si como resultado de este procedimiento se comprueba que el ente investigado ha incumplido tales deberes, la Comisión de Acreditación deberá retirarle la acreditación.

Por otra parte, resulta de utilidad señalar la posibilidad jurídica existente de burlar la intención del legislador de sancionar o impedir en definitiva a una empresa dedicada a la certificación de firmas electrónicas y emisión de certificados

digitales, mediante simples tecnicismos jurídicos. En el parte final del artículo de comentario se indica una serie de sanciones para las entidades certificadoras de firmas electrónicas, que van desde la amonestación hasta la revocación definitiva de la acreditación y prohibición para operar en Costa Rica como entidad de certificación acreditada. Al respecto, sería prudente que la sanción no se impusiere a la persona jurídica solamente, sino también a los gerentes de ellas que resulten personalmente responsables de los hechos. De otra manera, sería muy fácil para cualquier sujeto responsable utilizar una nueva persona jurídica, con otro nombre y razón social, para seguir operando en la misma actividad que se le ha prohibido. De nada serviría, pues, semejante sanción si los sujetos personalmente responsables no son sancionados directamente.

Por último, recordemos que la jurisprudencia constitucional ha declarado inconstitucionales los castigos permanentes y usualmente los ha reducido a un término decenal. Así las cosas, y para prever una posible acción de inconstitucionalidad sobre esta norma, sugerimos que la prohibición indicada en el inciso e) de este numeral sea reducida a diez años, con las condiciones mencionadas anteriormente para los gerentes responsables.

Igualmente, debe indicarse en el texto de la norma que estas sanciones se aplicarán sin perjuicio de las conductas que puedan resultar adecuadas a los tipos penales correspondientes.

23.-

Comentario al artículo 26.-

Las formalidades que se incluyen en el párrafo primero, referentes a impugnaciones y recursos contra las resoluciones de la Autoridad de Acreditación deben constar con más detalle, pues esta materia en forma alguna debe relegarse al reglamento.

Además, resulta conveniente, una vez más, apelar a la existencia de normas que regulan la materia, tal como la ley No.8279 de 2 de mayo de 2002, la cual ordena en su artículo 24 lo

siguiente:

Artículo 24.—Funciones de la Junta Directiva. La Junta Directiva del ECA tendrá las siguientes funciones:

(...)

d) Resolver las apelaciones presentadas contra los procedimientos y los resultados finales de las acreditaciones, así como los procedimientos de sanción contra los entes acreditados.

Como se ve, el legislador parece haberse adelantado en la emisión de normas genéricas que regulen la existencia de autoridades de acreditación, entes acreditadores, sanciones y demás temas relacionados. Por ello, es necesario que el texto del proyecto de ley se adecue a los términos de la ley preexistente, o bien, que la modifique en lo pertinente, según sea la voluntad del Poder Legislativo.

De esta forma, dejamos planteadas nuestras inquietudes sobre el contenido del proyecto de ley sometido a nuestra consideración. Igualmente, esperamos que las observaciones indicadas sean de utilidad para el estudio de un instituto tan novedoso e importante como la firma electrónica para lo cual no dudamos en ofrecer nuestra colaboración institucional para el estudio y análisis de la firma electrónica.

3 DIRECCIÓN GENERAL DE TRIBUTACIÓN DIRECTA

A.Impuesto de ventas sobre el comercio electrónico

[DIRECCIÓN GENERAL DE TRIBUTACIÓN DIRECTA][3]

“

Señora

[...]

Área Grandes Empresas Territoriales -Subgerencia de Fiscalización
Administración Tributaria de San José

Estimada señora:

Se da respuesta a su oficio GETES-344-2003 de 29 de setiembre adicionado con el oficio GETES-349-2003 de 1 de octubre ambos del año 2003, mediante los cuales consulta sobre las actividades realizadas por la empresa [...], según el siguiente detalle:

1.- Las empresa vende licencias de [...] con las siguientes especificaciones:

OEM: este producto lo venden con las computadoras clones. [...] tiene en el mundo replicadores autorizados, en este caso [...] ubicada en Miami (queman los cd´s con autorización de la casa matriz e incorporan el número autorizado de licencia en cada cd). Cuando este producto ingresa a la aduana paga el impuesto general sobre las ventas. Al valor de este producto (valor físico, no intelectual), se le agrega el valor intelectual para que refleje el costo real. Por estos productos no se cobra el impuesto

general sobre las ventas. Al valor de este producto (valor físico no intelectual), se le agrega el valor intelectual, para que refleje el costo real. Por estos productos no se cobra el impuesto general sobre las ventas, pero si se remesa el 25% por concepto de royalty (derechos de autor). No obstante esta indicación de la primera consulta fue modificada con su segunda nota, al indicar que el contribuyente le manifestó que en estos casos si cobra el impuesto general sobre las ventas.

MOLP: Este producto lo compran a través de internet. Básicamente [...] emite un número de autorización, por una determinada cantidad y variedad de licencias, que son específicamente para el usuario final. En ellas se consigna el nombre del mayorista, distribuidor y usuario final. Al cliente se le factura sin el impuesto general sobre las ventas y se le retiene el 25% por concepto de derechos de autor.

2- La empresa consulta a la Administración Tributaria de Cartago si como distribuidores autorizados de licencias de [...], se encuentran obligados a efectuar el cobro del impuesto general sobre la ventas, a lo que les indicaron que la venta de licencias, se encuentra exenta del impuesto en mención.

3- Según oficio Nº 051 del 16 de enero de 1998, la Dirección General y mediante el Fallo Nº 320/97 dictado por la Sala Primera del Tribunal Fiscal Administrativo a las ocho horas del día diecisiete de octubre de mil novecientos noventa y siete, se consideró que si vende la licencia en calidad de uso de los paquetes de software, se debe recaudar el impuesto general sobre las ventas, por tratarse de la venta de una mercancía no exenta, en cuyo costo está incluido el valor de la licencia.

Ante esta disyuntiva, solicitan criterio para el presente caso.

Al respecto está Dirección le manifiesta que en casos como el presente se deben considerar los siguientes aspectos:

En primer lugar se debe considerar que cuando se habla de una licencia de uso de software se refiere al uso de una serie de programas que sólo elabora y comercializa la empresa dueña de la licencia, la cual en el presente caso es de [...], por lo que sin la autorización de la empresa propietaria de la marca, no se podría contar con el software.

En segundo lugar se debe apreciar que nuestro ordenamiento tributario vigente no contiene normas específicas que regulen los aspectos sustanciales y formales de transacciones realizadas mediante el "comercio electrónico" en sus diversas manifestaciones, por lo que se debe encuadrar el tratamiento respectivo en las normas generales vigentes, en tanto ello no configure situaciones que sean materia reservada a la ley, con fundamento en lo establecido en el artículo 5 del Código de Normas y Procedimientos Tributarios, conforme al cual, y en lo que interesa, solo la ley puede crear , modificar o suprimir tributos, definir el hecho generador de la relación tributaria, establecer las tarifas de los tributos y sus bases de cálculo, e indicar el sujeto pasivo.

En tercer lugar en relación con el comercio electrónico se pueden dar dos tipos de contrataciones: off line y on line. El comercio

electrónico off line es aquél en el que los bienes comercializados necesitan ser enviados a través de canales tradicionales de distribución, por ejemplo, envío postal y servicios de mensajería. Por su parte, el suministro on line es aquél donde el pedido, pago y envío de los bienes intangibles y/o servicios, se produce a través de la página Web, como por ejemplo programas informáticos, servicios de información, etc. Se aplica sólo a bienes digitalizados y, por tanto susceptibles de ser transmitidos por las líneas de telecomunicaciones. En estos casos, el bien o servicio adquirido es descargado desde el ordenador del proveedor al ordenador del cliente.

Los suministros off line suelen ser bienes materiales que se transportan por los medios tradicionales o servicios profesionales contratados a través de la red, los suministros on line son siempre bienes o derechos derivados de la propiedad intelectual. Esto no significa que no puedan transmitirse bienes derivados de la propiedad intelectual off line, pues se puede adquirir un libro o un disco en una página Web, los cuales llegarán a nuestras manos por los medios tradicionales de transporte.

La propiedad intelectual está integrada por los derechos de carácter personal y patrimonial que atribuyen a su autor la plena propiedad y el derecho exclusivo de explotación de la obra y los programas de ordenador se incluyen entre ellos.

De lo antes expuesto tenemos que en el caso de las ventas OEM se está ante el caso de venta off line por ser bienes materiales que se transportan por los medios tradicionales, ya que conforme usted lo indica el producto se vende en las computadoras clonadas, en que se queman los cd’s y se incorpora el número autorizado de licencia en cada cd y el producto ingresa vía aduana, por lo que en este caso sí corresponde cobrar el impuesto general sobre las ventas correspondiente al valor agregado del bien que se comercializa.

En el caso de la modalidad denominada MOPL, nos encontramos ante un caso de comercio on line, por lo que no corresponde cobrar el impuesto general sobre las ventas, por cuanto no se trata de una mercancía, sino de un servicio que no se encuentra contenido en la lista de servicios gravados que contiene el artículo 1° de la Ley del Impuesto General sobre las Ventas, N° 6826 de 8 de noviembre de 1982 y sus reformas.

No omitimos manifestarle que en cuanto al impuesto sobre la renta, procede efectuar la retención por remesas al exterior, en ambos casos, según indica el párrafo penúltimo del artículo 59 de la Ley del Impuesto sobre la Renta N° 7092 de 21 de abril de 1988 y sus reformas.

Atentamente,

Lic. José Armando Fallas Martínez

DIRECTOR GENERAL

[1] TRIBUNAL PRIMERO CIVIL. Resolución N°466 -L- de las ocho horas veinte minutos del veinte de junio del año dos mil dos.

[2] PROCURADURÍA GENERAL DE LA REPÚBLICA DE COSTA RICA. Opinión

Jurídica N°: 028 - J , del 19/02/2003.

[3] DIRECCIÓN GENERAL DE TRIBUTACIÓN DIRECTA . Oficio N°DGT - 33 – 04, de 7 de enero del 2004.