Universidad de Costa Rica

Facultad de Derecho

"CONCEPTO, VALOR JURÍDICO Y REGULACIÓN DE LA FIRMA DIGITAL EN COSTA RICA"

Tesis para optar por el grado de Licenciatura en Derecho

Carmen de Téramond Peralta

Mónica Fernández Fonseca

2002

UNIVERSIDAD DE COSTA RICA
FACULTAD DE DERECHO
AREA DE INVESTIGACIÓN

San José, 27 de agosto del 2002.

Dr.
Rafael González Ballar
Decano, FACULTAD DE DERECHO

Hago de su conocimiento que el Trabajo Final de Graduación de las estudiantes:

DE TERAMOND PERALTA CARMEN Y HERNANDEZ FONSECA MONICA

Titulado: ***"CONCEPTO, VALOR JURÍDICO Y REGUACION DE LA FIRMA DIGITAL EN COSTA RICA!"*** fue aprobado por el Comité Asesor, a efecto de que el mismo sea sometido a discusión final. Por su parte, el suscrito ha revisado los requisitos de forma y orientación exigidos por esta Área y lo apruebo en el mismo sentido.

Asimismo le hago saber que el Tribunal Examinador queda integrado por los siguientes profesores:

Presidente: LIC. MIGUEL VILLEGAS ARCE
Secretario: LIC. ARON MONTERO SEQUEIRA
Informante: LIC. PEDRO BERNAL CHAVES CORRALES
Miembro: LIC. STEVEN ALVARADO ACOSTA
Miembro: LIC. HUGO PICADO LEON

La fecha y hora para la PRESENTACION PUBLICA de este trabajo se fijó para el día jueves 5 de setiembre del 2002, a las 18:00 p.m. horas.

Atentamente,

UNIVERSIDAD DE COSTA RICA
FACULTAD DE DERECHO

DR. DANIEL GADEA NIETO
DIRECTOR
AREA DE INVESTIGACIÓN
FACULTAD DE DERECHO

San José, 16 de agosto de 2002

Doctor
Daniel Gadea Nieto
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica

Estimado Dr. Gadea:

Por este medio le manifiesto mi aprobación al Trabajo Final de Graduación de los estudiantes Carmen de Téramond Peralta, carné 971140, y Mónica Fernández Fonseca, carné 971321, denominado "*Concepto, Valor Jurídico y Regulación de la Firma Digital en Costa Rica*", el cual tuve el agrado de dirigir.

El trabajo describe ampliamente el funcionamiento de la firma digital y su tratamiento en la doctrina y regulación en el derecho comparado. Asimismo, esta investigación realiza un análisis detallado del Proyecto de Ley No. 14.276 "Ley de Firma Digital y Certificados Digitales", en trámite ante la Asamblea Legislativa. Finalmente, el trabajo incluye importantes consideraciones sobre el valor jurídico de la firma digital.

Este trabajo de investigación constituye un importante aporte al estudio de la firma digital en Costa Rica. Este es un tema de gran actualidad y de vital importancia en las relaciones jurídicas, que las estudiantes tratan con mucha seriedad y responsabilidad. Lo anterior se evidencia por la importante labor de investigación y las conclusiones muy atinadas con respecto al tema estudiado

Por esas razones otorgo la aprobación de su trabajo final.

Se despide atentamente,

Pedro Chaves Corrales
Director

Dr. Alfredo Chirino Sánchez
Director
Escuela Judicial
Tel: 295-33-46
alfredochirino@hotmail.com

San José, 16 de agosto de 2002.

Doctor
Daniel Gadea
Director
Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Presente

Estimado Dr Gadea:

Me es muy grato comunicarle que he leído, en mi condición de miembro del grupo asesor, la tesis intitulada "Concepto, Valor y Regulación Jurídica de la Firma Digital en Costa Rica" de las estudiantes de esta Facultad, Carmen de Teramond y Mónica Fernández.

El tema escogido por las estudiantes tiene un enorme valor para el debate existente en Costa Rica, desde hace ya algunos años, sobre la necesidad y conveniencia de la regulación jurídica de la firma digital, y, por esa vía, crear condiciones para la prestación de servicios de autenticación y certificación electrónicos para diversas contrataciones modernas.

El debate nacional ha transitado diversas etapas hasta concluir con un proyecto de ley que ha sufrido diversos cambios. A pesar de la importancia del tema, sin embargo, no ha habido un planteamiento técnico que permita comprender los diversos aspectos involucrados con el proceso de autenticación electrónica, que es, por supuesto, un elemento central para comprender la necesidad y orientación de la ley.

Asimismo, la discusión no ha estado del todo alejada de una incomprensión del foro nacional, el cual considera que un proyecto de este jaez afectará la función notarial de certificación, lo que ha provocado, en última instancia, que el proyecto tenga injustificadamente algunos adversarios.

La tesis que las estudiantes nos ofrecen hoy es una forma de poner al día la cuestión de la firma digital en una perspectiva comparada, enriqueciéndonos con un enfoque constructivo conducente a una modificación del proyecto de ley actualmente en la agenda legislativa.

Se trata de una investigación muy informativa y con valiosas fuentes tanto de bibliografía documental como de internet, lo que le permite al investigador e interesado en la materia profundizar en aquellos temas que más le interesen, sin perder de vista los criterios expuestos por las estudiantes.

Dr. Alfredo Chirino Sánchez
Director
Escuela Judicial
Tel: 295-33-46
alfredochirino@hotmail.com

Este trabajo constituirá, sin duda, la piedra angular para reconducir el proceso de investigación en nuestra Facultad sobre estos temas tecnológicos y para colaborar con el proceso de debate legislativo de esta novedosa normativa.

Por lo anterior, creo que la tesis no solo cumple a cabalidad los requisitos de forma y fondo exigidos por el Departamento a su digno cargo, sino que constituye un valioso aporte al conocimiento sobre el tema, por lo que estimo conveniente invitar a la disputación oral de la misma.

Sin otro particular, se suscribe,

Cordialmente,

Prof. Dr. Alfredo Chirino Sánchez
Lector de la Tesis

San José, 14 de agosto de 2002

Doctor
Daniel Gadea Nieto
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica

Estimado Dr. Gadea:

Por este medio le manifiesto mi aprobación al Trabajo Final de Graduación de las estudiantes Carmen de Téramond Peralta, carné 971140, y Mónica Fernández Fonseca, carné 971321, denominado *"Concepto, Valor Jurídico y Regulación de la Firma Digital en Costa Rica"*.

El trabajo describe ampliamente el funcionamiento de la firma digital y su tratamiento en la doctrina y regulación en el derecho comparado. Asimismo, esta investigación realiza un análisis detallado del Proyecto de Ley No. 14.276 "Ley de Firma Digital y Certificados Digitales", en trámite ante la Asamblea Legislativa. Finalmente, el trabajo incluye importantes consideraciones sobre el valor jurídico de la firma digital.

Las estudiantes tratan el tema con mucha seriedad y responsabilidad, lo que se evidencia por la importante labor de investigación y las conclusiones muy atinadas con respecto al tema estudiado.

Por esas razones otorgo la aprobación de su trabajo final.

Se despide atentamente,

Eric Scharf Taitelbaum
Lector

CONCEPTO, VALOR JURÍDICO Y REGULACIÓN DE LA FIRMA DIGITAL EN COSTA RICA

DE TÉRAMOND PERALTA, Carmen y FERNÁNDEZ FONSECA, Mónica. **"CONCEPTO, VALOR JURÍDICO Y REGULACIÓN DE LA FIRMA DIGITAL EN COSTA RICA"**. Tesis para optar por el grado de licenciadas en Derecho, Facultad de Derecho, Universidad de Costa Rica, San José, Costa Rica, 2002.-

DIRECTOR: Pedro Chaves Corrales

LISTA DE PALABRAS CLAVES: firma digital [valor jurídico], firma electrónica, firma digital avanzada, Internet, comercio electrónico, certificados digitales, autoridades de certificación, documento digital, criptografía, principio de equivalencia funcional, principio de neutralidad tecnológica, compatibilidad internacional, libre competencia, acreditación voluntaria, uso de la firma digital por el Estado, autenticidad, integridad, no repudio, confidencialidad, derecho comparado, proyecto de ley sobre firma digital y certificados digitales, autonomía de la voluntad, principio de legalidad.

RESUMEN DEL TRABAJO: La firma digital, tema actual y relevante, es un mecanismo que nace como respuesta a las

necesidades de brindar seguridad en las transacciones electrónicas. Es un instrumento de naturaleza técnica que se basa en sistemas de encriptación digital, regido por el principio de neutralidad tecnológica. La aparición de Internet ha causado una revolución en todos los aspectos de la vida humana. Esta Red ha creado un espacio paralelo al mundo físico, al cual se han trasladado muchas de las transacciones habituales de las personas. Por tratarse básicamente del flujo de información, uno de los riesgos principales es la alteración de ésta a nivel electrónico. Se vuelve necesario un sistema jurídico que dé seguridad en el intercambio de datos. Una de las formas de lograr una plena seguridad es la firma digital; obteniendo la autenticación, la integridad, el no rechazo en origen y destino y la confidencialidad de la información. Hay un gran interés sobre este tema a nivel mundial y en la práctica se aplica desde hace varios años, lo cual ha llevado a diferentes países a aprobar leyes sobre este tema. Otros organismos de derecho internacional, como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI, o por sus siglas en ingles UNCITRAL) y la Unión Europea, han redactado cuerpos normativos al respecto. Asimismo, encontramos diversos países

con proyectos de ley sobre este tema en trámite de discusión, como Costa Rica. Por medio de la firma digital se logran las garantías necesarias para equiparar la firma digital con la manuscrita. Se asegura la identidad del firmante comprobando que quien firma un mensaje de datos digitalmente es quién dice ser. Se garantiza adicionalmente la integridad del mensaje, es decir, que éste no ha sido alterado con posterioridad a la firma. Además se logra el no repudio de la información transmitida, esto ofrece la seguridad inquebrantable de que el autor del documento no pueda retractarse en el futuro de haber enviado el mensaje. Estas garantías permiten el desarrollo del principio de equivalencia funcional: la firma digital tiene el mismo valor jurídico que la firma manuscrita. El reconocimiento jurídico de la firma digital no crea ninguna nueva figura en el derecho, es una mera equiparación que conlleva las mismas consecuencias jurídicas que la firma manuscrita. Esto tiene importantes consecuencias para el reconocimiento del documento electrónico como un documento en términos jurídicos asegurándole plenos efectos probatorios.

INTRODUCCIÓN

La aparición de Internet ha causado una revolución en todos los aspectos de la vida humana, así como lo hizo la revolución industrial en el siglo XVIII, cuando se pasó de una economía agrícola y artesanal a una dominada por la industria y la manufactura. La base de esta revolución fue la aplicación sistemática del conocimiento para desarrollar formas más eficientes de producción. Tuvo innumerables consecuencias en los diferentes ámbitos de la vida humana, como el transporte, las comunicaciones, la forma de trabajo, el derecho, la banca, en resumen, todo lo relacionado con el ámbito social, cultural, económico y político. De la misma manera, la búsqueda de modelos más eficientes de trabajo, ha llevado a la creación de nuevas tecnologías que asistan al ser humano en su vida diaria. De estos avances recientes, podemos decir que el más importante es Internet y el uso generalizado que ha alcanzado en los últimos años.

La utilización de este poderoso instrumento ha transformado el estilo de vida de las personas y su modo de operar. Esta

Red ha creado un espacio virtual paralelo al mundo físico, al cual se han trasladado muchas de las transacciones habituales entre las personas. Constituye, asimismo un poderoso instrumento para el cambio y el desarrollo de la sociedad.

Se pasa de esta manera, de un esquema basado en el papel, a un mundo dominado por lo digital, con un cambio radical en los medios de producción de cualquier forma de información. Por ejemplo, se puede hacer llegar el contenido de un libro de forma digital a millones de personas a un costo casi cero. Esto significa un gran cambio y todo gran cambio implica riesgos. La utilización de las nuevas tecnologías presenta un obstáculo práctico, que es la necesidad de dar seguridad a las comunicaciones. Se vuelve necesario, entonces, un sistema jurídico que brinde seguridad en el intercambio de datos e información. Una de las formas de lograr este objetivo es con la aplicación de la firma digital, asegurándole valor jurídico, ya que la firma digital como tal es una herramienta ideal para ser aplicada a las transacciones en Internet.

La firma digital es un mecanismo que nace como respuesta a las necesidades de seguridad en el tráfico electrónico. Su

estudio es un tema reciente que está actualmente desarrollándose en doctrina y al cual las legislaciones nacionales y regionales están empezando a dar respuesta.

El tema de la firma digital, que es actual y relevante. Ha generado numerosos trabajos y artículos que no han logrado pasar del desarrollo de los conceptos, sin profundizar en las repercusiones en las diferentes ramas del derecho. Por ser su campo de aplicación la red Internet, que tiene incidencia en prácticamente todas las áreas la vida humana, las posibilidades de uso y estudio de la firma digital son inacabables. Es por estas razones que el tema esta muy lejos de ser agotado y, más bien, los estudios en este campo son sumamente necesarios.

El **objetivo general** del presente trabajo es desarrollar el concepto de firma digital, analizar su valor como institución jurídica y estudiar las normas que la regulan o deben regular, con especial atención al ordenamiento jurídico costarricense.

Como **objetivos específicos**, nos proponemos: **1)** Delimitar el campo de aplicación de la firma digital, la cual tiene sus principales efectos en Internet y el comercio electrónico en sentido amplio. **2)** Proponer la firma digital como mecanismo para lograr seguridad y confianza en las transacciones que se realizan en Internet. **3)** Demostrar que la firma digital tiene el mismo valor jurídico que la firma manuscrita y ológrafa. **4)** Realizar un estudio de derecho comparado de la legislación sobre el tema. Analizar el proyecto de ley numero 14.276 "Ley de Firma Digital y Certificados Digitales, presentado a la Asamblea Legislativa en febrero del año 2001.

Debido a la novedad del tema en cuestión, existen pocos trabajos de investigación que profundicen al respecto. Encontramos un gran número de artículos de periódico y documentos publicados en Internet. En los últimos años, se ha desarrollado un gran interés sobre la firma digital a nivel mundial y, en la práctica, este instrumento ya se aplica con regularidad. Esto ha llevado a diferentes países a promulgar legislación referente al tema, entre los que se encuentran Alemania, Argentina, Chile, Colombia, España, Estados Unidos de América, Francia, Italia, Japón, Malasia y Perú. Otros

sujetos de derecho internacional, como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL, por sus siglas en ingles) y la Unión Europea, han redactado cuerpos normativos al respecto, con el propósito de brindar un marco modelo para el desarrollo de esta legislación en los demás países. Asimismo, encontramos diversos países que tramitan actualmente proyectos de ley que pretenden regular la firma digital, tales como Costa Rica. Finalmente, existe un interés académico y profesional al respecto, por lo cual se realizan con frecuencia, tanto en nuestro país como en el extranjero, seminarios, conferencias y otras actividades.

La hipótesis base de este trabajo de investigación es la siguiente: la firma digital tiene un valor equivalente a la firma manuscrita, en cuanto a autoría y aprobación de documentos y funciona, además, como un mecanismo de seguridad.

La metodología utilizada en la realización de este trabajo, consistió principalmente en la recolección de información, sobretodo en artículos publicados en Internet, pues aquí es

donde existen los más recientes estudios de los últimos cambios que se dan con relación a nuestro tema. Además consultamos diversos libros, tanto de la teoría general del derecho como de la nueva rama del derecho informático. Asimismo, analizamos en forma comparada, la legislación existente en diversos países, dándole énfasis a la propuesta de ley costarricense. En cuanto a trabajos de campo efectuamos entrevistas a abogados y profesionales del área de informática sobre el tema y asistimos a seminarios y conferencias.

El presente trabajo se divide en dos títulos. El primero se concentra en hacer un estudio general sobre la firma digital. Dos capítulos conforman este título, el primero trata el concepto, desarrollo e importancia de Internet y del comercio electrónico. El segundo capítulo analiza los aspectos técnicos de la firma digital y sus aplicaciones. El segundo título es un estudio de los aspectos jurídicos de dicha firma. Se divide a su vez, en tres capítulos, el primero desarrolla la naturaleza y efectos jurídicos de la firma digital, el segundo capítulo analiza la regulación internacional de este instrumento y por último, el tercer

capítulo profundiza sobre la firma digital a la luz del Proyecto de Ley costarricense sobre el tema.

TÍTULO I: NOCIONES GENERALES SOBRE LA FIRMA DIGITAL

La firma digital es un instrumento de naturaleza tecnológica cuyo uso actual es más frecuente en el ámbito internacional. Por su complejidad técnica, es necesario analizar, en primer lugar, qué es y cómo funciona, previo al estudio de los aspectos jurídicos. En consecuencia, en el presente título analizaremos algunos antecedentes y nociones generales sobre la firma digital, primeramente el desarrollo histórico de Internet hasta la aparición del comercio electrónico; seguidamente, la aparición de la firma digital, su concepto y su funcionamiento y, por último, mencionaremos algunos ejemplos de su aplicación.

CAPÍTULO I: DESARROLLO HISTÓRICO DEL COMERCIO ELECTRÓNICO Y NACIMIENTO DE LA FIRMA DIGITAL

La aparición de Internet ha revolucionado todos los aspectos de la vida humana. Este poderoso instrumento ha transformado el estilo de vida de los individuos y las sociedades. Sus efectos son palpables en campos muy diversos como el comercio, las telecomunicaciones, la investigación, el sector académico, científico, de salud, ambiental; son todas las áreas que, de una u otra forma, están relacionadas con la información y la tecnología. Son notables los cambios que la nueva Era de la Información ha producido en el comercio. El comercio electrónico ha modificado la forma en que se efectúan los negocios. El tema de seguridad se vuelve entonces crítico para la eficiencia de los intercambios y la confiabilidad de este nuevo mecanismo de comunicación y, por ende, la manera de realizar las transacciones.

En este sentido, la firma digital se utiliza para otorgar seguridad a las transacciones comerciales electrónicas y a la

transferencia electrónica de datos[1] y apunta a que las partes en un negocio electrónico puedan autenticar todos y cada uno de los mensajes que hayan intercambiado, asegurando la identidad de las partes, la integridad del mensaje, el no repudio del emisor y la confidencialidad.

I. DESARROLLO, CONCEPTO E IMPORTANCIA DEL COMERCIO ELECTRÓNICO

Para entender el desarrollo, funcionamiento, utilidad, difusión e importancia del comercio electrónico, es necesario estudiar, en primer lugar, el nacimiento de Internet y su evolución. Si bien es cierto que no todas las transacciones comerciales electrónicas utilizan Internet como plataforma de comunicación y transferencia de información[2], esa red es el pilar fundamental del ámbito de los negocios.

---

[1] DEVOTO, Mauricio y LYNCH M. Horacio. **Banca, Comercio, Moneda Electrónica y La Firma Digital** en Revista Electrónica de Derecho Informático. 1998. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/No._02_-_Septiembre_de_1998/devoto

[2] HERNANDEZ, Edgar y GÁMEZ, Marco Vinicio. **Seguridad de la Información en la Era de los Negocios Sociales.** San José, Costa Rica: Rho-Sigma, S.A., 2001.

1. INTERNET

El primer recuento de comunicación a largas distancias del que tengamos noticias, está reseñado en Agamenón, escrito por Esquilo en 458 a.C., cuando después de la caída de Troya, Agamenón regresa a su tierra y señales de su regreso son enviadas de montaña a montaña, utilizando con faros de bronce en la noche. La información era enviada a simple vista. Agamenón regresa a su casa, y su esposa y el nuevo esposo de ésta, que ya se habían enterado de su llegada con esta técnica, lo esperan para matarlo.[3]

En 1800, Volta inventa la pila, que permite mediante la conexión de un par de cables metálicos establecer un circuito eléctrico; cuando se abre o se cierra el circuito, se envía una señal que se transmite a la velocidad de la luz a través de los cables. Este es el principio del telégrafo, al abrir y cerrar un interruptor con la pulsación del dedo se transmiten

---

[3] The New Enciclopædia Britannica. Volumen 18. Edición número 15. Chicago: Enciclopædia Británica, Inc. 1974.

señales que llevan el mensaje utilizando la clave Morse. El telégrafo fue utilizado por dos siglos como el instrumento de comunicación más importante. De esta forma, se logra transmitir información a grandes distancias, por ejemplo de Paris a Nueva York. Como el cable por el que se transmitía la información presentaba grandes problemas si se ponía bajo el mar, se instaló el cable de Nueva York hasta la Costa Oeste de Estados Unidos, pasando luego por Canadá, Alaska, el Estrecho de Bering, traspasando toda Siberia, después Moscú, atravesando Europa hasta llegar a París. Esta es la primera comunicación que se da entre continentes. Es así como Tolstoi en 1865, redactaba La Guerra y La Paz y un operador enviaba vía clave morse el texto a sus editores en Nueva York ha medida que Tolstoi avanzaba con su obra.

Concurrentemente, se efectuó un enorme esfuerzo tecnológico de ingeniería para instalar un cable directo sobre el fondo del Atlántico entre Nueva York e Inglaterra. Iniciativa que culminó exitosamente años más tarde, después de varios intentos fallidos.

---

[4] The New Enciclopædia Britannica. Op. Cit.

Hoy en día, como en el pasado, la información se transmite a la velocidad de la luz; con la diferencia que en el pasado la cantidad de información de un mensaje que se transmitía de un lugar a otro dependía del movimiento del dedo del operador del telégrafo, un carácter por segundo, mientras que los sistemas contemporáneos de fibra óptica no tienen límite en la velocidad de comunicación.

El próximo paso que se dio fue la transmisión de la voz de un punto a otro, al lograr enviar las frecuencias o tono de la voz mediante señales en un cable conductor, estableciendo una conexión física entre dos partes.

En los años cincuenta, en el Instituto Tecnológico de Massachussets (MIT por sus siglas en inglés) se empieza a pensar en un sistema de telecomunicaciones totalmente distinto, basado en la transmisión de paquetes de información. Estos paquetes parten el mensaje de texto o de voz en varios paquetes de información que se mandan uno tras otro. El modelo más famoso de este sistema llegó a ser la

Internet, que se inicia en Estados Unidos en los años sesenta con la conexión de cuatro computadoras.

Vint Cerf y Bob Kahn, creadores de Internet, inventan los protocolos TCP/IP (Transmission Control Protocol/Internet Protocol). Estos "*(…) protocolos de comunicación en los que se basa la red Internet (…) han demostrado que pueden adaptarse a todos lo medios físicos de transmisión posibles*" (cable, microonda, fibra óptica, etc.) "*a todas las tecnologías y a todo tipo de aplicaciones. Los sistemas contemporáneos de fibra óptica prácticamente no tienen límite en la cantidad de información que puede transportarse de un sitio a otro, lo que nos abre posibilidades apenas imaginables para el futuro de la humanidad*"[5]. Permite que la información se segmente en los paquetes TCP/IP, y que cada paquete lleve una etiqueta que indica de dónde viene, a dónde va y la información que transporta. Ya no se trata de un circuito físico entre dos personas, sino que el mismo medio

---

[5] DE TÉRAMOND PERALTA, Guy y RETANA, Álvaro. **Establecimiento de la Red Internet Avanzada y Creación de la Red Nacional de Investigación Avanzada**. Dictada en el Seminario Costa Rica en el Mundo Digital. Fotografía e Imprenta LIL, S.A., San José, Costa Rica, 2001, pág. 15.

físico se comparte entre millones de personas, reduciendo los costos astronómicamente.

El sistema pasó de cuatro computadoras y unos cuantos usuarios en los años sesenta a cien millones de computadoras con quinientos millones de usuarios en la actualidad. Esta red ha crecido exponencialmente en tan solo treinta años.

A raíz del conflicto de poderes y de la Guerra Fría, tanto Rusia como Estados Unidos pusieron especial énfasis en las comunicaciones, pues éstas son indispensables para ganar una guerra. La preocupación de Estados Unidos era la posibilidad de que, en caso de ataque bélico de la Unión Soviética, se destruyeran todas las comunicaciones del país. Se quería un sistema de comunicaciones al que, aunque se le destrozara una parte, siguiera funcionando. Así nace Internet en 1962 en DARPA (*Defense Advanced Research Proyects Agency*) del Departamento de Defensa de los Estados Unidos de América.

En 1975 DARPA pasa la administración de su proyecto al Departamento de Comunicaciones de Defensa de Norteamérica.

Para 1980, los protocolos TCP/IP ya eran una realidad, y para 1983 fueron adoptados por ARPANET, que se componía de cientos de computadoras pertenecientes a universidades, centros de investigación militar y algunas compañías, conectadas todas entre sí.

El servicio más popular entonces era el e-mail (*electronic mail*) o correo electrónico que permitía una fácil y rápida comunicación entre diferentes personas conectadas a ARPANET. El sistema operativo que más se utilizaba en Internet era el UNIX y en especial una versión de UNIX desarrollada por la Universidad de California llamada BSD UNIX.

Para 1985 las redes locales en computadoras personales habían alcanzado un grado importante de desarrollo y esto ayudó a completar la idea de Internet; ya se podía tener redes y sub redes y se podía conectar redes de banda ancha con redes de área local. En 1986, la NSF (*National Science Fundation*), inicia un programa para interconectar recursos de super cómputo en diferentes ciudades de Estados Unidos,

construyendo una red que las uniera a los centros avanzados de cómputo.

La NSF basó sus protocolos de comunicación en los protocolos de Internet y de esta manera se originó la red que se conoció como NSFNET, que fue el corazón de Internet hasta 1995; para ese entonces se utilizaba el e-mail, ftp, telnet, gopher y otros servicios.

Es en 1992 que Tim Berners-Lee en el Centro Europeo de Investigaciones Nucleares, crea el WWW (World Wide Web). Con esta invención el Internet se vuelve accesible para el mundo entero. Cualquier persona del planeta puede navegar en la red con sólo presionar el botón del "*mouse*". Es aquí cuando se le empieza a dar un uso comercial a Internet, porque hasta el momento lo utilizaban principalmente los sectores académicos, militares y gubernamentales. El sector comercial ve un potencial grande en Internet, lo toma en sus manos y es cuando se dan las primeras transacciones comerciales, que reciben el nombre de comercio electrónico.

2. COMERCIO ELECTRÓNICO

El comercio electrónico es la base de la nueva economía. Las transacciones electrónicas permiten modernizar, mejorar y facilitar los negocios. El comercio electrónico ha tenido un crecimiento impresionante entre el consumidor y la empresa, entre empresas y entre consumidores. Esto requiere, por supuesto, que los consumidores y los productores de bienes y servicios tengan acceso y estén conectados a redes digitales. El comercio electrónico ha sido definido así:

> *"De forma amplia y sin excesiva rigurosidad, [como] todo intercambio de datos por medios electrónicos, esté relacionado o no con la actividad comercial (...). De forma más estricta, entendemos que debe circunscribirse a las transacciones comerciales electrónicas, es decir de compraventa de bienes o prestación de servicios, así como las negociaciones previas y otras actividades ulteriores relacionadas con las mismas aunque no sean estrictamente contractuales (...) desarrolladas, a través de mecanismos que proporcionan las nuevas tecnologías*

de la comunicación (como correo electrónico, o el World Wide Web, ambas aplicaciones de Internet, o el EDI - Electronic Data Interchange, en su vertiente comercial)."[6]

Para efectos de nuestro trabajo, consideraremos el concepto de comercio electrónico de forma amplia, ya que el uso de la firma digital no sólo se limita a la actividad comercial. Sin embargo, las aplicaciones más importantes para el derecho comprenden: toda operación comercial de suministro o de intercambio de bienes o servicios; acuerdos de distribución, represtación o mandato comercial, arrendamiento con opción de compra (*leasing*), contratación de obras, consultoría, ingeniería, concesión de licencias, inversiones, financiación, banca, seguros, acuerdos o concesiones de explotación, empresas conjuntas y otras formas de cooperación industrial o comercial, transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.[7]

---

[6] MARTINEZ NADAL, Apolónia. **Comercio Electrónico, Firma Digital y Autoridades de Certificación.** Segunda Edición. Madrid, España: Civitas Ediciones S.L. 2000, pág. 27.

[7] Artículo 1 de la Ley Modelo de la UNCITRAL sobre Arbitraje Comercial Internacional, Artículo 1 de la Ley Modelo de la UNCITRAL sobre Comercio

A su vez, Sarra señala que:

> *"Comercio Electrónico es un concepto amplio que involucra cualquier transacción comercial efectuada por medios electrónicos, es decir que incluiría medios electrónicos como el fax, el télex, el teléfono, los EDI (Electronic Data Interchange) e Internet."*

En este sentido, delimitaremos el término de comercio electrónico a aquel conjunto de transacciones o intercambios efectuados a través de la red, sean sistemas cerrados o abiertos. Las redes cerradas son aquellas a las que sólo determinadas personas, debidamente autorizadas, pueden tener acceso. Este sistema otorga gran seguridad a las transacciones comerciales, ya que el acceso está restringido para las personas no autorizadas, por lo cual debe haber mediado una relación previa entre las partes. Por su parte, a las redes abiertas puede acceder cualquier persona, como es

---

Electrónico y Artículo 1 de la Ley Modelo de la UNCITRAL sobre Firmas Electrónicas.

[8] SARRA, Andrea Viviana. **Comercio Electrónico y Derecho**. Primera Edición. Buenos Aires, Argentina: Editorial Astrea. 2000, pág, 279.

el caso de Internet que es la principal red abierta. En efecto, el comercio electrónico incluye las transacciones realizadas por todos los medios electrónicos, incluido el fax y el teléfono, instrumentos que no interesan en el desarrollo del tema en estudio.

El tratadista, Jijena Leiva define el comercio electrónico como:

> *"(...) el intercambio telemático de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles o en un pedido electrónico de bienes tangibles."*

El autor, Paladella indica que el comercio electrónico

> *"no solo incluye la compra y venta electrónica de bienes o servicios, que es el concepto común que se*

---

[9] JIJENA LEIVA, Renato Javier. **Comercio Electrónico y Derecho. La Problemática Jurídica del Comercio Electrónico.** Universidad Católica de Valparaíso, 1999. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/index.cgi?/N% citado por KNORR BRISEÑO, Jolene Marie y ROLDÁN SAUMA, Marcelo. **La Protección del Consumidor en el Comercio Electrónico.** Primera Edición, San José, Costa Rica: IJSA. 2001, pág. 58.

tiene, sino que también incorpora el uso de las redes para actividades anteriores o posteriores a la venta, como son: la publicidad, la búsqueda de información, el tratamiento de clientes y proveedores, incluso inversores, trámites ante autoridades de control y fiscalización, la negociación de condiciones de compra, suministro, etc., la prestación de mantenimiento y servicios postventa y la colaboración entre empresas."[10]

El gran y desmesurado desarrollo que ha tenido el comercio electrónico en la red, instrumento que se caracteriza por su falta de regulación, ha planteado un sinnúmero de problemas jurídicos, dentro de los que se enumeran:

- La validez de la contratación electrónica, la formación del consentimiento, la competencia jurisdiccional y la legislación aplicable.

---

[10] DE PALADELLA SALORD, Carlos. **El Derecho en la Era Digital. Aspectos Jurídicos de las Nuevas Tecnologías de la Información y de las Comunicaciones**, Argentina, 1999. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/index.cgi?/N%FAMERO 14 - septiembre de 1999/5&0. citado por KNORR BRISEÑO, Jolene Marie y ROLDAN SAUMA, Marcelo. Op. Cit., pág. 59.

- La firma digital, la prestación de servicios de certificación y la validez de los mensajes de datos o documentos electrónicos.
- La protección del consumidor.
- El establecimientos de medios de pago seguros.
- La protección de la propiedad intelectual.
- La legislación sobre telecomunicaciones, para lograr la masificación del acceso a Internet.
- Tributación en Internet, esto se ejemplificará más adelante.
- Protección penal, a través de la tipificación del fraude informático.[11]

Entre las áreas que pueden requerir especial atención, podemos mencionar además el derecho a la privacidad y la libertad de expresión.

A su vez, Jijena Leiva, señala, entre otros problemas:

---

[11] MAGLIONA MARKOVICHT, Claudio Paul. **Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico** en Revista Electrónica de Derecho Informático. No. 4. 2001, disponible en http://derecho.org/redi/

- El momento y lugar en que se forma el consentimiento entre los contratantes.
- La necesidad de proteger la privacidad de las personas contratantes.
- El necesario reconocimiento legal de los mecanismos de encriptación o protocolos de seguridad para las transacciones.
- El valor probatorio o la admisibilidad en un proceso de la información contenida en un ordenador transmitida vía redes.
- La protección de la propiedad intelectual e industrial.[12]

Hay consenso en la doctrina sobre la importancia de regular la firma digital y los mecanismos de encriptación para otorgar confianza y seguridad a las negociaciones comerciales. El pleno desarrollo del comercio electrónico va ligado a la seguridad que se puede brindar a las transacciones comerciales, solución con la que puede

---

[12] JIJENA LEIVA, Renato. **Firma Digital y Entidades Certificadoras. Regulación Legal en la Administración Pública Chilena** en Revista Electrónica de Derecho Informático. Chile. Documento sin fecha, disponible en http://v2.vlex.com/global/redi/detalle_doctirna_redi.asp?articulo=10789

contribuir la firma digital, en los diferentes tipos de transacciones vía red.

3. CLASES DE COMERCIO ELECTRÓNICO

El comercio electrónico se ha clasificado tradicionalmente de acuerdo a la naturaleza de quienes intervienen en él. De esta forma encontramos:

A. COMERCIO ELECTRÓNICO ENTRE EMPRESAS Y CONSUMIDORES, COMERCIO ELECTRÓNICO ENTRE EMPRESAS Y COMERCIO ELECTRÓNICO ENTRE CONSUMIDORES

i. Comercio electrónico entre empresas y consumidores

Internet permite un aumento de la competencia entre oferentes de bienes y servicios. Los consumidores se benefician con la gran variedad de bienes y servicios a un bajo costo, la información con la que cuentan antes de realizar su compra, y además la posibilidad de realizar sus compras desde su propia

casa, examinando las diferentes opciones en todos los lugares del mundo.

Con este fenómeno se produce la desintermediación, donde el consumidor compra los bienes o servicios directamente del vendedor, que puede incluso encontrase en otro país. Son cada vez más frecuentes las transacciones internacionales, donde la transacción entre el comprador y el vendedor se efectúa en diferentes países. Esto cambia el viejo paradigma del derecho comercial internacional, donde el consumidor compraba un producto hecho en el extranjero, de un vendedor del mismo país del consumidor.[13]

ii. Comercio electrónico entre empresas

El comercio electrónico ha revolucionado la forma de organización de las empresas. La red provee un intercambio inmediato de comunicación, lo que facilita que, por ejemplo, las empresas puedan comunicarse de forma inmediata con sus distribuidores, disminuyendo costos. El problema de falta de

[13] KNORR BRISEÑO, Jolene Marie y ROLDAN SAUMA, Mauricio. Op. Cit.

seguridad y la incerteza de la transacción es menor que el comercio electrónico entre empresas y consumidores, porque por lo general se da entre partes que ya tienen negociaciones previas establecidas. [14]

iii. Comercio electrónico entre consumidores

Este tipo de actividad consiste en transacciones directas entre consumidores. El ejemplo más vivo de este tipo de comercio son las casas de subasta virtuales, donde los vendedores colocan sus productos, los interesados hacen ofertas de precio y se le vende al mejor oferente. Así, nace una relación directa entre el vendedor y el comprador, generalmente utilizando el correo electrónico como medio de comunicación para ponerse de acuerdo en la forma del intercambio del producto y el modo de pago. La casa de subasta funciona solamente como contacto y no interviene en la relación entre el vendedor y el comprador.

---

[14] KNORR BRISEÑO, Jolene Marie y ROLDAN SAUMA, Mauricio. Op. Cit.

B. COMERCIO ELECTRÓNICO DIRECTO E INDIRECTO

Otra clasificación del comercio electrónico es el directo e indirecto. El directo es la entrega en línea de bienes intangibles, "*se dice que es directo porque tanto la transacción como la entrega del bien se realiza directamente a través Internet; tal es el caso de la compraventa de software, servicios legales o música. Por su parte el comercio electrónico de bienes tangibles, a diferencia del primero lo único que se realiza en línea es la negociación ya que la entrega es material.*"[15] Este segundo es el comercio electrónico indirecto.

C. COMERCIO ELECTRÓNICO INTERNO Y COMERCIO ELECTRÓNICO INTERNACIONAL O TRANSFRONTERIZO

Esta clasificación se da en razón del ámbito geográfico de ejercicio.[16] El interno se refiere a las transacciones

---

[15] KNORR BRISEÑO, Jolene Marie y ROLDAN SAUMA, Mauricio. Op. Cit., pág. 63.

[16] AGUERO GUIER, Esteban y ECHERVERRIA HINE, Leonor. **Comercio Electrónico: El Contrato de Intercambio Electrónico de Datos (EDI). Estudio de Derecho**

realizadas dentro de un mismo país y el internacional es el realizado entre dos o más países.

D. COMERCIO ELECTRÓNICO ABIERTO Y COMERCIO ELECTRÓNICO CERRADO

El comercio electrónico abierto es el ejercido a través de las redes abiertas. Por su lado, el comercio electrónico cerrado, es el que se celebra por las redes cerradas, excluyendo a todas las personas no autorizadas y con quien no ha medido una relación contractual previa.

E. COMERCIO ELECTRÓNICO REGULADO DE MANERA INTERNA O PRIVADA Y COMERCIO ELECTRÓNICO REGULADO POR LEY

El comercio electrónico regulado de manera interna está regido por contratos privados, celebrados por la partes de previo al comienzo de la relación comercial. Son conocidos generalmente como contratos previos o acuerdos de

---

Comparado. Tesis para optar el título en licenciado en Derecho. Facultad de Derecho de la Universidad de Costa Rica, San José, Costa Rica, 2002.

intercambio. El comercio electrónico regido por ley, como su nombre lo indica es, aquel que se encuentra regulado por el derecho positivo de un país, región u organización internacional, sea mediante leyes, tratados internacionales o recomendaciones.[17]

[17] AGUERO GUIER, Esteban y ECHERVERRIA HINE, Leonor. Op. Cit.

CAPITULO II: LA FIRMA DIGITAL

El comercio electrónico presenta grandes riesgos e incertidumbres, ya que cualquier persona puede penetrar la red e interceptar el intercambio de datos. Los riesgos más importantes son: que el autor y la fuente del mensaje sean suplantados, que el mensaje sea alterado, ya sea de forma accidental o de forma maliciosa, que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido y que el contenido del mensaje sea leído por una persona no autorizada.[18] Por tanto, es necesario asegurar que el mensaje proviene de la persona que dice ser quien lo envía, que éste no ha sido alterado en el camino, que el emisor no pueda negar su envío ni el destinatario su recepción y garantizar la confidencialidad. En este sentido, la firma digital asegura la autenticación, la integridad del mensaje, el no rechazo o no repudio en origen y en destino y la confidencialidad del mensaje. La firma digital permite que

---

[18] DELPIAZZO, Carlos E. **Relevancia Jurídica en la Encriptación y la Firma Electrónica en el Comercio Actual**. Documento sin fecha. Documento sin numeración.

las partes en un negocio puedan autenticar todos y cada uno de los mensajes que hayan intercambiado.

I. CONCEPTO DE FIRMA DIGITAL

La firma digital es un mecanismo de seguridad, basado en un sistema de encriptación. Su funcionamiento y validez depende de la criptografía, los certificados digitales y las autoridades de certificación. Para entender a fondo el concepto de firma digital, es necesario comprender los aspectos técnicos de su funcionamiento.

1. CRIPTOGRAFÍA

Etimológicamente, el término criptografía quiere decir "escritura secreta", proviene del griego "krypto" ($\kappa\rho\upsilon\pi\tau\omega$) que significa esconder y "grafe" ($\gamma\rho\alpha\varphi\eta$) escritura, y es

definido como "el arte de escribir con clave secreta o de un modo enigmático".[19]

El tratadista Cornejo López define la criptografía como:

> *"aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Abarca por tanto a la Criptografía (datos, texto e imágenes), Criptofonía (voz) y al Criptoanálisis (ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave)".*[20]

Cifrar consiste en transformar una información (texto claro) en otra inteligible (texto cifrado), según un procedimiento y

---

[19] PASCALE, Maricarmen. **Firma Digital.** Uruguay. Documento sin fecha. Documento sin numeración.

[20] CORNEJO LOPEZ, Valentino. **Una Realidad Mexicana, La Firma Electrónica y la Participación del Notario Mexicano** en Revista Electrónica de Derecho Informático. Documento sin fecha. Documento sin numeración, disponible en: http://vz.vlex.com/global/redi/detalle_doctrina_redi.asp?atriculo=107899

usando una clave determinada, logrando que solo quien conozca dicho procedimiento y clave pueda acceder a la información original. La operación inversa se llama descifrar.

Encriptar un texto significa aplicarle un algoritmo que, en relación a una variable (clave de encriptación), lo transforma en otro texto incomprensible e indescifrable por parte de quien no posee la clave. La función es reversible, por lo cual la aplicación del mismo algoritmo o un algoritmo complementario y la misma clave al texto cifrado devuelve el texto original.

La criptografía nació alrededor del año 2000 a.C. en Egipto, donde los jeroglíficos eran usados para decorar las tumbas de los reyes y faraones. Estos jeroglíficos contaban la historia de la vida del faraón. Sin embargo, los jeroglíficos no pueden considerarse criptografía, pero sí su primer paso ya

que sólo podían ser entendidos por personas con conocimientos suficientes.[21]

Los espartanos inventaron un mecanismo de criptografía que consistía en cortar un royo de papiro, envolverlo alrededor de la scítala, que era un bastón de madera, cubriendo toda la superficie sin dejar ningún espacio y escribir el mensaje. Se enviaba el papiro sin el bastón y solamente el que tenía un bastón con el mismo diámetro podía descifrar el mensaje.[22] Con este ejemplo reconocemos los elementos constitutivos de cualquier sistema criptográfico:

- El algoritmo: es un conjunto de operaciones que permite hacer incomprensible el mensaje descomponiéndolo en una secuencia de caracteres no inteligibles inmediatamente. En este caso seria la acción de envolver el bastón con el papiro y escribir sobre él.
- La clave: el elemento que, asociado a un algoritmo criptográfico, permite la encriptación y la

---

[21] Anónima. **Introducción a la Criptografía. El Rincón de Quevedo.** Sin fecha, documento sin numeración, disponible en http://rinconquevedo.iespana.es/Criptografia/criptografia.htm

[22] Anónimo. **Introducción a la Criptografía. El Rincón de Quevedo.** Op. Cit.

desencriptación del texto cifrado. En el caso descrito sería el bastón.

La encriptación nace y se desarrolla para fines de seguridad en la transmisión de mensajes militares. Julio César utilizó un sistema de encriptación cuando quería intercambiar mensajes con los comandantes de su legión, el llamado método de traslación. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante.[23] A manera de ejemplo, tendríamos la siguiente tabla de equivalencia:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

En este sentido, la palabra "FIRMA DIGITAL", utilizando este sistema sería: "ILUPD GLJWAO". Para descifrar el mensaje, tenemos que ver el alfabeto y sustituir cada letra por la que está tres posiciones antes. En este caso el algoritmo seria

[23] Anónimo. **Introducción a la Criptografía. El Rincón de Quevedo.** Op. Cit.

sustituir cada letra por otra, según una clave previamente establecida, y la clave sería 3 letras hacia adelante del abecedario.

El fundamento de la firma digital es la criptografía basada en las nuevas tecnologías electrónicas y digitales. Se diferencia de los ejemplos descritos anteriormente, porque no nace de la invención humana. El método de encriptación más utilizado actualmente para efectuar transacciones seguras en la Internet está basado en el algoritmo RSA, inventado por R. L. Rivest, A. Shamir y L. Adleman en 1977. El algoritmo RSA está basado en el Teorema Fundamental de la Aritmética, o Teorema de la Factorización Única, corolario del Primer Teorema de Euclides y cuya seguridad depende de la dificultad de encontrar los factores primos de un número.[24] Los sistemas criptográficos modernos son mucho más fiables que la sustitución y transposición clásicas, los cuales son vulnerables a ser descifrados fácilmente, pues si existe alguien que las invente, existe también alguien que puede encontrar la clave para recuperar el contenido original.

[24] RSA Laboratories. **RSA-Based Cryptographic Schemes.** Estados Unidos de América, 2002. Documento sin numeración disponible en: http://www.rsasecurity.com/rsalabs/rsa_algorithm

Actualmente, se utilizan métodos que combinan los dígitos del mensaje con otros, o bien algoritmos de gran complejidad, como el RSA descrito arriba. Por ejemplo, un ordenador tardaría doscientos millones de años en interpretar las claves de encriptación de 128 bits. [25]

Hay dos tipos de encriptación utilizados para firmar digitalmente un documento electrónico: la encriptación simétrica, que obliga al emisor y al receptor del mensaje a utilizar la misma clave para encriptar y desencriptar el mensaje, y la encriptación asimétrica de claves públicas, la cual está basada en el concepto de pares de claves o claves complementarias, de tal forma que cada uno de los elementos del par (una clave) puede encriptar información que sólo el otro componente del par, la clave complementaria, puede desencriptar. El par de claves se asocia con una de las parte. Así, un componente del par (la clave privada) solamente es conocido por su propietario, mientras que la

[25] Anónimo. **Introducción a la Criptografía. El Rincón de Quevedo.** Op. Cit.

otra parte del par (la calve pública) es de conocimiento universal.[26]

A. La Encriptación Simétrica o de Clave Privada

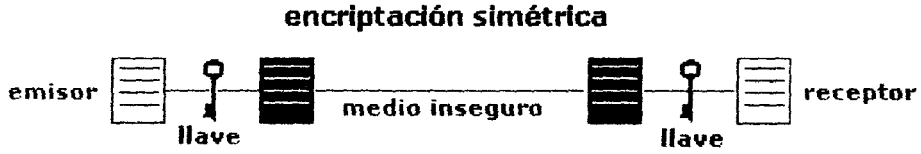
Es el sistema de cifrado más antiguo. Para cifrar y descifrar un mensaje, las partes deben haber intercambiado con anterioridad la clave correspondiente, que es la clave privada o simétrica. Se le llama simétrica porque las partes tienen la misma clave para encriptar el mensaje y para desencriptarlo. Dicha clave debe ser secreta, por lo que la protección de la clave es esencial. Este sistema es idóneo para la autenticación de las partes, pero presenta varias desventajas. Por ejemplo, si un tercero descubre cuál es la clave, puede descifrar el mensaje sin estar autorizado para hacerlo. Por otro lado, es un sistema que no funciona frente a terceros que no conocen la clave. Este sistema es más

---

[26] RAMOS SUÁREZ, Fernando. **Como aplicar la nueva normativa sobre Firma Electrónica** en Revista Electrónica de Derecho Informático. España. 2000. Documento sin numeración, disponible en http://publicaciones.Derecho.org/redi/No._19_-_Febrero_del_2000/1

rápido que la encriptación de llave pública, y resulta útil para el cifrado de grandes volúmenes de datos.

Un esquema que ilustra lo dicho es el siguiente:



B. La Encriptación Asimétrica o de Clave Pública

La criptografía de clave pública es un método especial de encriptación y desencriptación de mensajes por medio de un par de llaves relacionadas matemáticamente entre sí: una "clave o llave pública" que es de conocimiento público, y una "clave o llave privada", conocida sólo por su titular (o a veces ni siquiera por éste), como el caso de tarjetas inteligentes a la que se accede por medio de un número de identificación personal. Cualquiera de las dos llaves puede

ser utilizada para la encriptación o desencriptación de un mensaje.

Básicamente, la criptografía de llave pública se basa en la dificultad de revertir ciertas relaciones matemáticas, como se expuso anteriormente para el algoritmo RSA. Por ejemplo, multiplicar para encontrar un producto es fácil, mientras que factorizar para encontrar los números que fueron originalmente multiplicados entre sí es más difícil. Con números lo suficientemente grandes, un número podría ser guardado en secreto y el otro número podría ser publicado sin temor de que el número secreto vaya a ser adivinado por un tercero no autorizado. En ese sentido, cualquiera puede obtener el número público y encriptar un mensaje de forma tal que sólo el poseedor del número privado lo pueda descifrar.

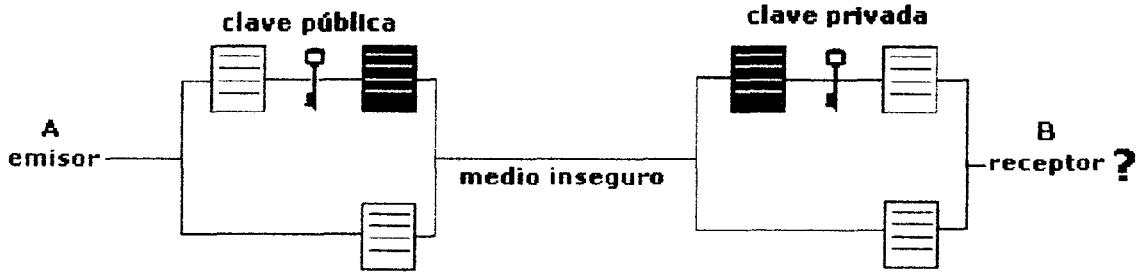
La tecnología de llave pública es de uso predominante. Si un mensaje es encriptado con una llave privada, cualquier persona podría tener acceso a su contenido utilizando la correspondiente llave pública. Garantiza que el autor del mensaje es, y sólo puede ser, el dueño de la llave privada,

además asegura la integridad del mensaje y el no repudio del mismo. Evidentemente, este procedimiento no garantiza la confidencialidad sobre el contenido del mensaje. Para lograr esto, es necesario además, encriptar el mensaje con la llave pública del receptor.

De esta manera, cuando una parte quiere verificar la firma digital generada por otra, quien verifica debe conocer la clave pública del firmante. Al igual, el emisor de un mensaje que desea cifrarlo, para asegurar que sólo el destinatario va a leer el mensaje, necesita la clave pública del destinatario. Ambos son usuarios de clave pública, tanto quien desea verificar una firma, como quien desea emitir un mensaje cifrado. En otras palabras, si una parte desea recibir mensajes encriptados, se utiliza la llave del receptor para encriptar el mensaje y sólo el receptor, con su llave privada, podrá desencriptar el mensaje. A su vez, el titular de la clave privada puede enviar mensajes encriptados con su llave privada, y éstos serán desencriptados con su llave pública, en este sentido el mensaje no es confidencial

puesto que cualquier persona puede descifrar el mensaje, pero garantiza la autoría del emisor.

A continuación se presenta un esquema que ejemplifica el sistema descrito:



Debemos tener claro, que si bien la criptografía otorga seguridad a las transacciones efectuadas en las redes abiertas de comunicación, existen ciertos peligros, que van más allá de la tecnología: el cuidado que deben tener las personas al usar estos sistemas. Por ejemplo, la criptografía no puede proteger documentos que no se encriptaron, ni puede proteger contra llaves robadas, o contra ataques al sistema, y no puede proteger contra error o traición humana.

2. FIRMA DIGITAL

Es importante tener claro que los términos "firma digital" y "firma electrónica", aunque a veces se usan indistintamente, no son sinónimos. "Firma electrónica" es un término amplio que comprende cualquier símbolo electrónico usado por una parte con la intención de autenticar un registro. Cubre una variedad de tecnologías, incluyendo firmas digitales, códigos y marcas distintivas. En otras palabras, "firma electrónica" designa cualquier método de identificación, como por ejemplo letras, caracteres o símbolos, manifestados por medios electrónicos o similares, ejecutados o adoptados por una parte en una transacción con la intención de autenticar un escrito. Por el contrario, "firma digital", según lo señalado, se basa en la criptografía y está comprendida dentro del concepto más amplio de firmas electrónicas.

La firma digital no debe ser definida con base en un sistema específico de encriptación, ya que de acuerdo al **principio de neutralidad tecnológica**, no se debe excluir ninguna tecnología, sino que se debe acoger toda eventual innovación

técnica en este campo. Este principio pretende considerar aptas para el comercio electrónico o, en nuestro caso, la firma digital, no sólo las tecnologías existentes en este momento sino también las futuras, sin necesidad de tener que hacer constantes modificaciones a la legislación. Sin embargo, actualmente, no hay duda que la firma digital más segura es la basada en la infraestructura de la llave pública, por lo que le daremos énfasis a dicha firma más adelante.

Se ha establecido que:

> "*La firma digital, técnicamente, es un conjunto o bloque de caracteres que viaja junto a un documento, fichero o mensaje y que puede acreditar cuál es el autor o emisor del mismo y que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación*".[27]

---

[27] Asociación de Usuarios de Internet. **Preguntas más Frecuentes**. Mesena, Madrid. Documento sin fecha. Documento sin numeración, disponible en: http://www.aui.es/biblio/documentos/consejos_seguridad/faqs-seguridad.htm

El proyecto de ley costarricense sobre firma digital: Proyecto de Ley de Firma Digital y Certificados Digitales (No. 14.276), dice que la firma es:

> *"(...) el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge."*

Podemos definir la firma digital como una secuencia de caracteres alfanuméricos que contiene los elementos que autentican al remitente aplicando una clave privada, garantizando así la integridad, autenticidad y el no repudio del mensaje.

La firma digital debe garantizar lo siguiente:

- Integridad: es la certeza del mensaje, es decir, que asegura que no ha existido ninguna manipulación posterior de datos. Cualquier modificación, aunque sea ínfima, puede ser detectada.

- Autenticidad: es la certeza del emisor, acredita quién es su autor. Se tiene la seguridad que las personas que intervienen en el proceso de comunicación son las que dicen ser. Permite identificar unívocamente al signatario.
- No rechazo o no repudio: no se puede negar la autoría de un mensaje enviado. Una vez que el emisor envía un mensaje, éste no puede negar ser el autor de dicho envío. No puede retractarse en el futuro de las opiniones o acciones consignadas en él, ni de haberlo empleado.
- Confidencialidad: que ninguna persona que no esté autorizada pueda leer el mensaje.

Por su lado, la función de una firma manuscrita es asegurar que la persona que firma el documento conoce el contenido del mismo y tiene, además, la intención de verse vinculado por él. La función de la firma digital es la misma, sólo que operando en el campo electrónico. A diferencia de una firma manuscrita, que es únicamente del firmante, pero consistente en todos los documentos que éste firme, la firma digital es

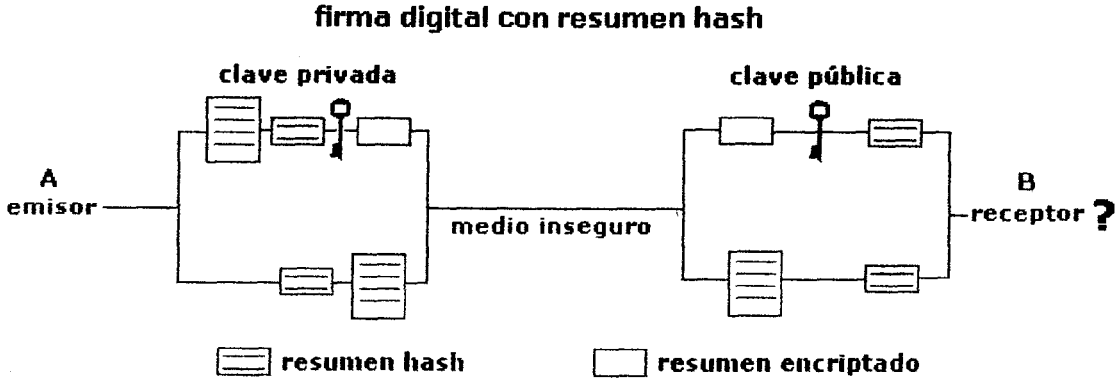
única en cada documento que se firma. Esto es así pues la firma digital es un derivado del documento que va a ser firmado digitalmente. Consecuentemente, cualquier cambio en el documento, produciría un cambio en el resultado de la firma digital

El uso de una firma digital basada en el sistema de clave pública involucra dos procesos: uno realizado por el firmante y el otro por el receptor. La creación de la firma digital utiliza un sistema denominado *"Función Hash"* o *"Hash Function"*. Este sistema resume el contenido del mensaje y da un resultado derivado del mensaje firmado con una llave privada dada, que además es única a éstos. Para que el resultado sea seguro, la posibilidad de que la misma firma digital haya podido ser creada de la combinación de otro mensaje o de otra llave privada, tiene que ser ínfima. En segundo lugar, la verificación de la firma digital es el proceso de revisarla con referencia al mensaje original y una llave pública dada, de manera que se determine que la firma digital fue creada para ese mismo mensaje usando la llave privada que corresponda a la llave pública referida.

El proceso en la creación de una firma digital de llave pública es el siguiente:

- El emisor genera un resumen del documento mediante una *función hash.*
- El emisor cifra el resultado de la *función hash* con su clave privada. De esta forma obtiene su firma digital, que es única para cada documento.
- Envía al receptor el mensaje original junto con la firma.
- El receptor descifra el resumen del mensaje mediante la clave pública del emisor.
- Aplica al mensaje la *función hash* para obtener el resumen.
- Compara el resumen recibido con el obtenido a partir de la *función hash*. Si son iguales, el receptor puede estar seguro de que quien ha enviado el mensaje es el emisor y que el contenido del mensaje no ha sido modificado.

El anterior proceso se ejemplifica mediante el siguiente grafico:



3. AUTORIDADES DE CERTIFICACIÓN

Subsiste el problema de verificar que la clave corresponde realmente a la persona o entidad que dice poseerla. Es aquí donde entran las autoridades de certificación, que son las terceras partes de confianza (*trusted third parties*). Su función es determinar que una clave corresponde a su titular. Se encargan de registrar las claves públicas de los usuarios y las certifican con lo que se llama un *certificado de clave pública*. Este certificado, es un archivo que contiene la clave pública del usuario, sus datos personales y que es firmado por la autoridad de certificación con su propia clave

privada. Así, la autoridad certifica y da autenticidad a esa certificación.[28]

Las autoridades de certificación permiten verificar que una clave pública pertenece a una determinada persona, evitando que alguien utilice una clave falsa para suplantar la personalidad de otro.[29] Brinda seguridad y confianza a todos los elementos de una comunicación segura, a través de las redes abiertas, como Internet.

El Real Decreto Ley-Ley14/1999 de España, llama a las Autoridades de Certificación "Prestadores de servicios de certificación", y las define como:

> *"aquellas personas físicos o jurídicas que expiden certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica."*

---

[28] PASCUALE, Maricarmen. Op cit.
[29] RAMOS SUAREZ, Fernando. **La Firma Digital: Aspectos Técnicos y Legales.** 2000. Documento sin numeración, disponible en http;//www.marketingycomercio/numero14/00abr firmadigital.htm

Las autoridades de certificación deben estar sumamente preparadas y deben poseer las mejores tecnologías. No es cualquiera el que está capacitado para efectuar esta función. Las autoridades de certificación deben estar al tanto de las realidades y procedimientos técnicos de quienes intervienen en el comercio electrónico.

Las autoridades de certificación, a su vez, pueden ser certificadas y ésta segunda autoridad que certificó también puede ser certificada. Es una cadena de certificaciones que puede llegar hasta donde quiera el usuario. La llave pública de las autoridades de certificación, entonces, debe ser igualmente de conocimiento universal. Lo que se pretende con esto es que el usuario sepa de forma fehaciente que ha sido una Tercera Parte Confiable la que emitió el certificado válido y vigente.[30]

---

[30] JIJENA LEIVA, Renato. **Firma Digital y Entidades Certificadoras. Regulación Legal en la Administración Pública Chilena.** Op Cit.

4. CERTIFICADOS DIGITALES

La tratadista Pascuale, define el certificado como:

> Un "*documento digital que identifica a la autoridad certificadora que lo ha emitido, identifica al firmante del mensaje o transacción, contiene la clave pública del firmante, y contiene a su vez la firma digital de la autoridad certificadora que lo ha emitido. Es la manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas digitales o de la integridad de un mensaje.*"[31]

El proyecto de ley costarricense de Firma Digital y Certificados Digitales, explica el certificado como:

> "*(...) la certificación digital que vincula unos datos de verificación de firma a un signatario y confirma su identidad.*"

---

[31] PASCUALE, Maricarmen. Op cit.

Los certificados son documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. Es decir, atestiguan que una clave pública pertenece a un determinado individuo o entidad y, a la vez, tratan de evitar que una persona utilice una clave haciéndose pasar por otro.

Básicamente, los certificados digitales deben contener:[32]

- El código único que identifica al certificado.
- La identificación de la autoridad certificadora que expide el certificado.
- La firma digital de la autoridad de certificación que expide el certificado, la cual da fe que el certificado expedido es válido y ha sido emitido de acuerdo con sus prácticas de certificación.
- La identificación del signatario, sea por su nombre y apellidos o por un seudónimo que conste de manera inequívoca.

---

[32] ÁLVAREZ MARAÑÓN, Gonzalo. **Los Secretos de la Firma Electrónica.** España.2000. Documento sin numeración, disponible en: http://www.idg.es/iworld/articulo.asp?id=106760&n=25&sec=iworld

- Los datos de verificación de la firma del emisor, es decir, la clave pública.
- El período de validez del certificado, desde cuándo y hasta cuándo es válido.
- Los límites de uso del certificado, en caso que sean previstos, como por ejemplo, compra a través de Internet, acceso a bancos, etc.
- Los límites de valor de las transacciones para las que puede utilizarse el certificado, si se indican. Esto permite controlar que con un certificado no puedan efectuarse transacciones por un valor superior al establecido en el certificado.

Esta lista no es taxativa. Un certificado puede contener mayor o menor información. Para que sea válido un certificado debe contener una información mínima que es básicamente, la clave pública y un nombre, el nombre de la autoridad certificante o certificadora, el número de serie del certificado y la firma digital que otorga el certificado.

Existen diferentes tipos de certificados:[33]

- Certificados de identificación: identifican y conectan un nombre a una clave pública.
- Certificados de autorización: ofrecen información del usuario, por ejemplo, su dirección, sus antecedentes, su edad, etc.
- . Certificados que colocan a la autoridad de certificación en el rol del notario: dan fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.
- *Digital time-stamp certificates*: los podemos traducir como "certificados que sellan el tiempo". Determinan el día y hora en que el mensaje fue digitalmente firmado. Permiten determinar si la firma digital fue ejecutada dentro del periodo de validez del certificado.

A manera de ejemplo, vamos a describir paso a paso como se obtiene un certificado ante una autoridad certificadora, en este caso ante la comapañía VeriSign.[34]

---

[33] RAMOS SUÁREZ, Fernando. Op. Cit.

1. Primero, hay que conectarse al centro de identificadores digitales de VeriSign, en la siguiente dirección:

   http://www.verisign.com/products/individual

2. Luego hay que seleccionar el botón que dice: "Enroll Now".

3. Seguidamente, se selecciona el identificador "Class 1 Digital ID". Esto permite enviar y recibir correo cifrado.

4. Hay que rellenar cuidadosamente el formulario que aparece en pantalla, y aportar varios datos como el nombre y apellido y una dirección de correo electrónico válida. El certificado quedará ligado a la dirección de correo electrónico que se especifique. Una vez terminado el formulario se pulsa el botón que dice: "*Accept*".

5. El navegador en este momento genera la clave pública y la clave privada.

---

[34] VeriSing, Inc, es un proveedor de servicios digitales que permite que las compañías y consumidores ejerzan sus actividades en el comercio electrónico de una forma segura. Tiene una infraestructura que maneja más de seis y medio billones de transacciones al día. Es una autoridad de certificación.

6. Después se le indica al usuario que dentro de una hora recibirá un correo electrónico, que indicará las instrucciones para obtener un certificado digital. Se especifica una página de Internet y un PIN.
7. Cuando se reciba el correo, se debe utilizar el mismo ordenador y el mismo navegador para conectarse a la página de Internet y se introduce el PIN, a no ser que se lea automáticamente.
8. Una vez hecho esto, el navegador guiará todos los pasos a seguir para la instalación del programa.

La mayoría de las legislaciones establecen ciertos requisitos que deben seguir los certificados para que tengan validez legal, a los que se les llama *certificados reconocidos*.

El proyecto de ley costarricense de firma digital define el certificado digital como:

> "*(...) el certificado que cumple con los requisitos establecidos en la presente ley y su reglamento, y*

que vincula un documento digital con determinada persona como sus signatario, mediante un proceso seguro de certificación y es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la Autoridad Competente de acreditación."

5. FIRMA DIGITAL AVANZADA

Estudiados los conceptos de firma digital, autoridades de certificación, certificados y certificados reconocidos, podemos entonces desarrollar qué se entiende por firma digital avanzada.

La firma digital avanzada es la que se puede comprobar empleando un certificado reconocido. Debe cumplir con los requisitos señalados en las diferentes legislaciones.

En Costa Rica, el proyecto de ley lo define así:

"Es la firma digital certificada por un prestador de servicios de certificación acreditado ante la autoridad competente de acreditación."

Esta firma tiene las siguientes características:

- Que la firma permita la identificación del signatario y haya sido creada por medios que éste mantiene bajo su exclusivo control, de manera que esté vinculada únicamente a él y a los datos a los que se refiere, lo que permite que se detecte la más ínfima modificación posterior del mensaje.
- Que la firma se haya generado con un certificado reconocido.
- Que la autoridad de certificación cumpla con lo establecido en la legislación.

La firma digital avanzada tiene reconocimiento legal y se equipara de forma absoluta con la firma manuscrita, con las consecuencias que más adelante estudiaremos.

6. DOCUMENTO ELECTRÓNICO

La firma digital es un dispositivo que se adjunta a un mensaje o documento electrónico y, por esta razón, es importante definirlo.

En el sentido tradicional, documento se refiere al instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje. Así, el documento electrónico, que es una secuencia informática de bits (números binarios) que pueden representar cualquier tipo de información,[35] cumple con los requisitos del documento en soporte de papel, en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el binario) sobre soporte (cinta o disco), destinado a durar en el tiempo.[36]

---

[35] ARCE, Alfonso José y DÍAZ LANNES, Federico Santiago. **La Firma Digital. Aspectos Jurídicos. Su Aplicación a las comunicaciones previstas por la ley 22.172** en Revista Electrónica de Derecho Informático. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107423

[36] CORNEJO LÓPEZ, Valentino. Op. Cit.

La Ley sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha firma, promulgada en Chile, define en su artículo 2 el documento digital como:

> "*toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior*".

Asimismo, el proyecto de ley de Costa Rica número 14.276, le da el siguiente significado al documento electrónico:

> "(...) *información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra naturaleza, y que se puede recuperar o reproducir en una forma perceptible o inteligible.*"

En el ordenamiento jurídico costarricense, las dos normas más importantes sobre documento electrónico son el artículo 6 bis de la Ley Orgánica del Poder Judicial y el 368 del Código Procesal Civil, que se citan a continuación y serán analizados con detenimiento posteriormente.

El artículo 6 *bis* de la Ley Orgánica del Poder Judicial establece que:

> *"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."[El destacado no es del original]

Por otra parte, el artículo 368 del Código Procesal Civil establece que:

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

II. ÁMBITOS DE APLICACIÓN DE LA FIRMA DIGITAL

La firma digital tiene consecuencias en todos los ámbitos de la vida humana. Desde la medicina hasta lo ambiental. Por ejemplo, un doctor va con su computadora portátil a visitar a un paciente, suscribe con su firma digital una receta al paciente, lo manda vía Internet a una farmacia y ésta lo lleva hasta la casa del paciente. El paciente, lo había pagado ya digitalmente. En este caso el paciente no tuvo ni

que moverse de la cama. Esto es un ejemplo sumamente simple de la vida cotidiana.

Es imposible describir y dar ejemplos del impacto que tiene la firma digital en los diferentes aspectos de la vida humana. Su ámbito de aplicación es infinito. Por esta razón, delimitaremos este subtítulo a dos ejemplos específicos y recientes que se están dando actualmente: la aplicación en el ámbito tributario y en los sistemas de votación "*en línea*", dejando de lado lo estrictamente jurídico ya que lo estudiaremos en el título segundo.

En Chile, en materia de "*e-government*", que se refiere a las transacciones en las cuales participa el Estado, el Servicio de Impuestos Internos implementó un sistema de presentación electrónica por Internet de las declaraciones tributarias. Para esto se modificó el Código Tributario Chileno, de manera que las declaraciones juradas de impuestos de venta (IVA) y de renta, puedan ser leídas en soportes tecnológicos. Para poner a operar un sistema como este se requiere implementar la firma digital, para identificar a la persona, asegurar la

integridad y contenido del documento enviado y evitar la posible repudiación por parte del contribuyente del envío de la declaración de impuestos.[37] En caso que actúe un apoderado en nombre de una persona jurídica, la autoridad certificadora deberá actuar como entidad de registro y solicitar y guardar la documentación que demuestra que dicho representante tiene la capacidad legal de ejercer tal representación. No sólo se hace la declaración de impuestos por Internet sino que, además, se implementó un sistema de pago de impuestos en línea. Existen dos alternativas de pago: se puede hacer por medio de un convenio de pago que el contribuyente previamente establezca con un banco o mediante el uso de certificados digitales específicos que deberán ser aceptados por una institución financiera que efectúe cargos directos en las cuentas bancarias de los contribuyentes, a la cual el Servicio de Impuestos Internos le envía el certificado digital del contribuyente y los datos del pago correspondiente.[38]

---

[37] JIJENA LEIVA, Renato. **Impuestos, Firmas y Certificados Digitales** en Revista Electrónica de Derecho Informático. Chile, 2001. Número 8, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107924

[38] JIJENA LEIVA, Renato. **Impuestos, Firmas y Certificados Digitales.** Op Cit.

En España, el pago de impuestos por la red es una realidad, con la presentación de las declaraciones juradas ante la Agencia Estatal de Administración Tributaria (A.E.A.T.). La información cifrada de la declaración jurada conjuntamente con el pago electrónico, es remitida a la computadora personal del contribuyente, previa solicitud de éste a la Fabrica Nacional de Moneda y Timbre y sirve para realizar los pagos de los impuestos que le corresponde declarar o para solicitar la devolución de los pagos en exceso, utilizando para ello los servicios de banca electrónica. [39]

El 13 de junio de este año, la Agencia Tributaria Española, por medio del Ministerio de Hacienda, puso en práctica las subastas por red. Se subastan los bienes inmuebles embargados por deudas tributarias no pagadas. Este proceso permite que todas las acciones a cumplir para acudir a la subasta pueden hacerse de forma electrónica, desde la acreditación del pujador hasta la constitución del depósito o el pago del precio del remate. No se elimina la vía presencial, sino que

---

[39] ALVA MATTEUCCI, Juan Mario. **La Firma Digital y su Aplicación en la Administración Tributaria Peruana** en Revista Electrónica de Derecho Informático. Perú. 2000, Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107712

ambas actúan al mismo tiempo. Esto posibilita que un mayor número de personas accedan a la subasta y que el monto del remate aumente considerablemente.[40]

Otra aplicación de la firma digital es la votación en línea. La evolución de Internet y de las nuevas tecnologías inciden en los procesos de decisión de las democracias. Organizaciones, empresas y gobiernos ya están desarrollando medios para realizar, en un futuro no muy lejano, una democracia electrónica, con la que se gana rapidez y se ahorran costos. El primer sistema de votación a través de Internet y dispositivos inalámbricos se dio en Alemania en Esslingen. Para poder emitir el voto, el votante necesita simplemente una computadora estándar con una clave pública y una clave privada. El fin de este sistema de votación, por el momento, es reemplazar los actuales sistemas de votación por

---

[40] Noticias Vlex. España. **La Agencia Tributaria presenta el Nuevo procedimiento de subastas por la Red.** España, 2002, Documento sin numeración, disponible en: http://v2.vlex.com/es/asp/noticias_detalle.asp?articulo=157784

correo, pero el gobierno alemán estudia su implantación para las elecciones generales del 2006.[41]

Estados Unidos es el país mas adelantado en este tema. En las últimas elecciones presidenciales, doscientos militares de los marines emitieron su voto por medio de Internet.

---

[41] Yupi Internet Inc. **Primer Sistema de votación on-line en Alemania.** 2001, Documento sin numeración, disponible en://E:\FIRMA DIGITAL/votación online en Alemania.htm

TITULO II: LA FIRMA DIGITAL A LA LUZ DEL DERECHO

La firma digital es un instrumento de naturaleza tecnológica a la cual las diferentes legislaciones le otorgan el mismo valor que la firma manuscrita. En consecuencia, tiene efectos en el derecho que deben ser estudiados para una mejor aplicación. Estas consecuencias jurídicas serán objeto de análisis en este título. Estudiaremos primeramente la naturaleza y efectos jurídicos de la firma digital. Seguidamente, haremos un estudio comparado de las leyes promulgadas sobre la materia y, por último, analizaremos el Proyecto de Ley y Certificados Digitales de Costa Rica, número 14.276, que se tramita actualmente en la Asamblea Legislativa.

CAPITULO I: VALOR JURÍDICO DE LA FIRMA DIGITAL

En el presente capítulo se analizará el valor jurídico de la firma digital y las principales consecuencias de su equivalencia con la firma manuscrita, así como su impacto en otros conceptos como el de documento y el principio de prueba por escrito.

I. PRINCIPIO DE EQUIVALENCIA FUNCIONAL

La firma digital tiene poco de innovador en el plano estrictamente jurídico. Las regulaciones sobre firma digital, incluido el proyecto de ley costarricense sobre el tema buscan, más bien, basarse en una figura jurídica anterior: la firma manuscrita y equiparar ambas en validez y eficacia. Precisamente, esto es lo que pretende lograr el principio de equivalencia funcional. Según este principio, la firma digital es tan segura que puede ser utilizada para sustituir la firma manuscrita, con todas sus consecuencias en cuanto a validez y eficacia jurídica.

La firma se ha definido como:

> *"Nombre y apellido, o título, que se pone al pie de un escrito, para acreditar que procede de quien lo escribe, para autorizar lo allí manifestado o para obligarse a lo declarado.*
>
> *[...]*
>
> *La firma acredita la comparecencia de la persona y la conformidad con los hechos y declaraciones que suscribe, salvo haber sido obtenida por sorpresa, engaño o violencia. Por ello es exigida a las partes o a sus representantes en la totalidad de los negocios jurídicos escritos: contratos, testamentos, actas y demás documentos públicos o privados que deban tener alguna eficacia. De carecer de la firma, los escritos se consideran simples borradores o proyectos."*[42]

---

[42] CABANELLAS, Guillermo. **Diccionario de Derecho Usual.** Tomo II. Buenos Aires: Ediciones ARAYÚ, 1953.

Con ligeras modificaciones, esta es la definición que podemos encontrar en casi toda la doctrina de firma manuscrita. Tradicionalmente, se ha reconocido a la firma las siguientes funciones:

- identificar al firmante;
- hacer presumir la autoría o la atribución de un texto;
- denotar su conformidad con el texto que la antecede, y;
- hacer presumir la integridad del texto que se firma.[43]

El reconocimiento a la firma manuscrita como medio para identificar al autor de un documento y para asegurar la integridad de su contenido, se justifica cuando el procedimiento de firma del documento es de tales características que:

- cualquier alteración a la información escrita o cualquier escritura adicional sea visible y evidente;
- no sea posible agregar información, excepto a continuación de la firma manuscrita;
- el firmante utilice siempre la misma o similar firma manuscrita para firmar los documentos de su autoría;

---

[43] CAMPOLL, Gabriel Andrés. **Argentina: Firma Ológrafa y Firma No Ológrafa**. Documento sin fecha ni numeración. Disponible en: http://www.alfa-redi.org/revista/data/46-11.asp

- la firma manuscrita sea lo suficientemente compleja para que su falsificación no sea trivial;
- existan peritos calígrafos que puedan detectar las falsificaciones con razonable grado de certeza.

Estos requisitos que parecen obvios, son importantes, pues la firma digital los cumple a cabalidad. De conformidad con el principio de equivalencia funcional, la firma digital tiene el mismo valor y reconocimiento jurídico que la manuscrita. En virtud de las garantías básicas que asegura la firma digital, cumple con las funciones de la manuscrita.

La firma digital sirve para identificar al firmante, porque para que haya un dispositivo seguro de creación de firma digital, éste debe garantizar que los datos puedan producirse sólo una vez, que no puedan ser alterados ni falsificados y que puedan ser protegidos por el firmante contra su utilización por otros.

Igualmente, cumple con la función de demostrar que el firmante ha aceptado el contenido de lo firmado, ya que el mecanismo de firma no debe alterar el mensaje; asimismo, el

firmante tiene que haber tenido la posibilidad de conocer el contenido completo del documento antes de firmar y debe haber garantía de que el mensaje no va a ser cambiado después de firmado.

Todas estas garantías aseguran que el firmante pueda estar plenamente identificado, y que cada vez que aparezca su firma digital se tenga la certeza de que ha sido él y sólo él quien la ha utilizado. Además, el procedimiento para firmar digitalmente asegura que el firmante conoce el contenido total del documento antes de firmarlo. La firma digital constituye entonces una forma de manifestar conformidad con el contenido de lo firmado.

Cuando el ordenamiento jurídico exige el requisito de la firma manuscrita, este requisito se tendrá plenamente satisfecho con una firma digital. De ahí la importancia de dar una adecuada regulación a la firma digital y a su reconocimiento jurídico, en los términos que se señalará más adelante.

II. EL DOCUMENTO FIRMADO DIGITALMENTE

El documento, en sentido amplio, está definido en el Diccionario de la Real Academia Española como:

> *"[...] **3.** fig, Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo."*[44]

Esta definición contiene tres elementos importantes: en primer lugar, el asiento material (escrito); en segundo lugar, que contiene datos fidedignos; y en tercer lugar, que éstos puedan servir como prueba.

Couture señala que un documento es:

> *"un instrumento, objeto normalmente escrito, en cuyo texto se consigna o representa alguna cosa apta para esclarecer un hecho o se deja constancia de una declaración de voluntad que produce efectos jurídicos."*[45]

---

[44] Diccionario de la Lengua Española. Real Academia Española. Vigésima Primera Edición. Tomo I. Madrid, España: Editorial Espasa Clape, S.A., 2000.

[45] COUTURE, Eduardo J. **Vocabulario Jurídico**. Facultad de Derecho y Ciencias Sociales. Montevideo, 1950.

En consecuencia, podemos afirmar que un documento es cualquier representación material, que tenga como fin el reproducir o representar algo, un hecho o un acto jurídico y que esté calificado para tal fin.[46]

El documento digital, como se estudió en el Título I, es simplemente una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información. Esta representación de la información en base a dígitos implica, en el ámbito informático, una representación binaria, es decir, por medio de unos y ceros.[47]

Todo tipo de información es apta para ser representada digitalmente: mediante el escaneo, la imagen de una fotografía o la de un documento que esté en soporte de papel; mediante un procesador de palabras, la información escrita; mediante una plaqueta digitalizadora, la voz, la música y el video; mediante hojas de cálculo, la información numérica y

---

[46] PROCURADURÍA GENERAL DE LA REPÚBLICA. Dictamen C-283-98

[47] COMISIÓN REDACTORA DEL ANTEPROYECTO DE LEY DE FIRMA DIGITAL (ARGENTINA). **Informe de la Comisión Redactora.** Documento sin fecha ni numeración. Disponible en http://www.pki.gov.ar/PKIdocs/Informe.html

financiera; y mediante bases de datos, la información estadística y diversos bancos de información.

En este sentido, todo tipo de información representada digitalmente constituye un documento digital y es susceptible de ser firmada digitalmente. Es por ello que la firma digital puede utilizarse para otorgar validez jurídica o eficacia probatoria a toda declaración de voluntad o de conocimiento, con independencia de su extensión o de su medio de almacenamiento, sin limitación alguna.

III. LA FIRMA DIGITAL Y EL PRINCIPIO DE PRUEBA POR ESCRITO

La relación de los conceptos de firma digital y de documento electrónico, y su equivalencia con la firma manuscrita y el documento en sentido tradicional, tiene importantes consecuencias en la aplicación de las reglas sobre prueba.

Para que haya principio de prueba por escrito es necesario, en primer lugar, que el escrito del que se pretende hacerlo resultar, emane de la persona a quien se opone y, en segundo lugar, que tal escrito haga verosímil el hecho alegado.

En este sentido, un documento firmado digitalmente es susceptible de cumplir a cabalidad con los requisitos de este principio. La firma digital permite comprobar de quién ha emanado un documento y, además, da la seguridad de que el contenido no ha sido alterado, por lo que ese contenido puede ser utilizado para hacer verosímil el hecho alegado.

Adicionalmente, el documento firmado digitalmente puede ser útil para hacer presumir la causa de la obligación que en él se consigna, al igual que puede serlo cualquier otro documento.

Finalmente, un documento privado que ha sido firmado digitalmente hace fe entre las partes y con relación a terceros, en cuanto a las declaraciones en ellos contenidas cuando ha sido reconocido judicialmente o declarado como reconocido, de conformidad con la ley.

CAPÍTULO II: ANÁLISIS DE LA REGULACIÓN INTERNACIONAL SOBRE FIRMA DIGITAL Y SU APLICACIÓN EN LOS DIFERENTES PAÍSES

I. LEGISLACIÓN EN OTROS SISTEMAS DE DERECHO

Cada vez son más los países que han legislado con respecto a la seguridad aplicable al comercio electrónico, otorgando efecto legal a la firma digital y reconociendo a las autoridades de certificación. Varias leyes promulgadas en diferentes países le otorgan la misma validez legal a la firma digital que a la firma manuscrita. Prácticamente todas las leyes regulan la firma digital, las autoridades de certificación y los certificados digitales. A continuación, analizaremos las normas concernientes a la firma digital, al ser éste nuestro tema de tesis.

1. AMÉRICA

A. Estados Unidos de América

El primer país en promulgar una ley sobre esta materia fue Estados Unidos, cuando el Estado de Utah aprueba en 1995 la ley sobre firma digital que, conjuntamente con la Guía de Firma Digital (Digital Signature Guidelines), publicada en octubre del mismo año por "The American Bar Association's Information Security Committee" (Comité para la Seguridad de la Información de la Asociación de la Barra Americana, ABA por sus siglas en inglés), son la base de la mayoría de leyes emitidas por los diferentes Estados de Estados Unidos y diferentes países alrededor del mundo.

Existe una ley a nivel federal y varias leyes por Estado. Estudiaremos la ley federal y la ley del Estado de Utah por ser la primera ley emitida sobre la materia.

i. Ley Federal (ANEXO I)

Los Estados Unidos le ha dado gran importancia a esta materia ya que el comercio electrónico ha redefinido la economía del país. En el año 2001, las compras por Internet en ese país fueron de 490 billones de dólares. Para el año 2004, se espera que este monto aumente a 3.2 trillones de dólares.[48] Por esta razón, se ve la necesidad de crear una ley federal que le dé seguridad y confianza a las transacciones comerciales electrónicas. Es así como en octubre del 2001 se promulga la ley "*The Electronic Signatures in Global and National Commerce Act*" (Ley de Firmas Electrónicas en el Comercio Internacional y Nacional), con el fin de otorgar validez legal a las firmas electrónicas, a los contratos y cualquier otro record electrónico que influya en el comercio, ya sea nacional o internacional, dando el mismo valor legal a los contratos electrónicos que a los celebrados por escrito.

Esta ley utiliza el término de firma electrónica y lo define en la sección 106, inciso 4, como:

---

[48] STERN, Jonathan E. **The Electronic Signatures in Global and National Commerce Act.** Berkeley Technology Law Journal. California. 2001.

"un sonido electrónico, símbolo o proceso que esté adherido o lógicamente asociado con un contrato u otro récord y emitido o adoptado por una persona con la intención de firmar el record". [traducido por las autoras]

Esta definición es sumamente amplia. Le da validez legal a la firma electrónica y no contempla exclusivamente la firma digital. La firma electrónica designa cualquier método de identificación, como por ejemplo letras, caracteres, símbolos o sonidos manifestados por medios electrónicos o similares, ejecutados o adoptados por una parte en una transacción con la intención de autenticar un escrito. Es decir, que con sólo hacer "clic" con el "mouse" en un botón en la pantalla que diga "acepto" está vinculando legalmente a ambas partes del contrato.

Esta ley expresa el principio de neutralidad tecnológica. Dentro de esta definición cabe el uso de cualquier tecnología. La ley trata de ser lo suficientemente amplia para estar acorde a los cambios diarios del mundo

electrónico, dejando de lado la seguridad que debe brindar la firma digital.

Ahora bien, esta es una ley a nivel federal, que busca uniformar las leyes de los diferentes Estados. A nivel estatal, estudiaremos la ley de firma digital promulgada por el Estado de Utah, ya que fue la primera ley emitida en tal sentido.

ii. Ley del Estado de Utah sobre Firma Digital (ANEXO II)

La ley de firma digital del Estado de Utah comenzó a regir el 9 de mayo de 1995. Su propósito es promover el uso de la firma digital y brindar seguridad en las transacciones electrónicas.

Esta ley se divide en cinco partes: Interpretación y Definiciones, Licencia y Regulación de las Autoridades de Certificación, Deberes de la Autoridad de Certificación y del Firmante, Efectos de la Firma Digital y Servicios del Estado. Basaremos nuestro análisis en la primera y cuarta parte, que se refieren a la firma digital.

En la sección 46-3-103, inciso 10, de la ley en mención se define la firma digital como:

> *"Una secuencia de bits creada por una persona con la intención de firmar, en relación con un mensaje que está claramente delimitado, corriendo el mensaje a través de una función unidireccional, después encripta el mensaje resultante, usando un sistema criptográfico asimétrico y luego utilizando su llave privada."* [Traducido por las autoras]

Esta ley confina la utilización de la firma digital a la infraestructura de la llave pública, obviando el principio de neutralidad tecnológica. Esto no es una definición, sino que explica cuál es el proceso a seguir para utilizar una firma digital. Se denota una gran diferencia entre la ley a nivel federal y la ley en estudio. Esta ley se inclina por la seguridad. Con la firma digital se podrá saber sin lugar a duda quién es el autor del documento, si el mensaje fue alterado y el mensaje no podrá ser objeto de repudio por parte del emisor.

La parte cuarta sienta los requisitos que se deben cumplir para que la firma digital surta efectos jurídicos:

> *"(1) que la firma digital sea verificada con la llave pública del emisor, emitida por un certificado válido, expedido por una autoridad de certificación que tenga licencia;*
>
> *(2) que el documento se haya firmado digitalmente con la intención del emisor;*
>
> *(3) que el receptor no tenga conocimiento que el emisor haya:*
>
> *(a) incumplido algún requisito como suscriptor; o*
>
> *(b) que la llave privada haya estado bajo el estricto uso del emisor."* [traducido por las autoras]

Estos requisitos van más allá de una firma digital avanzada, pues exigen requisitos subjetivos, casi imposibles de probar. La utilización de la firma digital presupone que el firmante

haya tenido la intención de obligarse por su contenido, como sucede también con la firma manuscrita; sin embargo, esta presunción admite prueba en contrario. Un requisito como este invierte la presunción de la prueba sin justificar el porqué se atenta contra la regla general.

B. Colombia (ANEXO III)

La ley colombiana número 572 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones", sigue los lineamientos de la ley modelo en comercio electrónico de la UNCITRAL. Fue aprobada el 18 de agosto de 1999. Esta ley es muy amplia, consta de cuatro partes. La primera parte es general y tiene tres capítulos que desarrollan la definición, requisitos jurídicos y comunicación de los mensajes de datos. La segunda parte trata del comercio electrónico en materia de transporte de mercancías. La tercera parte se divide en seis capítulos, el primer capitulo está dedicado a la firma digital. Los demás capítulos son sobre las entidades de certificación, los

certificados y de los suscriptores de la firma digital. La última parte es sobre la reglamentación y vigencia. Analizaremos los capítulos referentes a la firma digital.

El ámbito de aplicación de esta ley es sumamente amplio. El artículo primero establece:

> "*La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo los siguientes casos:*
>
> *a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;*
>
> b) *En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso y consumo.*"

Esta ley le da suma importancia al "mensaje de datos", para el cual es de suma importancia la firma digital y fundamenta

el contenido de la ley bajo esta definición. Lo define en el artículo 2 inciso a) como:

> *"La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax."*

En el mismo artículo, inciso c) define la firma digital:

> *"Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación."*

En esta ley se trata de definir la firma digital sin mencionar una tecnología determinada, pero se especifican términos que suponen la tecnología de la llave pública. Por

ejemplo, se indica que la firma en cuestión "es un valor numérico que se adhiere a un mensaje de datos, y utilizando un procedimiento matemático". Asimismo, utiliza la palabra "clave del iniciador", que se refiere a la clave privada que debe utilizar el emisor al firmar un mensaje y en relación con la *función hash*, no nos queda otra solución más que utilizar la infraestructura de la clave pública. Deja de lado, entonces, el principio de neutralidad tecnológica. Esta definición excluye aspectos medulares que debe garantizar la firma digital. Menciona la integridad del mensaje, pero deja por fuera la autenticidad de la persona y no repudio de la autoría del mensaje.

Esta ley solamente dedica un artículo a la firma digital. Así, su artículo 28 establece:

> "*Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.*"

A diferencia de la ley peruana, esta definición sienta una presunción jurídica, suponiendo que cuando un documento se firma digitalmente, su autor tiene la intención de vincularse con el mismo.

El párrafo siguiente del mismo artículo señala la equivalencia de la firma digital con la firma manuscrita, siempre y cuando se cumplan con ciertos requisitos:

> "*(...) El uso de la firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:*

1. *Es única a la persona que la usa.*

2. *Es susceptible de ser verificada.*

3. *Está bajo el control exclusivo de la persona que la usa.*

4. *Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.*

5. *Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional."*

Estas especificaciones no son requisitos que permiten hacer la equivalencia entre la firma digital con la manuscrita, sino deberes que debe tener el emisor en el cuidado de su firma. No sienta las garantías que debe dar la firma: integridad, autoría y no repudio, sino que solamente da una leve idea de estos conceptos al decir que la firma digital sea única a la persona que la usa" y que esté bajo su "exclusivo control", puede suponer la autoría. De igual forma el cuarto requisito supone la integridad del mensaje, pero de forma poco clara. Además, no hace referencia a la diferencia entre una firma digital y firma digital avanzada, que supone su certificación por una autoridad de certificación. Tampoco especifica cuáles son sus efectos jurídicos. Hace un intento en su artículo 10 al tratar de darle fuerza probatoria al mensaje de datos:

"Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original."

Se deja de lado toda mención a la firma digital, no queda claro si es necesario firmar digitalmente un documento para que tenga fuerza probatoria.

Esta ley abarca diversos aspectos, es sumamente amplia y no tiene un orden lógico y coherente. No define adecuadamente qué es una firma digital, no sienta sus efectos jurídicos ni establece las garantías que ésta debe cumplir.

C. Perú (ANEXO IV)

La Ley de Firmas y Certificados Digitales fue publicada en el Diario Oficial El Peruano, el 28 de mayo del 2000. Su objeto es regular la utilización de la firma digital. Asimismo, establece las funciones de las entidades de certificación y de registro. Esta ley se divide en cinco títulos: De la Firma Digital, Del Titular de la Firma Digital, De los Certificados Digitales, De las Entidades de Certificación y de Registro y de las Disposiciones Complementarias, Transitorias y Finales. Analizaremos el primer título por ser éste el que se relaciona más directamente con nuestro tema de estudio.

El artículo primero de la ley otorga la misma validez y eficacia jurídica de la firma manuscrita al uso de la firma digital. El segundo párrafo del mismo artículo define la firma electrónica como:

> "(...) *cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse* (...)"

Esta definición tiene una seria deficiencia conceptual que puede hasta desincentivar el desarrollo de la contratación electrónica. Con base en esta definición, la firma electrónica constituye un símbolo empleado con el propósito específico de quedar vinculado jurídicamente. Es decir, que si ese propósito no existe, el símbolo basado en medios electrónicos no tendrá legalmente el valor de firma electrónica. Al efecto, el tratadista Escobar Rozas explica:

> *"Cabe preguntarse (i) si en los inicios del siglo XXI resulta razonable hacer depender la validez de la una firma (manuscrita, electrónica, etc.) de la presencia de un fenómeno puramente subjetivo como la "intención precisa de vincularse"; y (ii) si ante la evidente inexistencia de dicho fenómeno, la correspondiente sanción que el ordenamiento imponga debe afectar a la firma. La respuesta a tales interrogantes (…) es negativa. En efecto, sin soslayar la importancia del componente voluntario en los actos y negocios jurídicos, no se puede desconocer que, en aras de la seguridad y la equidad, la solución al problema de la inexistencia de tal componente pasa por mantener la validez y*

eficacia de dichos actos y negocios en caso que la otra parte (o el tercero destinatario) no haya estado en aptitud de conocer tal problema. Por otro lado, sin negar la trascendencia del conocimiento que la otra parte (o el tercero destinatario) tenga de la existencia del componente voluntario, no se puede desconocer que ante tal situación lo que debe perder valor es la declaración y no la firma, en tanto que ésta es un simple instrumento de acreditación de autor de aquélla."[49]

En efecto, la firma digital debe producir todos sus efectos jurídicos sin que interese si el que envía el mensaje tuvo la voluntad de vincularse. Esto puede desincentivar el uso de la firma digital, ya que carece de seriedad un mensaje cuya firma electrónica puede ser considerada como "no puesta" en caso que el emisor demuestre que no tenía ánimo claro de quedar vinculado jurídicamente.

El artículo 3 de la misma ley cita:

---

[49] ESCOBAR ROZAS, Freddy. La Firma Electrónica en la Ley Peruana en Revista Electrónica de Derecho Informático. No 33. Perú. Sin fecha, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107888

"La Firma Digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas a una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no pueden derivar de ella la clave privada."

Hay inconsistencia en el término utilizado para especificar la firma, ya que en el artículo primero se habla de firma electrónica y en el artículo 3 se habla de firma digital. Asimismo, no se contempla el principio de neutralidad tecnológica, ya que limita la utilización de la firma digital a la tecnología de llave pública.

D. Chile (ANEXO V)

Para la elaboración de la Ley sobre Documentos Electrónicos, Firma Electrónica y los servicios de certificación de esa firma, Chile consideró como antecedentes el texto de Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés)

"(…) regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso."

El segundo párrafo del mismo artículo, menciona los principios que fundamentan la ley:

"Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel. Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados."

El artículo 2 establece varias definiciones. Específicamente, la ley entiende por firma electrónica y firma electrónica avanzada lo siguiente:

"Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor."

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

No se menciona la tecnología de llave pública y llave privada. Se ve que el legislador opta por un sistema de neutralidad tecnológica (siguiendo los principios mencionados en el párrafo segundo del primer artículo) sin desconocer a

la firma digital, ya que esta cabe dentro de la definición de firma electrónica avanzada.[51]

El artículo 3 desarrolla el principio de equivalencia del soporte electrónico al soporte de papel:

> *"Los actos o contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán validos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos o contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan por escrito."*

Los actos o contratos firmados electrónicamente tienen la misma validez y producen iguales efectos que los celebrados

---

[51] GONZÁLEZ OGAZ, Cristóbal. **Aspectos sobre el Proyecto Chileno de Ley sobre Firma Electrónica y Servicios de Certificación de Firma Electrónica** en Revista Electrónica de Derecho Informático. No. 35, Chile. Sin fecha, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?aticulo=107969

por escrito. Se establecen las siguientes presunciones de derecho: se reputarán como escritos dichos actos y contratos cuando la ley exija que consten por escrito y la firma electrónica tendrá los mismos efectos legales que la firma manuscrita y lo establece en el último párrafo del mismo artículo:

> *"La firma electrónica, cualquiera que sea su naturaleza, se mirará como firma manuscrita par todos los efectos legales (…)."*

El mismo artículo limita este principio, indicando tres excepciones: cuando la ley requiera una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, cuando se exige la concurrencia personal de las partes y para todo lo relativo al derecho de familia.[52]

El artículo 5 hace referencia a los documentos electrónicos firmados electrónicamente como medio de prueba:

---

[52] GONZÁLEZ OGAZ, Cristóbal. Op. Cit.

"Los documentos electrónicos podrán presentarse en juicio y, en el evento de que sean usados como medio de prueba, habrán de seguirse las siguientes reglas:

1.- Los señalados en el artículo anterior[53], harán plena prueba de acuerdo con las reglas generales: y

2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el numeral anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales."

Este artículo le da a los documentos firmados de forma electrónica efectos legales. Se admiten dentro de un juicio como plena prueba, siempre y cuando hayan sido suscritos con la firma electrónica avanzada.

---

[53] El artículo 4 de la Ley sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha firma, promulgada en Chile, establece: *"Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada."*

La Ley Chilena es una ley corta, de ocho páginas, y bastante completa. Regula todos los aspectos necesarios (documento digital, la firma electrónica, utilización de la firma por órganos del Estado, las autoridades de certificación y su acreditación y los certificados digitales) para que se dé una firma digital y se le otorgue la misma validez legal que la firma manuscrita. Se apega a los principios que enumera en su artículo 2, dejando muy claro el principio de neutralidad tecnológica. No limita la utilización de la firma digital a una tecnología (como sería la de llave pública) sino que, por el contrario, deja abierta la posibilidad a la utilización de cualquier tecnología siempre y cuando cumpla con los requisitos de necesarios para la identificación de la persona, su autoría y la integridad del documento. Esto es un gran paso, ya que si se descubre una tecnología que funcione mejor para la utilización de la firma digital, esta ley no queda obsoleta.

E. Argentina (ANEXO VI)

El procedimiento de creación de la ley de Argentina, fue inspirado en los lineamientos que sigue el informe del Comité de Seguridad de la Información de la American Bar Association y la ley de Utah. Esta ley sufrió un proceso de transformación desde la presentación del proyecto hasta su promulgación el 11 de diciembre del 2001. El proyecto de ley define la firma digital con la utilización de la infraestructura de llave pública, concepto que cambia por completo en la Ley de Firma Digital número 25.506.

Esta ley consta de nueve capítulos: Consideraciones Generales, Certificados Digitales, Certificador licenciado, Titular de un certificado digital, Organización institucional, Autoridad de aplicación, Sistema de auditoría, Comisión Asesora para la infraestructura de firma digital, Responsabilidad, Sanciones y Disposiciones complementarias. Haremos un análisis de esta ley con base en los capítulos referentes a la Firma Digital.

Desde el primer artículo, se le da eficacia jurídica a la firma digital:

> "*Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.*"

El artículo 2 indica que:

> "*(…) Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.*
>
> *Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados*

por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes."

Esta definición deja abierta la posibilidad de utilizar cualquier tecnología, siguiendo el principio de neutralidad tecnológica. Especifica el deber del firmante de tener bajo su exclusivo control el procedimiento matemático, para garantizar la autenticidad del autor del mensaje. Además, indica que esta firma debe ser verificada por terceras partes, que permita su identificación y detectar cualquier alteración del documento, para proteger la integridad del mensaje. El segundo párrafo de este artículo, da un paso más allá y establece que el procedimiento y verificación de la firma digital deben estar acordes con los estándares tecnológicos internacionales, estableciendo una pauta: que la firma digital vaya de la mano con la última tecnología. Esto otorga gran seguridad y confianza al comercio electrónico.

Esta ley diferencia la firma digital de la firma electrónica. En su artículo 5 establece:

"Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados

de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez."

Esta definición, además, establece la carga de la prueba sobre la validez de la firma electrónica para aquel que pretende hacerla valer.

La ley le da la misma validez a la firma digital que la firma manuscrita, así lo establece su artículo 3:

"(...) *Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia."*

Se le da equivalencia a la firma digital y no a la firma electrónica.

A su vez, el artículo 6, dice que el documento digital satisface el requerimiento de la escritura:

> *"Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura."*

Dicha ley excluye la utilización de la firma en los siguientes campos: [54]

a) a las disposiciones por causa de muerte;

b) a los actos jurídicos de derecho de familia;

c) a los actos personalísimos en general;

d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la

---

[54] Artículo 4 de la **Ley Firma Digital**, número 25 506 de la República de Argentina.

utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes."

El artículo 7 establece que la firma digital otorga autoría al emisor del mensaje:

"(…) *Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma."*

Garantiza de esta forma la certeza de quién es el autor del mensaje.

Asimismo, el artículo 8 garantiza la integridad del mensaje:

"(…) Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma."

No deja muy claro el procedimiento necesario para comprobar que un documento ha sido inalterado, ¿qué se entiende por "verdadero"? Sin embargo, esta norma busca asegurar la certeza del mensaje, que no exista una alteración posterior de los datos.

Para que la firma digital sea válida, el artículo 9 establece los siguientes requisitos:

> *"a) haber sido creada durante el período de vigencia del certificado digital válido del firmante;*
>
> *b) ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;*
>
> c) *que dicho certificado haya sido emitido o reconocido, según el artículo 16*[55] *de la presente [ley], por un certificado licenciado."*

---

[55] "ARTICULO 16.- Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser

Si bien es cierto que la ley en estudio no menciona el término de firma digital avanzada, este artículo encuadra la validez de la firma dentro del marco de la firma digital avanzada.

Esta ley contempla una figura muy interesante. El proceso de pasar de firma manuscrita a firma digital, requiere de adaptación de los diferentes grupos sociales que por lo general están acostumbrados a trabajar en papel. Poco a poco se ha ido dirigiendo hacia el mundo digital, pero es cierto que para comprender plenamente lo que es la firma digital y sus aplicaciones, se requiere de cierta abstracción. Esta ley dedica su capítulo VIII a la Comisión Asesora para la Infraestructura de Firma Digital. El artículo 35 expone:

"*Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará*

---

reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:
a) reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o;
b) tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la Autoridad de Aplicación."

integrada multidisciplinariamente por un número máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado Nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de Profesionales.

Los integrantes serán designados por el Poder Ejecutivo Nacional (…)

(…)

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la Autoridad de Aplicación regularmente informada de los resultados de dichas consultas."

Esta comisión tiene como funciones:

"Emitir recomendaciones (…) sobre los siguientes aspectos:

a) estándares tecnológicos;

b) sistema de registro de toda la información relativa a la emisión de certificados digitales;

c) requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

d) metodología y requerimiento del resguardo físico de la información;

e) *otros que le sean requeridos por la Autoridad de Aplicación.*"

Al ser un tema nuevo, esta Comisión busca que se sigan ciertos criterios necesarios para la debida aplicación de la firma digital, que pueden ser dejados de lado por desconocimiento en el tema, contando con la ayuda de expertos en el tema que tienen la libertad de consultar a todos los

sectores profesionales. Busca seguridad en el manejo de la firma, que se mantenga bajo los estándares tecnológicos internacionales, etc. Esta es una figura interesante y necesaria para la adaptación hacia la nueva era digital.

2. EUROPA

Alemania e Italia fueron los primeros países en desarrollar normativa para la regulación de la firma digital, cuyas primeras normas sobre la materia datan de 1997. Estas iniciativas legislativas fueron seguidas por otros países europeos como España y Francia. En 1999 el Parlamento Europeo aprobó la directiva 1999/93 en la que establece un marco comunitario para la firma electrónica. Esta disposición impulsó a estos y otros países europeos a promulgar leyes y decretar reglamentos para asegurar la implementación efectiva de este importante mecanismo de seguridad. En el presente punto se analizará lo concerniente a firma digital en las normas de derecho interno de Italia, Alemania, España, Francia y el Reino Unido, y en el próximo punto se analizará lo relativo a la Directiva de la Unión Europea, así como otros textos que codifican la nueva *lex mercatoria*.

A. Italia (ANEXO VII)

En Italia está vigente la ley número 59 del 15 de marzo de 1997, "que delega facultades al Consejo de Ministros para conferir tareas y funciones a Regiones y autoridades locales, con el fin de que busquen la reforma de la administración pública y la simplificación de los procedimientos administrativos". En su artículo 15, inciso 2, esta ley establece que:

> *"Las actas, datos y documentos creados por instituciones públicas y por particulares por medios de sistemas informáticos o telemáticos, contratos celebrados por tales medios, así como su almacenamiento o transmisión por medio de sistemas de cómputo serán legalmente válidos para cualquier efecto legal. Las normas que regulen la implementación de esta subsección por parte de las instituciones públicas y particulares deberán ser establecidas en un reglamento que deberá ser emitido, de conformidad con la sección 17(2) de la*

Ley No. 400 del 23 de agosto de 1998, dentro de los 180 días siguientes a la entrada en vigencia de esta ley. El borrador del reglamento deberá ser presentado a la Cámara de Diputados y al Senado de la República para que sea considerado por las Comisiones competentes." [traducido por las autoras]

En cumplimiento del mandato establecido en este artículo se emitió en Italia el Decreto Presidencial No. 513 del 10 de noviembre de 1997, "Reglamento que establece los criterios y los medios para la implementación del artículo 15, inciso 2 de la Ley No. 59 de 15 de marzo de 1997 para la creación, almacenamiento y transmisión de documentos por medios informáticos o telemáticos".

Este reglamento contiene todas las normas que permiten una correcta aplicación de la firma digital a la luz del ordenamiento jurídico italiano. El reglamento se encuentra dividido en tres partes: Principios Generales, Firma Digital e Implementación.

En ninguna parte de este reglamento se encuentra consagrado el principio de neutralidad tecnológica. Incluso la normativa italiana decide por la tecnología de criptografía asimétrica, dejando de lado otras posibilidades. Así, el artículo primero de este reglamento define la firma digital como:

> *"[...] el resultado de un proceso informático (validación) implementando un sistema de criptografía asimétrica que consista de una llave pública y una privada, por medio de la cual el firmante confirma con la llave privada, y el receptor verifica con la llave pública el origen y la integridad de uno o varios documentos electrónicos."* [traducido por las autoras]

En la parte segunda del Reglamento, titulada Firma Digital, se da pleno reconocimiento y validez legal a la firma digital y a los documentos en los cuales ésta ha sido utilizada. En este sentido el artículo 11, inciso 1 señala que:

> *"Los contratos concertados por medio de sistemas informáticos o telemáticos y firmados digitalmente de conformidad con las normas de[l] Reglamento serán*

válidos y relevantes para todo efecto legal." [traducido por las autoras]

Este Reglamento sí equipara la firma digital a la firma manuscrita. Asimismo, equipara la firma digital autenticada por un notario público u otra autoridad oficial competente a la firma manuscrita, según lo establecen los artículos 10, inciso 2 y 16, inciso 1. El artículo 10, inciso 2 del Reglamento establece que

> *"Adjuntar una firma digital a un documento electrónico o asociarle una [firma digital] tendrá los mismos efectos que poner la firma requerida en actos o documentos escritos [...] en papel."* [traducido por las autoras]

Por su parte, el artículo 16, inciso 2 establece que:

> *"Una firma digital autenticada por un notario público u otra autoridad pública autorizada será considerada un firma autenticada para los propósitos del [...] Código Civil."* [traducido por las autoras]

Merece especial atención el hecho que se considere válida la autenticación hecha por un notario público. La fe pública depositada en un notario público para la autenticación de una firma radica, en parte, en su capacidad de efectuar la verificación material de una firma manuscrita contra un documento de identidad válido. Cabe preguntarse si los notarios públicos actualmente autorizados tendrán el conocimiento necesario para realizar la verificación de una firma digital, lo que involucra varios aspectos técnicos, algunos de ellos muy complejos.

B. Alemania (ANEXO VIII)

En el ordenamiento jurídico alemán las normas sobre firma digital a nivel federal están contenidas en la Ley para la Regulación de las Condiciones Generales para los Servicios de Información y Comunicación, publicada el 13 de junio de 1997. En su artículo 3 esta ley regula lo concerniente a la firma digital. Por su parte, el 8 de octubre de 1997 se publicó el Reglamento para la Firma Digital.

En el inciso 1(2) del artículo 3, que es la sección de la ley que se refiere a la firma digital, se consagra el principio de neutralidad tecnológica al establecer lo siguiente:

> *"Hay libertad para la utilización de otros procedimientos para la firma digital, en el tanto la firma digital de conformidad con [la] ley no esté prohibida en otras normas."* [traducido por las autoras]

En el párrafo 2 de este artículo 3, que contiene las definiciones relevantes para este tema, de firma digital se define la firma digital como:

> *"Un sello impreso con una llave privada a datos digitales que, con la ayuda de la correspondiente llave pública denotada por un certificado de firma, permita identificar al poseedor de la llave firmante y confirmar la veracidad de los datos."* [traducido por las autoras]

Una primera lectura de ambos artículos haría pensar que estamos frente a una contradicción en esta ley alemana. Sin

embargo, se establece por un lado una definición muy específica de firma digital basada en la infraestructura de llave pública y, a la vez, se deja la puerta abierta para la utilización de otras tecnologías.

C. España (ANEXO IX)

El Real Decreto-Ley 14/1999 de 17 de septiembre sobre firma electrónica está basado, en gran parte, con tan sólo unas pequeñas modificaciones, en lo que en su momento era el proyecto de Directiva Europea en este tema, cuya versión final fue aprobada algunos meses después. Este esfuerzo merece reconocimiento, ya que para propiciar un debido desarrollo del comercio electrónico no es suficiente con dictar normas que regulen la firma digital, sino que se debe además procurar una armonía internacional de las disposiciones en la materia que brinde mayor certeza y seguridad a los usuarios de estas herramientas, como la firma digital, que se encuentran en diferentes países del mundo y que, para concretar sus transacciones, deben lidiar con diferentes ordenamientos jurídicos.

Un ejemplo de la conciencia de que estas disposiciones tendrán aplicación más allá de las fronteras españolas lo encontramos en el artículo 20 del Real Decreto-Ley que, en su inciso primero, establece que:

> *"Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el Diario Oficial de las Comunidades Europeas son conformes con los previsto en la letra a) del artículo 12 y en el artículo 19."*[56]

---

[56] **Artículo 12** Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.

Además de cumplir las obligaciones en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

a. Indicar la fecha y hora en las que se expidió o dejó de expedir un certificado.

[...]

Artículo 19. Dispositivos seguros de creación de firma electrónica.

A efectos del artículo 2.f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:

1. Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2. Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

Es importante destacar que el Decreto-Ley español utiliza el término más amplio de firma electrónica, definido en el artículo 2, inciso a. como:

> *"[...] el conjunto de datos, de forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge."*

Esta normativa recoge además el concepto de firma electrónica avanzada, definida en el inciso b. del mismo artículo de la siguiente manera:

> *"[e]s la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control,*

---

3. Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4. Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior."

En esta definición de firma electrónica avanzada encontramos consagrados las garantías de identidad del emisor y de integridad del mensaje.

Si bien es cierto se han formulado críticas en la doctrina a establecer dos conceptos de firma digital, uno simple y otro avanzado[57], es rescatable de esta iniciativa legislativa que se respeta el principio de neutralidad tecnológica, ya que solamente se establece lo que la firma digital debe garantizar, sin imponer una tecnología específica para la utilización de ésta.

---

[57] PÉREZ MERAYO, Guillermo Augusto. **Comentario acerca de las deficiencias que presenta el Proyecto de Ley sobre la Firma Digital.** En Revista Jurídica Electrónica, Instituto de Investigaciones Jurídicas de la Facultad de Derecho de la Universidad de Costa Rica, No. 1, junio 2001. Documento sin numeración, disponible en http//:www.iij.derecho.ucr.ac.cr/revista/rev1/firmadigital/index3.htm

Por su parte, el artículo 3 del Real Decreto-Ley establece los efectos jurídicos que el ordenamiento español otorga a la "firma electrónica avanzada" al reconocerle

> *"el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales."*

Lo anterior, siempre y cuando esta firma electrónica avanzada esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma. Especial mención merece el inciso 2 de ese mismo artículo 3, que establece que a una firma electrónica que cumpla con estos requisitos no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

En el Título III del Real Decreto-Ley se establecen los dispositivos de firma electrónica. En total respeto del principio de neutralidad tecnológica no se imponen las tecnologías necesarias para que se dé una firma electrónica,

sino que solamente se establecen los requisitos que esta firma debe garantizar para ser tal. En este sentido, para considerarse como se entienda que el dispositivo de creación de una firma electrónica es seguro, el artículo 19 exige:

> *"1. Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.*
>
> *2. Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.*
>
> *3. Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.*
>
> *4. Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida*

que éste se muestre al signatario antes del proceso de firma."

En ningún lugar del Real Decreto-Ley español se habla de tecnologías específicas como, por ejemplo, infraestructura de llave pública, dejando la definición de cuál tecnología se aplica a los avances que se den en este campo, a las necesidades del mercado y, en todo caso, a otras formas de regulación más flexibles como, por ejemplo, un reglamento.

D. Francia (ANEXO X)

La firma digital se encuentra regulada en Francia mediante la Ley No. 2000-230 del 13 de marzo de 2000 para la adaptación del derecho de la prueba a las tecnologías de la información y relativa a la firma electrónica. Esta ley se encuentra reglamentada por el Decreto No. 2001-272 del 30 de marzo de 2001 adoptado para la aplicación del artículo 1316-4 del Código Civil y relativo a la firma electrónica.

De conformidad con la Ley no. 2000-230, que reforma varios artículos del Código Civil francés, el artículo 1316-4 de dicho Código establece que:

> *"La firma necesaria para la perfección de un acto jurídico identifica a quien la crea. Ella manifiesta el consentimiento de las partes a las obligaciones que deriven de tal acto. Cuando es puesta, además, por una autoridad pública, ella confiere además autenticidad al acto.*
>
> *Cuando es electrónica, consiste en el uso de un procedimiento confiable de identificación que garantiza su ligamen con el acto al que se adjunta. La confiabilidad de dicho procedimiento se presume, hasta prueba en contrario, con el que se crea la firma electrónica, la identidad del firmante es asegurada y la integridad del acto es garantizada, en las condiciones fijadas por el decreto del Consejo de Estado."* [traducido por las autoras]

La ley 2001-272 establece una interesante presunción legal *iuris tantum* a favor de la firma electrónica en su artículo 2 en el sentido que:

"[l]a confiabilidad de un procedimiento de firma electrónica se presume hasta tanto no haya prueba en contrario" [traducido por las autoras]

Por su parte el artículo de 3 de esta ley establece que para que un dispositivo de creación de una firma electrónica sea seguro, éste debe:

"1. Garantizar por medios técnicos y procedimientos apropiados que los resultados de creación de la firma electrónica:

a) No puedan ser obtenidos más de una vez y que su confidencialidad esté asegurada;

b) No puedan ser deducidos y que la firma electrónica esté protegida contra toda falsificación;

c) Puedan ser protegidos de manera suficiente por el firmante contra su utilización por parte de terceros.

2. No comportar ninguna alteración del contenido del acto a firmar y no ser un obstáculo para que el firmante tenga un conocimiento exacto del contenido antes de firmar." [traducido por las autoras]

Estas disposiciones de la normativa francesa se apegan en gran medida a lo estipulado por la Unión Europea en su Directiva 1999/93 y respetan el principio de neutralidad tecnológica. Utilizan el concepto más amplio de firma electrónica y no amarran su definición a ninguna tecnología en específico, sino que establece las garantías que se buscan en una firma electrónica.

3. ASIA

Luego de analizar a fondo de las legislaciones en América y Europa, así como de los principales instrumentos internacionales sobre este tema, estudiaremos algunas disposiciones de los ordenamientos jurídicos asiáticos como un punto de referencia adicional; principalmente con el propósito de demostrar que el esfuerzo por regular adecuadamente la firma digital es mundial.

A. Corea del Sur

Corea busca la promoción del comercio electrónico. Existen varios proyectos de ley con el fin de obtener ese objetivo, dentro de las cuales existe el proyecto de ley para la implementación de la firma digital. El primero de julio de 1999 entró en vigencia la ley sobre comercio electrónico. Esta ley le otorga efectos jurídicos a las transacciones electrónicas y dar un entorno seguro. Con esta razón, se creó el Programa para la Promoción del Comercio Electrónico y el Instituto de Corea para el Comercio Electrónico.

B. India

En este país existe la Ley sobre Tecnología de la Información, promulgada en diciembre de 1998, que regula aspectos del comercio y la firma digital. En junio del 2000 se promulgó otra ley con el mismo nombre, que regula la utilización de las firmas digitales y los registros electrónicos. Esta ley otorga validez legal a las transacciones realizadas por medios electrónicos.

C. Japón

El primero de abril del 2001 se aprobó la ley sobre Firma Electrónica y Servicios de Certificación. Otorga validez legal a todo registro electromagnético si está firmado electrónicamente.

D. Malasia

En 1997, se promulgó la ley 562, que regula la firma digital y se reguló la licencia y actividad de las autoridades de certificación.

E. Singapur

En junio de 1998 se emitió la ley de firmas electrónicas y digitales, registros electrónicos y comercio electrónico. Regula las firmas electrónicas, las firmas digitales y los registros electrónicos. Sus objetivos son facilitar el comercio electrónico, eliminar el fraude y promover el uso de

la firma digital para darle autoría a los mensajes enviados por medios electrónicos.

4. NUEVA *LEX MERCATORIA*

A. Comisión de Las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés) (ANEXO XI)

La Ley Modelo sobre Firmas Electrónicas, cuyo texto final fue adoptado por la Asamblea General de la Organización de las Naciones Unidas (ONU) durante su octogésima quinta sesión, el 12 de diciembre de 2001, constituye un paso más en una serie de instrumentos internacionales que han sido adoptados por la UNCITRAL para establecer modelos de carácter universal sobre la materia de comercio electrónico. La ley considera las modernas necesidades de comunicación, a la vez que promueve la reducción del formalismo de los sistemas jurídicos nacionales, buscando la uniformidad de las distintas legislaciones.

A manera de ejemplo, la finalidad con la que se preparó la Ley Modelo sobre Comercio Electrónico fue ofrecer a los legisladores nacionales un juego de normas internacionalmente aceptables sobre cómo pueden ser removidos una serie de obstáculos legales, y cómo se puede crear un ambiente jurídico más seguro para el comercio electrónico.

La Ley Modelo sobre Firmas Electrónicas desarrolla puntos específicos de la normativa sobre el comercio electrónico, concretamente el artículo 7 de la Ley Modelo de la UNCITRAL sobre Comercio Electrónico[58]. En este sentido, constituye una forma de proporcionar información detallada sobre el concepto del "método fiable para identificar" a una persona y "para indicar que esa persona aprueba la información que figura en el mensaje de datos". Junto con la Ley Modelo Sobre Firmas

---

[58] *Artículo 7. Firma*

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma

[...]

Electrónicas, la Asamblea General de la ONU adoptó el texto de la Guía para la Incorporación al Derecho Interno de esta ley.

El artículo 12 de la Ley Modelo reconoce que uno de los principales fines es armonización de la regulación sobre firma digital que, en consecuencia, otorga mayor seguridad jurídica para los usuarios de esta herramienta, y establece que:

> *"1) Al determinar si un certificado o una firma electrónica produce efectos jurídicos, o en qué medidas los produce,* ***no*** *se tomará en consideración:*
>
> *a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni*
>
> *b) el lugar en que se encuentre el establecimiento del expedidor o firmante*
>
> *2) Todo certificado expedido fuera [del Estado promulgante] producirá los mismos efectos jurídicos*

en [el Estado promulgante] que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

3) Toda firma electrónica creada o utilizada fuera [del Estado promulgante] producirá los mismos efectos en [el Estado promulgante] que toda firma electrónica creada o utilizada en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

4) A efectos de determinar si un certificado o una firma electrónica presenta un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2) o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5) Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas

electrónicas y certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable." [el destacado no es del original]

Cabe destacar que el reconocimiento del certificado y de la firma electrónica no se basa en formalismos como, por ejemplo, el lugar dónde se expidieron, sino que opta por criterios más sustanciales, como el grado de fiabilidad que brindan. Sin embargo, el concepto de "fiabilidad sustancialmente equivalente" queda establecido en una forma vaga y finalmente remite a "las normas internacionales reconocidas", sin mayores especificaciones. Aquí hubiera sido oportuno reiterar (porque sí está establecido en otras secciones de la Ley Modelo) que para lograr ese grado de fiabilidad es necesario que la firma electrónica garantice: la autoría del mensaje, el no repudio de éste y su integridad.

La Ley Modelo reviste la forma de un texto legislativo que se recomienda a los Estados para que lo incorporen a su derecho

interno. Al hacerlo, los Estados pueden modificar, incluir o excluir algunas de sus disposiciones. Sin embargo, para lograr un grado satisfactorio de armonización y certeza, la misma UNCITRAL recomienda a los Estados que hagan el menor número posible de modificaciones al proyecto[59]. En efecto, en la Guía para la Incorporación al Derecho Interno de la Ley Modelo, la UNCITRAL sugiere, además, que de hacerse estas modificaciones

> *"se tengan debidamente en cuenta sus principios básicos, como los de neutralidad tecnológica, no discriminación entre las firmas electrónicas nacionales y extranjeras, la autonomía de las partes y el origen internacional de la Ley Modelo".*

En su artículo 2, la Ley Modelo define la firma electrónica (esta ley utiliza este concepto y no el de firma digital) de la siguiente manera:

> *"los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados*

---

[59] Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas.

para identificar al firmante en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos".

Se evidencia con esta definición, y con la lectura a lo largo de la Ley Modelo, que el Grupo de Trabajo de la UNCITRAL sobre Comercio Electrónico observó el principio de neutralidad respecto de la tecnología, pero consciente de que las "firmas numéricas", es decir, las firmas electrónicas obtenidas mediante la aplicación de una criptografía de doble clave, eran una tecnología considerablemente difundida[60]. Esta idea está reforzada por lo que establece el artículo 3, en el sentido que:

"[n]inguna de las disposiciones de la [...] Ley [...] será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla con los requisitos enunciados en el párrafo 1) del artículo 6 o que

[60] A/CN.9/484, párrafo, 54

cumpla de otro modo los requisitos del derecho aplicable".[61]

Ante la evolución de las innovaciones tecnológicas, la Ley Modelo establece criterios para el reconocimiento jurídico de las firmas electrónicas, independientemente de la tecnología utilizada (a saber, firmas electrónicas basadas en la criptografía asimétrica; los dispositivos biométricos, que permiten la identificación de personas por sus características físicas; la criptografía simétrica; la utilización de números de identificación personal; etc.). Entre esos criterios, encontramos en la definición del artículo 2 importantes garantías, como la identificación del emisor del mensaje y el no repudio del contenido del mensaje.

Esta noción de "firma electrónica", además, aspira a abarcar todos los usos tradicionales de una firma manuscrita con consecuencias jurídicas, siendo la identificación del

---

[61] *Artículo 6. Cumplimiento del requisito de firma*

1) Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan fiable que resulte propia a los fines para los cuales se generó o comunicó ese mensaje.

[...]

firmante y la intención de firmar sólo el mínimo común denominador de los diversos criterios relativos a la "firma" que se hallan en los diversos ordenamientos jurídicos.

En su artículo 8 la Ley Modelo establece la conducta recomendada para el firmante. Esta disposición, además, establece que el firmante incurrirá en responsabilidad por el incumplimiento de estos requisitos. De conformidad con este artículo, cuando puedan utilizarse datos de creación de firmas para la creación de la misma con efectos jurídicos, cada firmante deberá:

> *"a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;*
>
> *b) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:*
>
> *i) sabe que los datos de creación de la firma han quedado en entredicho; o*

ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su ciclo vital o que hayan de consignarse en él sean exactas y cabales".

Esta norma, en conjunto con las contenidas en los artículos 9 (Proceder del prestador de servicios de certificación), 10 (Fiabilidad) y 11 (Proceder de la parte que confía en el certificado) son medulares para alcanzar la seguridad jurídica deseada al regular la aplicación de estos procedimientos. Establecen reglas claras para la determinación de la responsabilidad de las partes involucradas.

B. Unión Europea (ANEXO XII)

Existen, dentro del marco de los lineamientos emitidos por los órganos de la Unión Europea, dos instrumentos fundamentales en materia de firma digital: en primer lugar la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 con la que se establece un marco comunitario para la firma electrónica y, en segundo lugar, la Iniciativa Europea de Normalización de firma electrónica (EESI).

El Parlamento Europeo y el Consejo de la Unión Europea, al adoptar la Directiva mencionada consideraron, entre otros, lo siguiente:

> *"La comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio*

electrónico. Por un lado, un marco claro comunitario sobre las condiciones aplicables a la firma electrónica aumentará la confianza en las nuevas tecnologías y la aceptación general de las mismas. La legislación de los Estados miembros en este ámbito no debería obstaculizar la libre circulación de bienes y servicios en el mercado interior."

Esta directiva define, en su artículo primero, su ámbito de aplicación, y deja muy claro que su propósito es darle reconocimiento jurídico a la firma electrónica como tal, sin entrar en discusiones sobre otros aspectos como la celebración de contratos o la exigencia de formalidades para determinados actos jurídicos. El artículo primero establece, en lo que interesa, lo siguiente:

"La [...] Directiva tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. [...]

La [...] Directiva no regula otros aspectos relacionados con la elaboración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afecta a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos."

Es claro de la lectura de este artículo, y como se verá más adelante, que la Directiva no pretende dictar lineamientos sobre el perfeccionamiento y eficacia de los contratos, ni tampoco sobre otras formalidades de naturaleza no contractual relativas a la firma. En este sentido, las firmas electrónicas avanzadas relacionadas con un certificado reconocido y creadas mediante un dispositivo seguro de creación de firma, se pueden considerar jurídicamente equivalentes a las firmas manuscritas si se cumplen los requisitos aplicables a las firmas manuscritas (que, en términos generales, ya se encuentran establecidos en las legislaciones nacionales con mucha antelación a la promulgación de ésta y otras normas sobre firma electrónica).

El artículo 2 de la Directiva, que contiene las definiciones relevantes a efectos de esta normativa, maneja los dos conceptos de firma electrónica y firma electrónica avanzada, y los define de la siguiente manera:

> *"«firma electrónica»: los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación;*
>
> *«firma electrónica avanzada»: la firma electrónica que cumple los requisitos siguientes:*
>
> *a) estar vinculada al firmante de manera única;*
>
> *b) permitir la identificación del firmante;*
>
> *c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;*

d) estar vinculada a los datos a los que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable".

De esta definición se infiere que la Unión Europea respeta plenamente el principio de neutralidad tecnológica, al no vincular su definición de firma electrónica a ninguna tecnología en específico. Además, establece cuáles son las garantías con las que cualquier tecnología tendría que cumplir para gozar de reconocimiento jurídico. La Directiva elabora más profundamente sobre este punto en su Anexo III, donde establece los siguientes requisitos de los dispositivos seguros de creación de firma electrónica:

"1. Los dispositivos seguros de creación de firma garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

a) los datos utilizados para la generación de firma sólo pueden producirse una vez en la práctica y se garantiza razonablemente su secreto;

b) existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad;

c) los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.

2. Los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma."

Estos requisitos, además de garantizar la identificación del firmante y de asegurar la integridad del mensaje, garantías básicas de la firma digital, pretenden asegurar que el firmante conoce y acepta el contenido del mensaje firmado, especialmente por la frase *"[l]os dispositivos seguros de*

creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma". Esto permite equiparar plenamente la firma digital a la firma manuscrita, cuyo función principal es justamente recoger la manifestación de aceptación del contenido de un documento por parte del firmante.

Una vez definida la firma electrónica, la Directiva de la Unión Europea reconoce efectos jurídicos a esta firma en su artículo 5 de la siguiente manera:

> *"1. Los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma:*
>
> *a) satisfaga el requisito jurídico de la firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y*

b) sea admisible como prueba en procedimientos judiciales

2. Los Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho que:

- *ésta se presente en forma electrónica, o*

- *no se base en un certificado reconocido, o*

- *no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o*

- *no esté creada por un dispositivo seguro de creación de firma."*

La forma en que la Directiva le reconoce efectos jurídicos a la firma electrónica nos hace entender el porqué se manejan los dos conceptos de firma electrónica y firma electrónica

avanzada; al reconocer la firma electrónica simple hay seguridad de que no se le negará validez en una forma total por el simple hecho de ser un medio electrónico y no encontrarse estampado en papel. Esto guarda relación con la intención del Parlamento y el Consejo que, al exponer sus consideraciones previas a la Directiva, señalaron:

> *"Los Estados miembros no deben prohibir a los proveedores de servicios de certificación operar al margen de los sistemas de acreditación voluntaria*
> *(...)*
>
> *(...)*
>
> *La (...) Directiva contribuye al uso y al reconocimiento legal de la firma electrónica en la Comunidad; no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrados entre un número determinado de participantes. En la medida en que lo permita la legislación nacional,*

ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales."

5. ANÁLISIS JURISPRUDENCIAL

La firma digital y su regulación es un tema sumamente nuevo. Como se estudió anteriormente, la primera ley sobre firma digital fue la del Estado de Utah en Estados Unidos y surgió como una ley pionera en su campo, promulgada en 1995. Esta iniciativa inspiró la promulgación de otras leyes e instrumentos internacionales tendientes a regular la firma digital. La mayoría de las leyes fueron promulgadas hace poco menos de un año y, en muchos otros casos incluido el de Costa Rica, las leyes sobre firma digital se encuentran aún en trámite de aprobación.

En países como Costa Rica, donde sólo el 3.4% de los hogares tienen acceso a Internet[62], es evidente que el paso al uso de la firma digital, que pretende suplantar la firma manuscrita, no puede ser automático, sino que debe ir acompañado de un cambio en la mentalidad de la población. En todo caso, de una investigación exhaustiva de los archivos judiciales, se puede concluir que los conflictos surgidos de la utilización de medios electrónicos, en caso que se hayan presentado, no han llegado todavía a los tribunales de justicia. De ahí que no hay antecedentes jurisprudenciales sobre este tema.

Un fenómeno similar se da en otros países del mundo, en donde tampoco se han encontrado decisiones judiciales referentes a la aplicación de la firma digital.

En Argentina, el Juzgado Comercial, bajo el expediente No. 39.749, se refirió al tema de la firma digital el 23 de octubre del 2001. En el caso, el accionante solicitaba a la Corte:

---

[62] DE TÉRAMOND PERALTA, Guy y PARDO EVANS, Rogelio. La **Nueva Sociedad del Conocimiento.** San José, Costa Rica: Ministerio de Ciencia y Tecnología (2000-2006), 2002.

> *"la constatación judicial acerca de la existencia en los equipos de computación sito en las oficinas de la calle [...] de mensajes electrónicos enviados a la bandeja de entradas de Outlook y/o sistema similar donde se archiven los mails".*

Al referirse a esta solicitud, el juez argentino consideró, entre otras cosas, que:

> *"[Argentina] carece todavía tanto de una ley de regulación del comercio electrónico, como de otra relativa a la certificación de la firma digital, necesaria para validar la autenticidad, integridad y el no repudio del llamado documento electrónico".*

Finalmente, la solicitud de diligencia preliminar objeto de esta decisión fue rechazada, en gran medida porque en ese momento no existía la regulación adecuada que permitiera dar valor probatorio a los mensajes electrónicos.

II. PRINCIPALES FIGURAS CONTEMPLADAS EN LA LEGISLACION COMPARADA

A continuación, se destacarán las principales figuras reguladas en las legislaciones estudiadas.

1. PRINCIPIO DE NEUTRALIDAD TECNOLÓGICA / TECNOLOGÍA ESPECÍFICA

Existen dos posiciones bien definidas en cuanto al concepto de firma digital en los diferentes ordenamientos jurídicos estudiados. Por un lado, se define dicha firma sin hacer mención a alguna tecnología en específico, apegándose al principio de neutralidad tecnológica. La Ley Modelo de la UNCITRAL, efectuada con el fin de brindar ayuda a la redacción de la ley de firma digital en los diferentes países, aboga por que se respete el principio en mención. De igual forma, los lineamientos emitidos por la Unión Europea sugieren que la firma digital no se amarre a una tecnología. Asimismo, las leyes sobre Firma Digital de Estados Unidos (a nivel federal), la de Chile, Alemania y Francia, dejan abierta la posibilidad de utilizar cualquier tecnología. Esto

es una gran ventaja ya que si la tecnología cambia, la ley no queda obsoleta y no hay necesidad de emitir una nueva. Sin embargo, en aras de la seguridad, es necesario que se especifiquen cuáles son las garantías que debe asegurar dicha firma.

Por otro lado, hay leyes que conceptúan la firma digital con base en una tecnología específica. Tal es el caso de la Ley del Estado de Utah que amarra la utilización de la firma a la infraestructura de la criptografía asimétrica, haciendo referencia a la clave pública y privada. Igualmente, Perú, Colombia e Italia limitan el uso de la firma digital a la tecnología de la llave pública.

Como se estudiará adelante, Costa Rica opta por definir la firma digital con base en el principio de neutralidad tecnológica.

2. PRINCIPIO DE EQUIVALENCIA FUNCIONAL

El objetivo de todas las leyes es otorgar el mismo valor jurídico a la firma digital que a la firma manuscrita. Con

esto se le da equivalencia al soporte electrónico con el soporte de papel. De esta manera los actos o contratos firmados electrónicamente tienen la misma validez y producen los mismos efectos que los realizados por escrito con soporte de papel. Se establece una presunción legal: cuando la ley requiera una firma manuscrita, esta quedará satisfecha por una digital. Todas las normas estudiadas desarrollan la teoría de los efectos jurídicos de la firma digital con base a este principio.

3. COMPATIBILIDAD INTERNACIONAL

Entre los fines de la Ley Modelo de la UNCITRAL, está lograr uniformidad entre todas las leyes promulgadas por los diferentes países. Al ser Internet un instrumento de uso global, es necesario que las normas dictadas en diversos ordenamientos sean compatibles, con el fin de evitar problemas en su aplicación. El uso de la firma digital sobrepasa los límites nacionales. Por esta razón, prácticamente todas las leyes reconocen los certificados expedidos transfronterizamente, siempre y cuando se cumplan

con ciertos requisitos, similares para los dispositivos de creación y verificación de la firma.

4. LIBRE COMPETENCIA

Todas las leyes consagran el principio de libre competencia entre las autoridades de certificación. Cualquier persona, sea física o jurídica, pública o privada, puede otorgar este servicio, siempre y cuando cumpla con ciertos requisitos establecidos en la ley. Es necesario que se enumeren los requisitos, ya que las autoridades de certificación deben otorgar una mínima seguridad.

5. ACREDITACIÓN VOLUNTARIA

Las leyes sobre firma digital están dentro del ámbito del derecho privado, por lo cual debe regirse por el principio de autonomía de la voluntad, donde las partes pueden hacer todo lo que no se les prohíba expresamente. Las partes pueden contratar los servicios de certificación con quien deseen, sea una entidad acreditada o no. Ninguna ley obliga a dichas entidades a someterse al procedimiento de acreditación. Sin

embargo, se crea la figura de acreditación, para quien lo desee con el fin de brindar mayor seguridad.

6. USO DE LA FIRMA DIGITAL POR EL ESTADO

Son pocas las leyes que le otorgan expresamente al Estado la facultad de usar la firma digital. Las leyes que sí le otorgan este uso, están simplemente cumpliendo con el principio de legalidad, autorizando al Estado a utilizarla.

7. GARANTÍAS

Todas las leyes buscan garantizar con la firma digital la autenticidad del emisor, la integridad del mensaje y el no repudio en origen y destino del mensaje. Muchas legislaciones lo indican expresamente en sus normas y en otras se da a entender por medio de la interrelación e interpretación de sus diferentes artículos.

CAPÍTULO III: LA FIRMA DIGITAL EN COSTA RICA: ANÁLISIS DEL PROYECTO DE LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES No. 14.276

I. ANTECEDENTES DEL PROYECTO DE LEY

Costa Rica no se ha quedado atrás en el esfuerzo mundial por dar una adecuada regulación a la firma digital. El 20 de febrero del 2001, el Poder Ejecutivo presentó a la Asamblea Legislativa el Proyecto de Ley titulado "Ley de Firma Digital y Certificados Digitales". Este proyecto se tramita en la Asamblea Legislativa bajo el expediente número 14.276, mediante el procedimiento de proyecto de ley ordinario. En el acta de sesión Plenaria No. 42 celebrada el 8 de marzo del 2001, se aprobó una moción para que se le dispensen los trámites de publicación y espera[63]. El proyecto fue conocido inicialmente por la Comisión Especial No. 13.655, "Comisión Especial que estudie, analice y dictamine la legislación que sobre Propiedad Intelectual requiere nuestro país para

[63] Proyecto de Ley de Firma Digital y Certificados Digitales. Expediente número 14.276

enfrentar los desafíos y compromisos internacionales asumidos a la fecha". Esta Comisión cumplió su mandato y se encuentra actualmente archivada; en consecuencia el proyecto pasó a conocimiento de la Comisión de Asuntos Jurídicos.

El Archivo Nacional y el Instituto Costarricense de Derecho Notarial (ICODEN) remitieron sus observaciones al proyecto, en las cuales realizaron consideraciones de fondo sobre él proporcionaron algunas sugerencias, a la vez que solicitaron audiencia ante la Comisión que lo estudia.

El Informe Técnico de febrero del 2002, del Departamento de Servicios Técnicos de la Asamblea Legislativa, en relación con el proyecto de ley, señala como consultas obligatorias, de conformidad con el artículo 190 de la Constitución Política, las que deben realizarse a las siguientes instituciones: Instituciones autónomas, Corte Suprema de Justicia, Consejo Nacional para Investigaciones Científicas y Tecnológicas (CONICIT) y Universidades Públicas (UCR, UNA, ITCR y UNED). Además, recomendó consultar el proyecto a otras instituciones públicas y privadas, por razones de conveniencia y oportunidad, en virtud de la materia que trata

el proyecto de ley[64]. Las consultas recomendadas habían sido realizadas a más de 74 instituciones públicas, ministerios y universidades, el 26 de noviembre de 2001.

En términos generales, todas las instituciones que contestaron a la consulta realizada manifestaron su conformidad con el proyecto, alabando su oportunidad y conveniencia. Muchas se limitaron a manifestar que no "encontraban ningún problema en el proyecto".[65]

Entre las instituciones que sí presentaron observaciones, la principal recomendación señalada fue darle "más profundidad al proyecto" y "más claridad a los términos", aunque casi ninguna señaló propuestas concretas en este sentido.

---

[64] Asamblea Legislativa. Informe de servicios técnicos, pág. 38. Expediente número 14.276.

[65] Se recibió respuesta solamente por parte de: el Instituto Costarricense de Turismo, la Caja Costarricense de Seguro Social, el Banco de Costa Rica, el Banco Popular de Desarrollo Comunal, el Patronato Nacional de la Infancia, el INFOCOOP, la Compañía Nacional de Fuerza y Luz, la Junta de Protección Social de San José, Radiográfica Costarricense, el Ministerio de Comercio Exterior, el Instituto Costarricense de Puertos del Pacífico, la Refinadora Costarricense de Petróleo, la Contraloría General de la República, la Superintendencia de Entidades Financieras, el Archivo Nacional, el Tribunal Supremo de Elecciones, Correos de Costa Rica, S.A., el Ministerio de Hacienda, el Ministerio de Economía Industria y Comercio, el Banco Nacional de Costa Rica, INCOPESCA, el Banco Crédito Agrícola de Cartago, el Registro Nacional, el Ministerio de Gobernación y Policía, el Ministerio de Relaciones Exteriores, el Ministerio de Trabajo y Seguridad Social y el Ministerio de Salud.

De las consideraciones remitidas, se observa también que hay confusión en algunas instituciones en cuanto al certificado digital, pues lo entienden como el documento firmado digitalmente. En consecuencia, las sugerencias que indican no son procedentes, ya que no se ajustan a la realidad del funcionamiento de la firma digital y los certificados digitales. En general, se expresan dudas sobre este funcionamiento. Sin embargo, no corresponde a la ley explicarlo, sino limitarse a regularlo y reconocerle consecuencias jurídicas. Si bien es cierto, como se verá más adelante, hay artículos del proyecto de ley que pueden ser redactados en forma más clara, cualquier análisis y aplicación de esta ley, en caso de ser aprobada, debe partir de un conocimiento técnico mínimo sobre la tecnología de firma digital. Estos conceptos no pueden estar definidos en la ley, pues entre más especificaciones se incluyan sobre el funcionamiento de la firma digital, más se compromete el principio de neutralidad tecnológica, de central importancia en esta materia, como ya se ha expuesto.

Algunas observaciones acertadas, que incluso fueron recogidas en versiones posteriores del proyecto, comprenden la omisión

de establecer responsabilidades y sanciones en caso de no cumplimiento con las normas dictadas, así como mayor definición sobre la Autoridad Acreditadora y sus funciones, y la problemática que plantea mencionar a los abogados y notarios en el artículo 6 de la primera versión del proyecto[66]. Ambos aspectos serán analizados más adelante.

El 21 de febrero de 2002 el Departamento de Servicios Técnicos de la Asamblea Legislativa remitió su informe técnico. En este informe realizó varias consideraciones de fondo sobre el proyecto y se refirió, además, a aspectos de técnica legislativa.

Una vez recibidas las observaciones, un nuevo proyecto de ley fue preparado y adoptado para su discusión, el 13 de marzo de 2002. Esto fue logrado mediante una moción para que el texto base de la discusión sea esta última versión. Este texto será el analizado en los acápites siguientes.

---

[66] **Artículo 6.-** Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado, o de cualquier otra forma reconocido, verificado o certificado, tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma digital o Firma Digital Avanzada.

Esta última versión del proyecto está divido en seis capítulos: Disposiciones Generales, Del Órgano Rector y la Autoridad Acreditadora, De los Certificados Digitales, Deberes de las Partes Intervinientes, Sanciones y Disposiciones Finales. A continuación, se hará un estudio del proyecto a la luz del ordenamiento jurídico costarricense.

II. EL PROYECTO DE LEY EN EL ORDENAMIENTO JURIDICO COSTARRICENSE

A continuación, estudiaremos cómo se acoplaría este proyecto de ley, en caso de aprobarse su texto final (tal y como fue adoptado para su discusión el 13 de marzo del 2002), en el ordenamiento jurídico costarricense.

Todo análisis de una norma, en relación con el ordenamiento jurídico del cual entraría a formar parte, debe iniciar con la norma de mayor jerarquía, sea la Constitución Política. Esto, en virtud de que en caso de contener alguna disposición que vaya en contra de una norma o principio constitucional,

implicaría la inconstitucionalidad de esa disposición y sería cuestión de tiempo, antes de que sea declarada como tal por la Sala Constitucional, con lo que desaparecería del ordenamiento jurídico. Por otro lado, aún las normas que en sí mismas no presenten problemas de constitucionalidad, deben ser leídas en armonía con las disposiciones constitucionales, a las cuales se deben ajustar todas las normas de menor jerarquía.

Siguiendo con el análisis, la principal innovación de este proyecto de ley es el reconocimiento del principio de equivalencia funcional, según el cual un documento (digital) firmado digitalmente tiene el mismo valor que un documento en papel, firmado en forma manuscrita, consagrado en el artículo 4 del proyecto de ley. Este principio tiene importantes consecuencias en relación con las disposiciones del Código Civil y del Código de Comercio, que regulan lo relativo a documentos y al requisito de la firma en las transacciones civiles y comerciales. En este sentido, las disposiciones ya existentes sobre firma y sobre documentos pueden ser compatibles con las nuevas disposiciones sobre firma digital,

aunque es recomendable la reforma de algunos artículos para dar mayor claridad, como se verá más adelante.

Importante es también el análisis de otras consecuencias prácticas de la aplicación de esta ley, como por ejemplo las pautas especiales que, sobre su interpretación, deban seguirse.

Posteriormente, se analizará el caso de algunas otras disposiciones, tanto legales como reglamentarias, sobre todo relacionadas con el trámite judicial, en las cuales ya se ha abierto la posibilidad de utilizar medios electrónicos. Es importante destacar que, muy acertadamente, en estas disposiciones siempre se ha respetado el principio de neutralidad tecnológica, explicado anteriormente. En este sentido, la firma digital constituye el dispositivo necesario y adecuado para implementar debidamente estas disposiciones. Este análisis se hace a manera de ejemplo, ya que las aplicaciones que la firma digital tiene en la tramitación judicial y administrativa son innumerables. Cada vez que un documento deba ir firmado, esa firma manuscrita puede ser sustituida por la digital, con evidentes ventajas en términos

de seguridad y agilidad en la tramitación, sin contar los importantes beneficios para el medio ambiente.

Al tratar este proyecto de ley de regular una materia nueva, sobre la cual no se encuentran antecedentes jurisprudenciales, el análisis se hará al tenor literal de los artículos pertinentes.

1. ASPECTOS CONSTITUCIONALES (AUTONOMÍA DE LA VOLUNTAD / PRINCIPIO DE LEGALIDAD)

Uno de los principales elementos que hay que destacar en relación con este proyecto de ley es que el uso de la firma digital ya se está dando entre los particulares. El proyecto intenta regular dicha actividad con el fin de asegurarle valor jurídico a determinados actos.

El segundo propósito de esta ley es el dar una autorización al Estado para que cuente también con la posibilidad de utilizar la firma digital en sus transacciones, en sus actuaciones internas, así como también en su interrelación con los administrados. Por supuesto, esta es apenas la

autorización legal, y hace falta además un esfuerzo económico y de reorganización y modernización de la administración, en general, para lograr una implementación total de estas disposiciones; es el primer paso del "gobierno digital" (*e-government*).

Ambas consideraciones están recogidas en el artículo primero de la ley que establece lo siguiente:

> *"La presente ley tiene por objetivo reconocer y regular el uso de la Firma Digital y los Certificados Digitales, otorgándole a los documentos firmados digitalmente la misma validez y eficacia jurídica que aquellos con firma manuscrita que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización."*

Según el principio de autonomía de la voluntad, los particulares pueden hacer todo aquello que no esté expresamente prohibido por el ordenamiento jurídico. En relación con el primer punto, el artículo 28 de la Constitución Política establece en su párrafo segundo que:

> *"[l]as acciones privadas que no dañen la moral o el orden público o que no perjudiquen a tercero, están fuera de la acción de la ley."*

En este sentido el proyecto de ley es concordante con esta disposición constitucional, especialmente en su artículo 9 que establece:

> *"Las disposiciones de [la] Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de la contraparte."*

Esta disposición que podría parecer obvia y redundante, sobretodo a la luz del artículo 28 constitucional, en realidad, es muy necesaria. Esta norma evidencia que la intención de la ley no es limitar la libertad de los

particulares para usar la firma digital ni la posibilidad de pactar las condiciones para su uso. La ley pretende dar valor jurídico a una actividad que ya está siendo desarrollada por las partes.

Una norma similar se encuentra contenida en la Ley Modelo sobre Firmas Electrónicas de la UNCITRAL[67], así como en la Directiva 1999/93 del Parlamento Europeo y del Consejo de la Unión Europea.

En el párrafo considerativo número 16 de la Directiva, el Parlamento y el Consejo de la Unión expresaron su preocupación sobre este punto en los siguientes términos:

> *"[...] no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrados entre un número determinado de participantes. En la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán*

[67] Ley Modelo de la CNUDMI sobre Firmas Electrónicas, artículo 3.

las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales".

Una consecuencia lógica de una consideración como la anterior, es la adopción de un artículo en los términos del numeral 5.2 de la misma directiva, que establece que no se le deberá negar valor jurídico, ni en cuanto a su eficacia, ni en cuanto a su carácter de prueba, a un documento por el simple hecho de ser electrónico. No encontramos en el proyecto de ley costarricense ninguna norma en este sentido. De alguna forma queda incompleta la consideración, ya que si bien se establece que se respeta la libertad para pactar las condiciones que se crean más convenientes en cuanto a la firma digital, se está obligando a las partes a utilizar los procedimientos de acreditación establecidos en la ley, si se quiere que ésta tenga reconocimiento del ordenamiento jurídico costarricense. En todo caso, esto no roza con el principio de libertad constitucional, porque las partes están en libertad de determinar las condiciones de uso de la firma

digital, pero el Estado fija ciertas pautas para dar reconocimiento jurídico a sus actividades.

La situación del Estado es exactamente opuesta a la de los particulares. De conformidad con el principio de legalidad, la Administración Pública sólo puede realizar aquellos actos para los cuáles ha sido expresamente autorizada por el ordenamiento jurídico.

Este principio está recogido en el artículo 11 de la Constitución Política, que establece lo siguiente:

> *"[l]os funcionarios públicos son simples depositarios de la autoridad y no pueden arrogarse facultades que la ley no les concede"*

El principio de legalidad que rige la actuación de la Administración, también se encuentra consagrado en el párrafo primero del artículo 11 de la Ley General de la Administración Pública, en los siguientes términos:

> *"La Administración Pública actuará sometida al ordenamiento jurídico y sólo podrá realizar aquellos actos o prestar aquellos servicios*

públicos que autorice dicho ordenamiento, según la escala jerárquica de sus fuentes."

El artículo primero del proyecto señala como uno de los fines de la Ley de Firma Digital y Certificados Digitales, el autorizar al Estado para la utilización de la firma digital. Desarrollando lo establecido en dicho artículo, el artículo 6 del proyecto de ley, prescribe lo siguiente:

"Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales y cualquier dependencia del sector público, incluso en las estructuras según modelos organizacionales del Derecho Privado, para la utilización de la firma Digital acreditada en los documentos electrónicos en sus relaciones internas, entre ellos y con los particulares, así como para poder actuar como entidades certificadoras siempre que cumplan con todos los requisitos que para ese efecto se establezcan, de conformidad con las previsiones de [la] Ley y su reglamento. En lo

atinente a los documentos electrónicos firmados digitalmente se deberá cumplir en los [sic] que sea aplicable con lo que establece la Ley 7202, Ley del Sistema Nacional de Archivos."

De la lectura de ambos artículos se entiende que la intención del redactor del proyecto es simplemente brindar esta autorización al Estado para poder utilizar la firma digital, en virtud del referido principio de legalidad[68].

Esta disposición, además, encuentra concordancia en otras regulaciones sobre firma digital. A manera de ejemplo, en Italia, la regulación de la firma digital se introdujo como la autorización necesaria a la Administración Pública para utilizar este mecanismo. Con base en esa disposición, se desarrolló la normativa pertinente para el pleno reconocimiento en el ordenamiento jurídico italiano de la firma digital. En efecto, la principal norma sobre documento electrónico en Italia, con base en la cual se dictó el Reglamento sobre firma digital, es el artículo 15 de la ley

---

[68] Asamblea Legislativa. Informe técnico, Departamento de Servicios Técnicos, pág. 19. Expediente número 14.276. Entrevista con Oscar Solís, abogado del Ministerio de Ciencia y Tecnología. 17 de julio de 2002.

No. 9 del 15 de marzo de 1997, analizada anteriormente. El párrafo segundo de este artículo autoriza a la Administración Pública para la utilización de medios telemáticos o informáticos en sus gestiones.

En igual sentido, el Real Decreto-Ley español sobre firmas electrónicas también incluye en su artículo 5 la autorización a la Administración Pública para que pueda utilizar la firma electrónica.

En consecuencia, resulta infundada la crítica realizada al proyecto de ley sobre una posible confusión en cuanto a la intención del proyecto de excluir a los particulares del uso de la firma digital, y establecer un monopolio para su uso a favor del Estado costarricense[69].

Es obvio que los particulares no necesitan una autorización para utilizar la firma digital, como sí la necesita el Estado, en virtud del principio de legalidad.

---

[69] PÉREZ MERAYO, Guillermo Augusto. Op. Cit.

De la relación de ambos principios constitucionales, el de autonomía de la voluntad y el de legalidad, es claro que los artículos 1, 6 y 9 del proyecto no pueden ser entendidos en el sentido de excluir a los particulares del uso de la firma digital, ni de establecerlo exclusivamente para el Estado.

Tampoco se establece un monopolio a favor del Estado, pretendiendo que las autoridades de certificación sean públicas. El artículo 6 establece como una facultad, que los órganos del Estado pueden ser autoridades de certificación. En realidad, cualquier persona física o jurídica puede constituirse en una autoridad de certificación, y cualquier autoridad de certificación puede someterse al procedimiento de acreditación voluntaria. Ni el artículo 12, ni el 14 del proyecto, que regulan la figura de las autoridades de certificación, excluyen de esta actividad a los particulares.

En este sentido, la Directiva de la Unión Europea señala en su parte considerativa que:

> *"Los servicios de certificación pueden ser prestados tanto por entidades públicas como por personas físicas o jurídicas cuando así se*

establezca de acuerdo con el Derecho nacional. Los Estados miembros no deben prohibir a los proveedores de servicios de certificación operar al margen de los sistemas de acreditación voluntaria; ha de velarse por que los sistemas de acreditación no supongan mengua de la competencia en el ámbito de los servicios de certificación."

De la consideración de todos estos elementos se colige que el servicio de certificación puede ser prestado tanto por entidades públicas como privadas, sin ninguna restricción, más que la de cumplir con los requisitos que garanticen seguridad, y el proyecto de ley costarricense es coincidente con esta conclusión.

No debe confundirse la posibilidad de que cualquier persona física o jurídica, pública o privada, pueda actuar como autoridad de certificación, con la función exclusiva del Ministerio de Ciencia y Tecnología como Órgano Rector en esta materia, ni con las funciones de la Autoridad Acreditadora que se establece mediante esta ley.

La firma digital es una aplicación cuyo éxito depende en gran medida de la confianza que se tenga en el mecanismo, como en la empresa o prestador del servicio de certificación. De ahí que es importante la figura de la acreditación voluntaria recogida en este proyecto de ley, que además es coincidente con otras normas sobre este mismo punto.

Establecida la necesidad de un mecanismo como el de la acreditación voluntaria, queda la duda sobre ¿a quién será conveniente encargarle esta importante labor? El Estado goza de neutralidad en este punto, ya que aparte de ser el Estado, es uno más de los usuarios de la firma digital. Además, se cuenta con la garantía constitucional de la revisión jurisdiccional de las actuaciones de la Administración, a través de la vía contencioso-administrativa[70], de las actuaciones de la entidad acreditadora. De todos los Ministerios del Poder Ejecutivo, por la competencia por la materia, el de Ciencia y Tecnología es el de mayor afinidad con este tema y, además, el que puede contar con mayores elementos técnicos, en infraestructura, personal y

[70] Constitución Política, artículo 49.

conocimiento, para manejar la función de servir de Autoridad Acreditadora. [71]

Es necesario analizar porqué se le da a esta institución y no a otra, tan importante función. Dentro de las funciones de este Ministerio, otorgadas por la ley número 7169, está dirigir el desarrollo tecnológico. Además, dentro de las competencias que tiene el MICIT, está la secretaría del Ente Nacional de Acreditación (ENA)[72], ente encargado de acreditar y verificar los productos y servicios de las empresas. Al ser la firma digital un producto, el MICIT tiene plena competencia otorgada por ley de ser el Órgano Rector, encargado de la acreditación de las entidades de certificación.[73]

---

[71] Entrevista con Oscar Solís, abogado del Ministerio de Ciencia y Tecnología. 17 de julio de 2002.
[72] Ley de Sistema Nacional de Calidad, número 8279.
[73] Entrevista con Oscar Solís, abogado del Ministerio de Ciencia de Ciencia y Tecnología. 17 de julio del 2002.

2. ASPECTOS LEGALES Y REGLAMENTARIOS

A. PRINCIPIO DE EQUIVALENCIA FUNCIONAL CON LA FIRMA MANUSCRITA

El proyecto de ley se relaciona principalmente con el Código Civil, en el cual se encuentran consagradas las principales normas sobre el consentimiento, y con el Código de Comercio, donde se pueden encontrar importantes disposiciones sobre la firma.

En Francia, la firma digital se introdujo, en primer lugar, como una reforma al artículo del Código Civil que regula la firma manuscrita. Con posterioridad, se dictó el decreto No. 2001-272 que contiene todas las disposiciones para la aplicación de la firma digital. En Costa Rica, al redactar el proyecto de ley para regular la firma digital, se consideró inicialmente que una reforma al Código Civil podía ser la vía para hacerlo[74].

[74] Entrevista con Oscar Solís, abogado del Ministerio de Ciencia y Tecnología. 17 de julio de 2002.

La firma manuscrita cumple una doble función en el derecho: por un lado, identifica al firmante y, por el otro, indica que éste ha aceptado el contenido de lo firmado e incluso que tiene intención de vincularse por lo expresado.

El reconocimiento del principio de equivalencia funcional es el objetivo principal del proyecto de ley; así está consagrado en el artículo primero, en los siguientes términos:

> *"La [...] Ley tiene por objetivo reconocer y regular el uso de la Firma Digital y los Certificados Digitales, otorgándole a los documentos firmados digitalmente la misma validez y eficacia jurídica que aquellos con firma manuscrita que conlleve manifestación de voluntad, [...]."*

En aplicación de este principio, el artículo 4 del proyecto de ley señala, en el primer párrafo, que:

> *"La Firma Digital, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en*

forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel."

Como se señaló anteriormente, es posible dar equivalencia a la firma digital con la firma manuscrita por las garantías que la firma digital debe asegurar. En este sentido, el artículo 7 del proyecto de ley establece los siguientes requisitos para que un dispositivo de creación de firma pueda ser considerado seguro:

1.- Garantizar que los datos utilizados para la generación de firma puedan producirse sólo una vez y corresponden exclusivamente al firmante, asegurando razonablemente su secreto, dentro de las posibilidades o limitaciones tecnológicas.

2.- Que exista seguridad razonable de que dichos datos no pueden ser alterados o falsificados con la tecnología existente en un momento dado y que es posible detectar cualquier alteración de la firma hecha con posterioridad al momento de firmar.

3.- Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros y que en el momento de firmar estén bajo su control.

4.- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

5.- Que sea posible detectar cualquier alteración de esa información, hecha con posterioridad al momento de firmar.

Todas estas garantías aseguran que el firmante pueda estar plenamente identificado, y que cada vez que aparezca su firma digital ha sido él y sólo él quien la ha utilizado. Además, el procedimiento para firmar digitalmente establecido en el inciso 4 de este artículo, asegura que el firmante conoce el contenido total del documento antes de firmarlo. La firma digital constituye entonces una forma de manifestar conformidad con el contenido de lo firmado.

Sobre el consentimiento, el artículo 1008 del Código Civil establece que:

> *"El consentimiento de las partes debe ser libre y claramente manifestado.*
> *La manifestación puede ser hecha de palabra, por escrito o por hechos de que necesariamente se deduzca."*

Para efectos de la aplicación de este artículo, la utilización de la firma digital no consiste en "hechos de los cuales se deduce el consentimiento", sino que es una manifestación clara del mismo. En este sentido, es una forma de consentimiento por escrito.

Como una consideración adicional se puede señalar que, además de las garantías de la firma manuscrita, la firma digital asegura también que el mensaje no ha sido alterado después de firmado, e incluso puede garantizar la confidencialidad del mensaje.

La firma manuscrita, además, está establecida como un requisito en diferentes actos jurídicos, entre ellos, los contratos que deban constar por escrito. En este sentido, el artículo 413 del Código de Comercio establece lo siguiente:

> *"Los contratos que por disposición de la ley deban consignarse por escrito, llevarán las firmas originales de los contratantes. [...] Las cartas, telegramas o facsímiles equivaldrán a la forma escrita, siempre que la carta o el original del telegrama o facsímil estén firmados por el remitente, o se pruebe que han sido debidamente autorizados por éste."*

De conformidad con lo señalado anteriormente sobre el principio de equivalencia funcional en el proyecto de ley, se entiende que el requisito de "firma original de los contratantes" queda satisfecho plenamente con la firma digital.

Una especial consideración merece el artículo 414 del Código de Comercio que establece, sobre la firma, lo siguiente:

"La firma reproducida por algún medio mecánico no se considerará eficaz, salvo [en] los negocios, actos o contratos que la ley o el uso lo admitan, especialmente cuando se trate de valores emitidos en número considerable."

Es claro que este artículo no es aplicable a la firma digital, porque ésta no es una "forma de reproducción mecánica de la firma manuscrita", sino que es un método independiente de firmar, basado en una aplicación informática y que, como se ha estudiado, asegura todas las garantías, y aún otras adicionales, de la firma manuscrita.

En la sección de disposiciones generales sobre obligaciones y contratos del Código de Comercio encontramos también el artículo 411, que establece lo siguiente:

"Los contratos de comercio no están sujetos, para su validez, a formalidades especiales, cualesquiera que sean la forma, el lenguaje o idioma en que se celebren, las partes quedarán obligadas de manera y en los términos que aparezca que quisieron obligarse. Se exceptúan de esta disposición los

contratos que, de acuerdo con este Código o con leyes especiales, deban otorgarse en escritura pública o requieran forma o solemnidades necesarias para su eficacia."

Hay ocasiones en las que la ley exige el requisito de escritura pública, lo que es reconocido en este artículo. Por ejemplo, en el artículo 1256 del Código Civil se establece que el poder especial para actos inscribibles en el Registro Público debe ser protocolizado. Este requisito permanece inalterado por el proyecto de ley sobre firma digital.

La utilización de la firma digital no supone una sustitución del notario público por la autoridad de certificación. Según el principio de equivalencia funcional, la firma digital equivale a la firma manuscrita simple, no a la autenticada o certificada. El proyecto no extiende los efectos de la utilización de la firma digital hasta considerarla equivalente a la firma autenticada por Notario o por otro funcionario público, como por ejemplo el Oficial de Autenticaciones del Ministerio de Relaciones Exteriores.

Cada vez que la ley exija la formalidad la firma autenticada, deberá constar la autenticación del Notario o del funcionario público competente. En el mismo sentido, en caso de que el ordenamiento requiera la celebración de un acto mediante escritura pública, ésta deberá ser confeccionada por el Notario público, como hasta ahora se ha hecho.

En relación con este punto, se puede plantear un problema práctico: ¿cómo proceder cuando una firma digital deba estar autenticada o certificada por un funcionario público? El mismo proyecto de ley contiene una disposición que pretende dar una solución a este problema. El artículo 5 dispone que el funcionario público competente podrá autenticar una firma digital acreditada utilizando su propia firma digital.

Como se ve, el requisito de la autenticación, cuando esté establecido en una ley o en un reglamento, permanece inalterado, y a cargo del mismo funcionario. La innovación del proyecto de ley consiste en la forma en que se lleve a cabo esa autenticación. Con el proyecto de ley existe la posibilidad de tener un documento con dos firmas digitales en

vez de dos firmas manuscritas: una autenticando a la otra. Concretamente el artículo 5 establece lo siguiente:

> *"Cuando una ley requiere que un documento o firma esté certificado o de cualquier otra forma reconocida, verificado tal requisito se tendrá por cumplido si una firma digital acreditada de un funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma Digital acreditada."*

Es importante señalar que en el proyecto originalmente presentado a la Asamblea se incluía a los notarios públicos y abogados en este artículo[75]. Sin embargo, fueron eliminados en esta última versión.

Este artículo plantea todavía otro problema práctico: ¿cuáles criterios debe utilizar el funcionario público para

---

[75] El artículo 6 del proyecto original establecía que:
"Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado, o de cualquier otra forma reconocido, verificado o certificado, tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma digital o Firma Digital Avanzada."

autenticar o certificar una firma digital? En el caso de la firma manuscrita el procedimiento es muy sencillo: se reduce a la confrontación de la firma por autenticar con otra de la misma persona contenida en algún documento de identificación o en un registro de firmas. En el caso de la firma digital, se deben utilizar los dispositivos de verificación, cuyas garantías mínimas están reguladas en el artículo 8 del proyecto de ley[76].

B. EL DOCUMENTO ELECTRÓNICO Y EL PRINCIPIO DE PRUEBA POR ESCRITO

Sobre el documento electrónico el proyecto de ley en el párrafo 2 del artículo 4 establece que:

> *"Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal*

---

[76] Artículo 8 del Proyecto de Ley:
"Los dispositivos de verificación de Firma Digital Acreditada deben garantizar al menos lo siguiente:
1.- Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.
2.- Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.
3.- Que aparezca correctamente la identidad del signatario.
4.- Que se verifique de forma fiable el certificado.
5.- Que puede detectarse cualquier cambio relativo a su seguridad e integridad.
6.- Los demás que el reglamento establezca."

requisito será plenamente satisfecho por un documento digital, si el mismo ha sido firmado mediante una Firma Digital Acreditada."

En el ordenamiento jurídico costarricense no existe una definición puntual de lo que se debe entender por documento. Más bien encontramos una lista de elementos que deben o pueden ser considerados para establecer el carácter de documento, lista que no es taxativa. A continuación, se analizarán los artículos más relevantes que hacen referencia al documento y cómo se relacionan con las definiciones de documento contenidas en el proyecto de ley.

Una de las disposiciones más relevantes en materia de documento electrónico está contenida en el artículo 6 *bis* de la Ley Orgánica del Poder Judicial, que establece lo siguiente:

"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." [el destacado no es del original]

Este artículo constituye uno de los primeros reconocimientos del documento electrónico como válido y eficaz. Es interesante destacar que, con gran visión, este reconocimiento está redactado en términos tecnológicamente neutros, sin especificar ninguna tecnología. El requisito de *"garantizar (…) autenticidad, integridad y seguridad"* no

puede referirse a otra cosa más que a la firma digital. En este sentido, las disposiciones sobre firma y documento digital contenidas en el proyecto de ley no sólo están en armonía con lo establecido en este artículo, sino que están ya previstas en él.

A pesar de esto, el párrafo 4 de este artículo presenta contradicciones con el proyecto de ley, específicamente con lo que ya se ha dicho sobre el principio de equivalencia funcional. En este sentido, el requisito para las partes de tener que presentar el "documento original" dentro del tercer día, quedaría tácitamente derogado con la aprobación de la ley sobre firma digital y certificados digitales. Si un documento electrónico firmado digitalmente tiene el mismo valor que uno en papel que contenga una firma manuscrita, ya no habría "documento original" que presentar; el documento electrónico debidamente firmado sería en sí mismo el original.

Una posible justificación para el requisito del párrafo 4 es que siempre se necesitaría el documento en papel, porque los expedientes se llevan en ese soporte y todavía no existe la

infraestructura necesaria para poder tramitar los procedimientos en forma completamente electrónica. En ese sentido, se podría crear un mecanismo de autorización especial para tramitar un caso en forma electrónica, tal vez por medio de un incidente. Como sucede ahora con las notificaciones por fax: quien desee ser notificado por este medio lo puede solicitar expresamente, a la vez que todavía se utilizan los medios tradicionales de notificación para los demás casos. De esta forma, sería posible sustituir el papel por medios electrónicos, que ya estaría previsto en el ordenamiento jurídico con la aprobación de la ley sobre firma digital, sin tener que forzar una reforma de todo el sistema de tramitación judicial. Incluso, el artículo 147 de la Ley Orgánica del Poder Judicial, contiene esta posibilidad:

> "*La Corte podrá disponer la utilización de sistemas informáticos para notificaciones, citaciones, comunicación entre oficinas judiciales y externas, públicas o privadas, archivo, manejo de documentación e información, atención al usuario, y para cualquier otro acto en que se demuestre que el uso de la informática agiliza el procedimiento, caso en que las constancias propias del sistema*

resultan suficientes para acreditar la realización del acto procesal que las generó, salvo acto en contrario."

También encontramos disposiciones sobre el documento en el Código Procesal Civil, sobre todo relacionadas con la prueba en el procedimiento en general y, especialmente, el civil.

El artículo 368 del Código Procesal Civil establece la siguiente definición:

> *"**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."*

En el proyecto de ley, a su vez se establecen dos definiciones más de documento: la del documento electrónico y

la del documento digital. En el artículo 2 de dicho proyecto se expresan estas definiciones en los siguientes términos:

> *"Para los propósitos de la [...] Ley se establecen las siguientes definiciones:*
>
> ***6.- Documento electrónico:*** *es toda representación electrónica de actos, hechos, datos o descripciones, y que se puede recuperar o reproducir en una forma perceptible e inteligible.*
>
> ***7.- Documento digital:*** *es un documento electrónico cuyo contenido está codificado. En la [...] Ley se utilizará el término digital como cualquier información codificada en dígitos binarios."*

El artículo 368 del Código Procesal Civil es lo suficientemente amplio como para incluir estas dos nuevas definiciones de documento, si se entiende que pueden estar comprendidas en la última frase del artículo. Para saber que es lo que en el ordenamiento jurídico costarricense se entiende por objeto mueble, debemos remitirnos al artículo 256 del Código Civil, que establece lo siguiente:

"Todas las cosas o derechos no comprendidos en los artículos anteriores [que definen los bienes inmuebles]*, son muebles."*

La lectura de este artículo, en conjunto con las definiciones del proyecto de ley y el artículo 6 *bis* de la Ley Orgánica del Poder Judicial, nos permite establecer que tanto el documento electrónico como el digital deben ser considerados como una clase de documento, a la luz del artículo 368 del Código Procesal Civil.

Esta conclusión tiene importantes consecuencias en la aplicación de las reglas sobre prueba establecidas en el mismo Código Procesal Civil, las cuales pueden ser aplicadas directamente al documento electrónico, sin ninguna distinción con el documento en papel.

El artículo 372 del Código Procesal Civil establece el principio de prueba por escrito al señalar lo siguiente:

"Para que haya principio de prueba por escrito es necesario:

1) *Que el escrito del que se pretende hacerlo resultar, emane de la persona a quien se opone, o de aquél a quien ella representa, o de aquél que la haya representado.*

2) *Que tal escrito haga verosímil el hecho alegado."*

Por su parte el artículo 373 del mismo cuerpo normativo establece la siguiente presunción:

> *"**Presunción de la causa.** El documento en el que se consigne una obligación sin expresar la causa de ella, hará presumir la existencia y legalidad de dicha causa, mientras el deudor no la niegue; pero si éste la niega, el acreedor estará obligado a probar la existencia de la causa, en cuyo caso el documento servirá como principio de prueba escrita.*

Finalmente, el artículo 379, también del Código Procesal Civil, señala que:

> *"**Documentos privados.** Los documentos privados reconocidos judicialmente o declarados como*

reconocidos conforme con la ley, hacen fe entre las partes y con relación a terceros, en cuanto a las declaraciones en ellos contenidas, salvo prueba en contrario."

En virtud de lo expresado, en relación con el documento electrónico a la luz de los artículos 368 del Código Procesal Civil y 6 *bis* de la Ley Orgánica del Poder Judicial, estas tres normas pueden ser aplicadas al documento electrónico, aunque el proyecto de ley no le reconozca el carácter de prueba en juicio expresamente, como sí lo hacen otras leyes.

Una especial consideración merecen las disposiciones sobre fecha cierta contenidas también en el Código Procesal Civil. El artículo 380 de ese Código establece lo siguiente en relación con este punto:

*"**Fecha cierta** La fecha cierta de un documento privado no se contará respecto de terceros, sino desde que se verifique uno de los hechos siguientes:*

1) La muerte de alguno de los firmantes.

2) La presentación del documento ante cualquier oficina pública, para que forme parte de un expediente con cualquier fin.

3) La presentación del documento ante un notario, a fin de que se autentique la fecha en que se presenta.

[...]"

En relación con esta disposición, existe una aplicación de los mecanismos de firma digital que es el sellado temporal. En su Informe Técnico sobre el proyecto de ley, el Departamento de Servicios Técnicos señaló:

"[...] se recomienda establecer en el proyecto, el sello temporal digital dentro del certificado como otro aspecto más de su contenido [de los certificados digitales], *de manera que se pueda garantizar que las firmas fueron creadas en un momento en que las claves y el certificado eran*

válidos. 'Sellar temporalmente un documento electrónico significa sellar temporalmente los datos mismos, de forma que sea imposible cambiar incluso un solo bit sin que el cambio se ponga de manifiesto; el sellado temporal implica también que es imposible sellar un documento con una hora y una fecha diferente a la actual [...]'"

El proyecto de ley sobre firma digital costarricense no establece esta posibilidad que, por el contrario, sí está regulada en otros sistemas, como por ejemplo el alemán.

Aunque el Departamento de Servicios Técnicos recomienda esta aplicación para dar más seguridad al certificado digital, el sellado temporal en sí mismo podría ser de utilidad para establecer la fecha cierta de un documento digital, en cuyo caso sería conveniente reformar el artículo 380 del Código Procesal Civil.

C. LA FIRMA DIGITAL EN LA TRAMITACIÓN JUDICIAL

Como ya se estudió, la misma Ley Orgánica del Poder Judicial contempla la utilización del documento electrónico en la tramitación judicial. La adopción de una regulación adecuada de la firma digital viene a llenar el requisito del artículo 6 *bis* en relación con *"los procedimientos establecidos para garantizar su autenticidad, integridad y seguridad."*

Existe una gran cantidad de normas donde ya están contempladas las posibilidades de utilizar medios electrónicos en la tramitación judicial. Estas disposiciones están redactadas en una forma muy amplia, y en ocasiones omiten señalar cuáles son las garantías que esos medios electrónicos deben brindar para poder ser aceptados. En este sentido, la ley de firma digital es necesaria para complementar estas normas, con el fin de que se puedan aplicar correctamente.

Las disposiciones más relevantes en cuanto a documento electrónico y su carácter de prueba en el proceso judicial ya fueron analizadas en el punto anterior. A continuación, se

analizarán algunas normas con carácter ilustrativo pero no exhaustivo, que demuestran el impacto que puede tener la aprobación de la ley de firma digital en el proceso judicial.

i. Notificaciones

La Corte Suprema de Justicia ya ha adoptado importantes normas, por vía reglamentaria, sobre la notificación por medios electrónicos.

El artículo primero del Reglamento para el Uso del Fax como Medio de Notificación en los Despachos Judiciales señala lo siguiente:

> "*Las oficinas centralizadas de notificación que fueren creadas de conformidad con la Ley número 7637 (de notificaciones, citaciones y otras formas de comunicaciones judiciales), al igual que los demás despachos judiciales, a los que se les haya dotado de fax, o que cuenten con los servicios de transmisión por fax a través de las unidades administrativas regionales o la sección de comunicaciones, podrán notificar por este medio a*

las partes que así lo hayan solicitado de modo expreso e inequívoco. El fax receptor puede estar instalado en cualquier lugar del territorio nacional."

El párrafo 2 del artículo 4 del mismo Reglamento establece que:

"Cuando la tramitación del caso tuviere respaldo informático, las comunicaciones y constancias se harán en él, sin necesidad de enviar comunicación o constancia por escrito."

Por otra parte, la Circular No. 36-2000, Reglamento de Notificaciones y Comunicaciones por Medios Electrónicos, señala en el artículo primero que:

"Se autoriza a los Tribunales de Justicia del I y II Circuitos Judiciales de San José, para notificar resoluciones judiciales por medios electrónicos."

Existen en el Código Procesal Penal varias normas que buscan dar mayor agilidad en el proceso de notificaciones. Al amparo de estas normas y con base al artículo 147 de la Ley Orgánica

del Poder Judicial, esta mayor eficiencia puede ser lograda utilizando la firma digital. [77]

ii. Otras aplicaciones prácticas

Los artículos 138 y 149 del Código Procesal Penal establecen lo siguiente:

---

[77] "Artículo 155: **Regla general.** Las resoluciones deberán notificarse a quien corresponda, dentro de veinticuatro horas después de ser dictadas, salvo que el tribunal disponga un plazo menor."

[...]

"Artículo 156, párrafo 2: Cuando deba practicarse una notificación fuera del asiento del tribunal, se solicitará el auxilio de la autoridad respectiva, sin perjuicio de que el notificador del despacho se desplace si así lo dispone el tribunal."

"Artículo 157: **Lugar para notificaciones.** Al comparecer en el proceso, las partes deberán señalar, dentro del perímetro judicial, un lugar para ser notificadas.

[...]

Los defensores, fiscales y funcionarios públicos que intervienen en el procedimiento serán notificados en sus respectivas oficinas, siempre que éstas se encuentren dentro del perímetro judicial."

"Artículo 160: **Forma especial de notificación.** Cuando el interesado lo acepte expresamente, podrá notificársele por medio de carta certificada, facsímil o cualquier otro medio electrónico. En este caso, el plazo correrá a partir del envío de la comunicación, según lo acredite el correo o la oficina de transmisión. También podrá notificarse mediante otros sistemas autorizados por la Corte Suprema de Justicia, siempre que no causen indefensión."

"Artículo 163: **Notificación en caso de urgencia.** En caso de urgencia, podrá notificarse por teléfono o por cualquier otro medio de comunicación similar. Se dejará constancia sucinta de la conversación y de la persona que dijo recibir el mensaje."

*"**Reemplazo del acta.** El acta podrá ser reemplazada, total o parcialmente, por otra forma de registro, salvo disposición expresa en contrario. En ese caso, quien preside el acto determinará el resguardo conveniente para garantizar la inalterabilidad y la individualización futura."*

*"**Copia auténtica.** Cuando, por cualquier causa se destruya, se pierda o sea sustraído el original de las sentencias o de otros actos procesales necesarios, la copia auténtica tendrá el valor de aquel.*

[...]

La reposición también podrá efectuarse utilizando los archivos informáticos del tribunal."

Ambos casos son ejemplos de situaciones donde ya se prevé la utilización de medios electrónicos en la tramitación judicial, y en donde, además, la firma digital puede aportar importantes contribuciones.

III. ANALISIS DEL PROYECTO DE LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITLES NÚMERO 14.276

El artículo primero del Proyecto de Ley de Firma Digital y Certificados Digitales, presentado por el Poder Ejecutivo, indica:

> *"La presente ley tiene por objeto regular el uso y el reconocimiento jurídico de la Firma Digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como autorizar al Estado para su utilización."*

La presente ley va directo al grano. En su primer artículo deja por sentado su objetivo: otorgarle la misma validez legal a la firma digital que a la firma manuscrita. La Asamblea Legislativa cambió la redacción de este artículo, de la siguiente forma:

> *"La presente ley tiene por* ***objetivo reconocer*** *y regular el uso de la Firma Digital y los* ***Certificados Digitales,*** *otorgándole* ***a los***

documentos firmados digitalmente *la misma validez y eficacia jurídica* ***que aquellos con firma manuscrita*** *que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización."*[Lo destacado no es del original]

Lo que está destacado son las modificaciones que se efectuaron al artículo en estudio. La redacción del artículo mantiene su estructura. Con estas modificaciones los legisladores pretenden darle claridad al texto, especificando que los documentos que estén firmados digitalmente tendrán el mismo valor que los firmados con una firma manuscrita. Incorporan el término de documento, lo que resulta redundante, pues para que exista una firma digital su soporte va a ser siempre un documento digital. Es importante tener claro que el objeto de la ley es la firma y no el documento digital. La inferencia de este concepto puede llevar a confusión. Al incorporar este término, los legisladores procedieron a definirlo en el artículo segundo:

"6.- Documento electrónico: es toda representación electrónica de actos, hechos, datos o

hacer distinción entre documento electrónico y digital, de la siguiente manera:

> "*Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra naturaleza, y que se puede recuperar o reproducir en una forma perceptible o inteligible.*"

Esta ley debe ser clara, concisa y simple, con una base tecnológica explicada de tal forma que sea entendida por todos. Las modificaciones efectuadas a este artículo son innecesarias y llevan a confusión.

El licenciado Pérez Merayo critica la última frase del artículo en estudio: "*(…), así como el autorizar al Estado para su utilización.*" Dice que "*esto confunde grandemente pues no tiene continuidad con lo anterior. ¿Cuál es la intención del redactor? ¿Es una exclusión que se hace a los particulares del uso de la firma digital?*"[78]

[78] PÉREZ MERAYO, Guillermo Augusto. Op. Cit.

No tiene sentido que la firma digital sea para uso exclusivo del Estado. Lo que busca este artículo es cumplir con el principio de legalidad para que el Estado pueda hacer uso de la firma, sin excluir a los particulares, como se estudió anteriormente.

Con base en el artículo 2, se discutió en la Asamblea Legislativa si el artículo debía eliminarse o mantenerse. Hubo dos criterios: por un lado, consagrar solamente definiciones en el reglamento y, por otro lado, al ser una ley sumamente técnica, mantener las definiciones en la ley para brindarle al lector una guía sin tener que acudir a un reglamento.[79]

Se mantuvo la segunda posición. Este artículo define los siguientes conceptos: acreditación, acreditación voluntaria del prestador de servicios de certificación, certificado digital, certificado digital reconocido, datos de creación de firma, documento electrónico, documento digital, firma digital, firma digital acreditada, información íntegra,

[79] Asamblea Legislativa. Proyecto de Ley de Firma Digital y Certificados Digitales, expediente número 14.275. Acta de la Comisión Técnica No 012.

mensaje de datos, prestador de servicios de certificación o entidad certificadora, dispositivo o procedimiento de verificación, parte que confía y signatario. Vamos a estudiar varias definiciones necesarias para nuestro análisis. El proyecto presentado por el Poder Ejecutivo contenía además lo que se entiende por: datos de verificación de firma, dispositivo de creación de firma, dispositivo seguro de creación de firma, documento (suplantado por documento electrónico y documento digital), información, iniciador, intermediario, procedimiento seguro, producto de firma digital, receptor, sistema y sistema de información.

Es necesario reducir las definiciones puesto que se trata de una ley, no de un diccionario, siempre y cuando estén todos los conceptos necesarios para que se entienda el contenido de la ley.

El inciso 8 del artículo en mención define la firma digital como:

> "(...) *el conjunto de datos asociados funcionalmente a un documento electrónico, utilizados como medio*

para identificar formalmente al firmante e indicar que este aprueba el contenido del documento."

Esta definición de firma digital se apega al principio de neutralidad tecnológica. La tecnología puede cambiar y la ley va a seguir regulando sin ningún problema la firma digital. La ley se mantiene lo suficientemente "elástica" para estar acorde con los cambios que sufre día a día el mundo tecnológico. No es una ley que queda obsoleta en el momento que cambie la tecnología. Asimismo, indica las garantías que debe tener la firma digital, que son las mismas que la manuscrita. Tales garantías que son poder identificar al firmante y que éste al firmar, apruebe el contenido del mensaje. No se mencionan los conceptos de llave pública ni llave privada o encriptación asimétrica, (aunque sea ésta tecnología la utilizada actualmente), ya que esto amarraría la utilización de la firma digital a una tecnología especifica.

El inciso 9 del artículo 2 del proyecto de ley indica lo que se entiende por firma digital acreditada:[80]

> "*Es la Firma Digital certificada por un prestador de servicios de certificación debidamente acreditado ante la Autoridad de Acreditación.*"

Esta definición respeta igualmente el principio de neutralidad tecnológica. Adelante estudiaremos los requisitos necesarios para que una firma digital sea acreditada.

El inciso 10 enuncia una de las garantías que debe brindar la firma digital, al definir lo que se entiende por información íntegra:

> "[es] *aquella información que haya permanecido completa e inalterada, sin menoscabo de cualquier adición o cambio accesorio, inherente al proceso de comunicación, almacenamiento, archivo o presentación.*"

[80] El proyecto de ley presentado por el Poder Ejecutivo, utilizaba el término de firma digital avanzada.

Pérez Merayo considera que este artículo debe excluir de estos conceptos la influencia de la firma digital avanzada (acreditada en la última versión del proyecto)[81] para que sea acorde al principio de neutralidad tecnológica.[82] Sigue diciendo el autor que "*como consecuencias de la confusión causada por la denominación de firma avanzada, el proyecto es omiso de las definiciones necesarias para establecer una infraestructura de llaves (claves) públicas o un Public Key Infrastructure (PKI). Para tal fin es preciso introducir conceptos tales como "llave pública y privada", así como la "función de hash" o hash function (…), que habilita la posibilidad de comprobar si un documento ha sido modificado o no desde que fue firmado;* (…)".[83]

El autor referido se contradice: primero expresa que es necesario que el proyecto de ley esté acorde al principio de neutralidad tecnológica, y que no podrá estarlo hasta que no se elimine el concepto de firma digital acreditada. No tiene sentido eliminar este concepto, ya que es necesario para poder otorgarle validez legal a la firma digital sin

---

[81] Ahora señalada en el proyecto de ley como firma digital acreditada.
[82] PÉREZ MERAYO, Guillermo Augusto. Op. Cit.
[83] PÉREZ MERAYO, Guillermo Augusto. Op. Cit.

amarrarla a una tecnología específica. Después indica el autor que es necesario implementar los conceptos de llave pública y llave privada. Esto no tiene sentido con lo dicho anteriormente ya que, al definir estos conceptos, el proyecto estaría atando la firma digital a la tecnología de criptografía asimétrica, contrario al principio en mención.

El artículo 3, reza:

> *"Ninguna de las disposiciones de la presente Ley, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear, de forma segura, una firma digital acreditada, que cumpla los requisitos de esta ley."*

Este artículo quiere brindar protección al reconocimiento de la firma digital. Aclara que una firma siempre va a tener validez legal, en el tanto cumpla con todos los requisitos exigidos por ley, independientemente del mecanismo utilizado para su creación. Por lo cual, este artículo resalta nuevamente el principio de neutralidad tecnológica.

El artículo 4 es fundamental, pues le otorga a la firma digital acreditada el mismo valor jurídico que la firma manuscrita, de la siguiente manera:

> *"La Firma Digital, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel."*

Se le da el mismo valor jurídico que la firma manuscrita a la firma digital avanzada o acreditada, la cual debe cumplir con los requisitos establecidos en la ley. Se exige en primer lugar que sea "basada en un certificado digital reconocido", el cual está definido en el inciso 4 del artículo 2 del proyecto de la siguiente manera:

> *"Es el certificado digital*[84] *que cumple con los requisitos establecidos en la presente Ley y su*

[84] El inciso 3 del artículo 2 del Proyecto de Ley de Firma Digital y Certificados Digitales define el certificado digital de la siguiente manera: "Es la estructura de datos que vincula unos datos de verificación de firma a un signatario y confirma su identidad, vinculándola con su firma digital."

reglamento, y que vincula una firma digital con determinada entidad como su signatario, mediante un proceso seguro de certificación y verificación; es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la Autoridad de Acreditación."

Este requisito exige que el certificado digital sea emitido por una autoridad de certificación acreditada ante el Órgano Rector. Posteriormente, se analizarán los requisitos necesarios para dicha acreditación. Para que el certificado se emita conforme a la ley, debe ser creado mediante "un proceso seguro de certificación y verificación". De esto se deduce que la tecnología utilizada para firmar un documento digitalmente debe ser segura, que la persona haya tenido la diligencia necesaria al usar su firma y que se utilice un mecanismo adecuado para su verificación. Al respecto, los artículos 7 y 8 establecen dichos requisitos:

"***ARTICULO 7.***- *Los dispositivos seguros de creación de Firma Digital para considerarse como tales deberán cumplir con:*

1.- Garantizar que los datos utilizados para la generación de firma puedan producirse solo una vez y corresponden exclusivamente al firmante, asegurando razonablemente su secreto, dentro de las posibilidades o limitaciones tecnológicas.

2.- Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado y que es posible detectar cualquier alteración de la firma hecho con posterioridad al momento de firmar.

3.- Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros y que en el momento de firmar están bajo su control.

4.- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

5.- Que sea posible detectar cualquier alteración de esa información, hecha con posterioridad al momento de firmar."

*"**ARTICULO 8**.- Los dispositivos de verificación de Firma Digital Acreditada deben garantizar al menos lo siguiente:*

1.- Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.

2.- Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.

3.- Que aparezca correctamente la identidad del signatario.

4.- Que se verifique de forma fiable el certificado.

5.- Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.

6.- Los demás que el reglamento establezca."

El proyecto, en su artículo 2, incisos 1 y 2 entiende por acreditación lo siguiente:

"***Acreditación:*** *Es el procedimiento mediante el cual la Autoridad de Acreditación, creada en esta ley, reconoce formalmente que una entidad o empresa es competente para realizar las tareas de certificación digital, de acuerdo a normas nacionales e internacionales."*

"***Acreditación voluntaria del prestador de servicios de certificación:*** *Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se emite, a petición del interesado, por la Autoridad de Acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa internacional aplicable."*

La acreditación es entonces voluntaria. Esta ley se encuentra dentro del derecho privado, donde las partes se rigen por el principio de autonomía de la voluntad. Por tanto, no se puede exigir que la acreditación sea obligatoria.

El segundo párrafo del artículo en estudio expresa:

> *"Cuando la Ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento digital si el mismo ha sido firmado mediante una Firma Digital Acreditada."*

Este inciso refuerza lo indicado en el artículo primero, haciendo hincapié en que la firma que tiene pleno reconocimiento jurídico es la firma digital acreditada y no la firma digital "simple". Se encuentra nuevamente el principio de equivalencia de documento digital y documento en soporte de papel.

El tercer párrafo del mismo articulo, indica:

"Se presumirá que la Firma Digital y el medio de creación de firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en esta Ley cuando el certificado digital reconocido es emitido por un prestador de servicios de certificación acreditado ante la Autoridad de Acreditación."

Para que la firma digital surta efectos legales, su certificado debe ser emitido por una autoridad de certificación y ésta, a su vez, debe estar acreditada ante la autoridad de acreditación. El articulo 11 crea la autoridad de acreditación como un órgano subordinado al Ministerio de Ciencia y Tecnología. Este Ministerio *"será el Órgano Rector en todo lo concerniente a esta ley"*.[85]

Las funciones de la autoridad acreditante, según el artículo 11, serán las siguientes:

[85] Artículo 10 del proyecto de Ley de Firma Digital y Certificados Digitales.

"a) Autorizar la actividad de las entidades de certificación en el territorio nacional otorgando licencias de operación.

b) Fiscalizar el funcionamiento y la eficiente prestación del servicio por parte de las Entidades de Certificación.

c) Imponer sanciones a las Entidades de Certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

d) Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las Entidades de Certificación.

e) Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en la presente ley.

f) Mantener, procesar, clasificar, resguardar y custodiar el Registro de las Entidades de Certificación de acuerdo a lo dispuesto en los reglamentos respectivos.

g) Recaudar multas de acuerdo a lo dispuesto en los reglamentos respectivos.

h) Actuar como mediador en la solución de conflictos que se susciten entre las Entidades de Certificación y sus usuarios, cuando ello sea solicitado por al menos una de las partes involucradas, sin perjuicio de las atribuciones que tenga el usuario, conforme a esta ley y los reglamentos respectivos.

i) La demás que le asigne el reglamento."

Básicamente, la función de la autoridad de acreditación es de control sobre las autoridades de certificación. Les otorga las licencias de operación, fiscaliza su funcionamiento, en caso de incumplimiento impone sanciones, etc. Además de estas

funciones se le nombra como mediador en la solución de conflictos entre las entidades de certificación y los usuarios, en caso que una de las partes así lo solicite.

El artículo 12 no estaba contenido en el proyecto original. Fue agregado por los legisladores, y es contrario a la definición de acreditación voluntaria que expone el artículo primero. Su primer párrafo indica que:

> *"Mediante la Autoridad de Acreditación, las empresas que emitan certificados de firma digital deberán someterse al proceso de acreditación que se defina en el reglamento."*

La definición de acreditación voluntaria y este artículo se contradicen. Este primer párrafo debe eliminarse, o ser reformado para que incluya el término de "acreditación voluntaria" y esté acorde a la esencia del proyecto. Éste no busca obligar que las autoridades de certificación a que se acrediten, pues la acreditación es facultativa. En este sentido, los particulares, conforme al principio de la autonomía de la voluntad, pueden crear su firma con la entidad de certificación que quieran, sea acreditada o no.

Ahora bien, una firma expedida por una entidad de certificación que esté acreditada tendrá el mismo valor legal que la firma manuscrita y una firma digital que esté emitida por una entidad de certificación no acreditada, seguirá siendo una firma digital, pero no gozará del mismo valor legal que la manuscrita.

El segundo párrafo del mismo artículo establece:

> *"Serán funciones de las empresas certificadoras las de emitir, suspender, cancelar o revocar certificados digitales, así como brindar otros servicios inherentes al propio certificado."*

La ubicación de este párrafo es ilógica e incoherente. En este capitulo se está hablando de la autoridad de acreditación y no de las entidades de certificación, por lo cual debe reubicarse e incorporarse en el capítulo IV: Deberes de las Partes Intervinientes.

El primer párrafo del artículo 14 indica:

> *"El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizará un sistema de*

acreditación, en el ámbito de los prestadores de servicios de certificación de Firma Digital, coordinando para ello con la Autoridad de Acreditación."

Esto fue modificado por la Asamblea Legislativa, ya que el proyecto presentado anteriormente indicaba:

"El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizara un sistema de acreditación voluntario, en el ámbito de los prestadores de servicios de certificación de Firma Digital Avanzada, coordinando para ello con la Autoridad de Acreditación, la cual será un ente con participación activa y equilibrada de los sectores involucrados."

Debe mantenerse el texto del primer proyecto, ya que especifica que se utilizará el sistema de acreditación voluntario, concepto eliminado en el actual artículo 14. Además, creaba una figura sumamente interesante, estableciendo que la Autoridad de Acreditación sería un "ente con participación activa y equilibrada de los sectores

involucrados". Se buscaba una participación interdisciplinaria. Esto guarda similitud con la ley de Argentina, mediante la cual se crea la Comisión Asesora para la Infraestructura de Firma Digital. Esta Comisión busca que se sigan ciertos criterios necesarios para la debida aplicación de la firma digital con la ayuda de expertos en el tema que consultan con los diferentes sectores profesionales. Es una figura necesaria para la adaptación al mundo digital.

El segundo párrafo del artículo en mención prescribe:

> *"La Autoridad de Acreditación mediante la función de acreditación, reconoce formalmente que una organización es competente para llevar a cabo tareas especificas de certificación digital, de acuerdo a los requisitos de normas nacionales e internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente los derechos de los usuarios."*

Este artículo da los lineamientos necesarios que deben cumplir las autoridades de certificación. Remite a los requisitos que se exigen internacionalmente en cuanto

seguridad y confianza para la protección del usuario. Es pertinente que la ley exprese cuáles son los requisitos que deben cumplir dichas autoridades para ser acreditadas. Esto no puede dejarse para ser regulado por reglamento, ya que debe existir un parámetro mínimo que no esté sujeto a modificaciones cada vez que se emita un decreto.

Debe incorporarse aquí el artículo 22 del proyecto que establece los requisitos para que una autoridad certificadora sea acreditada:

> "*Para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:*
>
> "*a) Los recursos humanos y financieros, incluida la existencia de un activo;*
>
> *b) La calidad de los sistemas de equipo y programas informáticos;*

c) Los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) La disponibilidad de información para los firmantes nombrados en el Certificado y para las partes que confíen en éste;

e) La periodicidad y alcance de la auditoria por un órgano independiente

f) La existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y

g) *Cualesquiera otros factores pertinentes."*

En este caso, habría que eliminar el inciso f). No tendría sentido que el Estado emita primero una declaración de que los recursos del prestador del servicio de certificación son

fiables y que éste puede ser acreditado, y que no baste esta declaración para que se dé la acreditación.

El artículo 5 indica:

> *"Cuando una Ley requiere que un documento o firma esté certificado o de cualquier otra forma reconocido, o verificado tal requisito se tendrá por cumplido si una firma digital acreditada de un funcionario publico, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma Digital Acreditada."*

Este artículo es poco claro. Puede redactarse de forma más simple como lo siguiente: "en caso que se requiera una certificación o documento firmado por un funcionario público, este podrá hacerlo mediante la utilización de su firma digital acreditada." Debe eliminarse "cualquier otra persona autorizada" o especificarse qué se debe entender por personas autorizadas. Con esta lectura se puede interpretar hasta que los notarios están autorizados a certificar digitalmente.

El siguiente artículo autoriza al Estado a utilizar la firma digital, cumpliendo con el principio de legalidad.

> "***ARTICULO 6.-*** *Se autoriza a los Poderes Legislativos, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales y cualquier dependencia del sector público, incluso en las estructuras según modelos organizacionales del Derecho Privado, para la utilización de la firma Digital acreditada en los documentos electrónicos en sus relaciones internas, entre ellos y con particulares, así como para poder actuar como entidades certificadoras siempre que cumplan con las previsiones de esta Ley y su reglamento.* (...)"

Para Pérez Merayo "*una interpretación rápida de este artículo deja entrever una intención en el proponente de crear un régimen de la firma digital de uso exclusivo solo por el estado; (...)*". Esto no tiene sentido, desde la lectura del primer artículo, pues es obvio que el fin de esta ley no es crear un régimen exclusivo para el Estado. Por el contrario,

está regulando la actividad entre particulares bajo el derecho privado. Este artículo lo único que pretende es autorizar al Estado a la utilización de la firma digital. Sería ilógico excluir algún sector del uso de la firma, pues lo que la ley busca es un uso generalizado de la figura.

El capítulo III regula los certificados digitales. El artículo 15 establece los requisitos que debe cumplir un certificado, de la siguiente forma:

> *"Los certificados digitales se vinculan con una persona, confirmando su identidad, los cuales deberán contener al menos:*
>
> *1.- Los datos que identifiquen individualmente al firmante.*
>
> *2.- Las normas utilizadas para la creación de la firma.*
>
> *3.- Los datos que identifiquen a la entidad de certificación.*

4.- Numero de serie del certificado.

5.-Fecha de emisión y plazo de vigencia.

6.-Los demás que el reglamento establezca."

Este artículo es completo y brinda la seguridad necesaria para la utilización de la firma. Sin embargo, el inciso 2, agregado por los legisladores, puede llevar a confusión, ¿qué se entiende por normas? Puede entrabar innecesariamente la simple emisión de un certificado.

El artículo 17 explica en qué casos se puede revocar un certificado, en aras de la seguridad.

"Los certificados digitales se podrán suspender, cancelar y revocar según el caso, en las siguientes circunstancias:

1.-A solicitud del titular de la firma.

2.-Por expiración del plazo de vigencia del certificado.

3.-Por cese de operaciones de la entidad de certificación.

4.-Por muerte del titular de la Firma Digital.

5.-Por incumplimiento contractual con la entidad de certificación.

6.-Por orden del un juez.

7.-Las demás que el reglamento establezca."

El artículo 18 es de gran importancia. Otorga equivalencia a los certificados emitidos en lugares diferentes a Costa Rica. Es una previsión necesaria ya que Internet es global y la firma digital es una aplicación de él, por lo cual un certificado puede ser emitido en cualquier parte del mundo y ser reconocido aquí. El artículo indica que:

"Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por

prestadores establecidos y acreditados en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y reconocidos por la autoridad de acreditación competente y cumpliendo con los requisitos fijados en esta Ley, su reglamento y normas internacionales correspondientes."

Este capítulo esta completo y claro, brindando la seguridad necesaria para la utilización de la firma digital.

Los legisladores incorporaron el capítulo IV, titulado Deberes de las Partes Intervinientes.

El artículo 19 indica las obligaciones que debe cumplir el emisor al firmar digitalmente un documento:

"*Para crear una firma digital el firmante deberá:*

1.-Actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de firma;

2.-Sin dilación indebida, utilizar los medios que le propicien el prestador de servicios de certificación o esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma digital o prestar servicios que la apoyen si:

a) El firmante sabe que los datos de creación de la firma han quedado en entredicho; o

b) Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma haya quedado en entredicho;

3-.Actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado que refrende su firma o que hayan de consignarse en él, son exactas y completas.

Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los deberes anteriores."

El último párrafo de este artículo sienta un régimen de responsabilidad para el firmante. Es importante establecer cuáles son los deberes y pautas a seguir por el emisor del documento firmado digitalmente para que, en caso que se presente posteriormente algún problema, se pueda demostrar si se actuó con la diligencia necesaria.

El artículo 20 establece los deberes del prestador de servicios de certificación:

"(...)

1.-Actuar de conformidad con las declaraciones que hizo ante la Autoridad de Acreditación respecto de sus normas, políticas y prácticas;

2.-Actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del

certificado que emite o que estén consignadas en él, son exactas y completas;

3.-Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a esta determinar mediante el certificado:

a) La identidad del prestador de servicios de certificación.

b) Que el firmante nombrado en el certificado tenía bajos su control los datos de creación de la firma en el momento en que se expidió el certificado;

c) Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

4. Proporcionar a la parte que confía en el certificado, medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

a) El método utilizado para comprobar la identidad del firmante;

b) Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

c) Si los datos de creación de la firma son válidos y no están en entredicho;

d) Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

e) Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho; en caso afirmativo, el prestador de servicios de certificación debe efectivamente proporcionar ese medio al firmante para que dé aviso;

f) Si se ofrece un servicio para revocar oportunamente el certificado; en caso afirmativo, el prestador de servicios de certificación debe cerciorarse de que existe un servicio efectivo para revocar oportunamente el certificado.

5. Al prestar sus servicios, utilizar sistemas, procedimientos y recursos humanos fiables.
Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los deberes anteriores."

El legislador tiene toda razón de incorporar este artículo. Establece un régimen de responsabilidad para las autoridades de certificación. Esto brinda seguridad para la utilización de la firma digital y está acorde a la normativa internacional. Todos los deberes enumerados son necesarios, no entraban injustificadamente el uso de la firma digital y dan confianza al usuario.

El artículo 21 prescribe las siguientes responsabilidades del receptor del mensaje, es decir, quien verifica la firma:

"(...)

1-.Verificar la fiabilidad de la firma electrónica;

2.-Verificar la validez, suspensión o revocación del certificado;

3.-Tener en cuenta cualquier limitación explicita en el certificado."

Se establece igualmente la responsabilidad para la parte que confía, lo cual es también de suma importancia. Sin embargo, este artículo contiene un grave error: en el primer inciso se habla de firma electrónica, concepto que nunca se define en el proyecto. Esta ley no busca regular la firma electrónica, sino la digital, por lo cual debe ser modificado sin lugar a duda.

Estos artículos incluidos por el legislador que sientan la responsabilidad de las partes son basados en la Ley Modelo sobre Firmas Electrónicas de la UNCITRAL.

El artículo 22, como ya lo señalamos, debe incorporarse al capítulo de la autoridad de acreditación.

El capitulo V del proyecto establece las sanciones.

El párrafo primero del artículo 23 establece que:

> *"Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que, en el perjuicio de su actividad ocasionen por la certificación y homologación de certificados de firmas digitales. En todo caso corresponderá al prestador de servicios de certificación demostrar que actuó con la debida diligencia."*

Hay un error en la redacción del texto en cuanto dice "en el perjuicio de su actividad". Esto no tiene sentido, debe modificarse a "en el **ejercicio** de su actividad". Se establece un régimen de responsabilidad para las autoridades de

certificación, este artículo viene a reforzar el artículo 20, y hay que leerlo en relación con el 24.[86] Pero además establece la carga de la prueba, va a ser la autoridad de certificación quien deba demostrar que actuó con la debida diligencia.

El segundo párrafo del artículo citado indica:

> *"Sin perjuicio de lo anterior, los prestadores de servicios de certificación no serán responsables de los daños o perjuicios que tengan en su origen el uso indebido o fraudulento de un certificado de firma digital por parte del suscritor."*

Este párrafo delimita el régimen de responsabilidad de las autoridades de certificación. Sin embargo, la carga de la prueba para dichas autoridades en estos casos se mantiene.

El artículo 25 describe las sanciones que puede imponer la autoridad acreditante:

---

[86] **"ARTICULO 24.-** Para los efectos de la presente ley se consideraran infracciones por parte de los prestadores de servicios de certificación, el incumplimiento de cualquiera de las disposiciones contenidas en esta ley y la negligencia en la prestación de servicios."

"La Autoridad de Acreditación, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, según la naturaleza y gravedad de la falta, las siguientes sanciones a los prestatarios del servicio de certificación que incumplan o violen las normas contenidas en la presente ley:

Amonestación por escrito.

Multa de cinco hasta veinte salarios base, de acuerdo con el artículo 2 de la Ley 7333.

Suspensión inmediata de todas o algunas de las actividades de la entidad infractora.

Prohibición a la entidad infractora de prestar directa o indirectamente los servicios de entidad de certificación por el término de hasta 5 años.

Revocación definitiva de la acreditación y prohibición para operar en Costa Rica como entidad de certificación acreditada."

Este artículo busca mantener la calidad del servicio que brinda la autoridad de certificación en aras a la protección del usuario. Es necesario que los estándares exigidos en la ley se mantengan en todo momento para dar la seguridad y confianza necesaria.

El artículo 26 garantiza el derecho de defensa que tienen las personas al establecer que:

> "*Las resoluciones de la Autoridad de Acreditación podrán ser impugnadas por los interesados cuando consideren que han sido perjudicados en sus intereses legítimos o en sus derechos.*
>
> *Contra dichas resoluciones podrá ser interpuesto el recurso de reconsideración contra la propia Autoridad de Acreditación o apelación ante el Titular del Ministerio de Ciencia y Tecnología.*
>
> *La Autoridad de Acreditación contará con un plazo de dos meses para decidir sobre el recurso de reconsideración interpuesto. Si en tal plazo no ha*

sido resuelto el recurso, la decisión se considerará favorable al recurrente.

De la misma forma, el Ministerio de Ciencia y Tecnología dispondrá de dos meses para resolver el recurso de apelación. Si en tal plazo este recurso no ha sido resuelto la decisión se considerará favorable al recurrente."

Se indican los lineamientos a seguir en caso que una resolución de la Autoridad de Acreditación sea impugnada.

IV. RECOMENDACIONES AL PROYECTO DE LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES, No 14.276

A lo largo del estudio de este tema, se denota que el concepto de firma digital no es de entendimiento general. Así lo expresa el diputado Belisario Solano Solano, coordinador de la Comisión Especial nombrada para que estudie, analice y dictamine la legislación que sobre Propiedad Intelectual requiere nuestro país para enfrentar los desafíos y compromisos internacionales asumidos a la fecha. En el acta

de la Comisión Técnica número 12, del martes 5 de marzo del 2002, después de la exposición del Master Edwin Aguilar Sánchez, especialista en el tema, el diputado Solano manifestó:

> *"Creo que nos hace falta mucho más tiempo, (…) hasta este momento yo he recibido una clase de chino, pero le prometo que voy a estudiar con detalle, máxime que yo soy el que tengo que ponerla cara ante la prensa para explicar ese tema en "cristiano" porque ese es el problema."*

Asimismo, en las respuestas a las consultas efectuadas por el diputado Solano a las diferentes instituciones del país, éstas recomiendan que se defina en el proyecto cómo es que funciona la firma digital y los sistemas de encriptación. Esto no es posible porque, en primer lugar atentaría contra del principio de neutralidad tecnológica y, en segundo lugar, una ley se emite con el fin de regular, no es un manual de instrucciones.

Si bien es cierto que es un tema complejo, este proyecto de ley de una manera muy simple, logra regular el tema de la

firma digital. Se apega al principio de neutralidad tecnológica establecido en la Ley Modelo de la UNCITRAL sobre Firmas Electrónicas, permitiendo que la ley fluya con los cambios del mundo informático y tecnológico. Asimismo, las normas de este proyecto son compatibles a nivel internacional. Es un excelente esfuerzo por parte del Poder Ejecutivo y Legislativo.

Sin embargo, hay cuestiones que hay que modificar. A continuación, señalaremos nuestras recomendaciones:

- En primer lugar, es necesario eliminar la distinción que se hace en el artículo 2, incisos 6 y 7, entre documento electrónico y documento digital, ya que no aporta nada al proyecto y, más bien, se puede prestar para confusiones. Hay que incorporar aquí la definición de documento que indicaba el primer proyecto presentado por el Poder Ejecutivo. A saber:

> "*Documento: Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra*

naturaleza, y que se puede recuperar o reproducir en una forma perceptible o inteligible."

- Es necesario dejar claro que la acreditación de las entidades de certificación es **voluntaria**. Como estudiamos anteriormente, esta ley busca regular un fenómeno que se da en el ámbito del derecho privado, regido por el principio de la autonomía de la voluntad. Se debe permitir que las partes contraten los servicios de certificación con quien deseen, sea entidades públicas o privadas, acreditadas o no acreditadas.

Por un lado, el proyecto en el artículo 2 define la "acreditación voluntaria del prestador de servicios de certificación", estableciendo que la acreditación será "a petición del interesado". Pero, por otro lado, el primer párrafo del artículo 12 puede prestarse a confusión, ya que indica que:

"(...) *las empresas que emitan certificados de firma digital deberán someterse al proceso de acreditación* (...)".

Hay que reformar la redacción de este artículo para que esté acorde a la esencia del proyecto y a las disposiciones de las leyes modelo de la UNCITRAL y la Unión Europea. Proponemos la siguiente redacción:

> "Mediante la Autoridad de Acreditación, las empresas que emitan certificados de firma digital, podrán someterse, si así lo desean, al proceso de acreditación que se defina en esta ley y su reglamento."

- El artículo 22 de la ley en estudio menciona los requisitos que deben cumplir las entidades de certificación para su acreditación. Expresa lo siguiente:

> "*Para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:*
>
> "*a) Los recursos humanos y financieros, incluida la existencia de un activo;*

b) La calidad de los sistemas de equipo y programas informáticos;

c) Los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) La disponibilidad de información para los firmantes nombrados en el Certificado y para las partes que confíen en éste;

e) La periodicidad y alcance de la auditoría por un órgano independiente

f) (…)

g) *Cualesquiera otros factores pertinentes."*

Este artículo debe incorporarse al capítulo de la autoridad de acreditación. Sin embargo, proponemos que este artículo se

elimine y, en su lugar, se incorpore el siguiente texto, basado en la ley chilena:

"Para ser acreditado, el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:

a) Demostrar la fiabilidad necesaria de sus servicios;
b) Garantizar la existencia de un servicios seguro de consulta del registro de certificados emitidos;
c) Emplear un personal calificado para la prestación de servicios ofrecidos, en el ámbito de la firma digital y los procedimientos de seguridad y gestión adecuados;
d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;
e) Haber contratado un seguro apropiado en los términos que señala el artículo 20; y
f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación."

A diferencia del artículo propuesto en el proyecto de ley, este artículo deja claro cuáles son los requisitos necesarios para que una entidad de certificación quede acreditada ante el Órgano Rector, y son requisitos que están acordes con las necesidades internacionales y estándares tecnológicos. Este artículo contempla la necesidad de las autoridades de certificación de contratar un seguro, figura sumamente interesante ya que todos los sistemas operativos pueden fallar. La ley delimita el ámbito de responsabilidad de las autoridades de certificación y del firmante, pero no queda claro qué ocurre en caso de fuerza mayor o caso fortuito, para lo cual habría que remitirse a las normas del Código Civil. De esta manera recomendamos incorporar como requisito, la necesidad de contratar un seguro en caso de fuerza mayor o caso fortuito. Este seguro no debería ser muy costoso ya que si se cumple con los estándares internacionales de tecnología, los riesgos que ocurra alguna falla son mínimos, lo cual no afecta la rentabilidad de prestar el servicio de certificación de forma acreditada. Todo esto en aras a la protección del usuario.

- El artículo 5[87] del proyecto debe modificarse. Pretende autorizar a los funcionarios públicos a utilizar su firma digital para los casos en que la ley así lo exija. Es necesario especificar quiénes son las "personas autorizadas" ya que queda muy amplio y puede prestarse a confusión. Se propone la siguiente redacción:

> "En caso que se requiera una certificación o documento firmado por un funcionario publico, éste podrá hacerlo mediante la utilización de su firma digital acreditada."

- El proyecto de ley le otorga a la firma digital acreditada el mismo valor que la firma manuscrita. Igualmente, define qué se entiende por firma digital "simple" pero no establece sus consecuencias. El documento firmado digitalmente por una firma acreditada tendrá pleno valor probatorio, pero qué sucede con la firma digital que no ha sido acreditada? Sugerimos que se incorpore al proyecto una

---

[87] "Cuando una Ley requiera que un documento o firma esté certificado o de cualquier otra forma reconocida, verificado tal requisito se tendrá por cumplido si una firma digital acreditada de un funcionario publico, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma Digital Acreditada."

norma similar al artículo 5, inciso 2 de la Directiva 1999/93 de la Unión Europea, de la siguiente manera:

> *"No se le negará eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma digital por el mero hecho de que:*
>
> *a) ésta se presente en forma electrónica, o*
>
> *b) no se base en un certificado reconocido, o*
>
> *c) no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o*
>
> d) *no esté creada por un dispositivo seguro de creación de firma."*

- Es necesario eliminar el término de "firma electrónica" y sustituirlo por el de "firma digital" en el artículo 21 de la ley. Como lo indica el título del proyecto: Ley de Firma Digital y Certificados Digitales, lo que se regula es la firma digital y no la firma electrónica, término que no se contempla en el texto de ley.

- Hay ámbitos donde la firma digital todavía no tiene cabida. Hay actos personalísimos que excluyen el uso de dicha firma. Por esta razón, es necesario que se excluyan de la ley ciertos campos. Sugerimos la redacción de este artículo de conformidad con el artículo 4 de la Ley de Argentina:

> "*Exclusiones. Las disposiciones de esta ley no son aplicables:*
>
> *a) a las disposiciones por causa de muerte;*
>
> *b) a los actos jurídicos del derecho de familia;*
>
> *c) a los actos personalísimos en general;*
>
> *d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.*"

- Esta ley es omisa en indicar cómo debe interpretarse sus normas. Por lo cual se propone incorporar el siguiente artículo, basado en la ley chilena:

"Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel. Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.

- Se ha criticado esta ley por no contener normas que otorguen protección al consumidor. Al respecto, Pérez Merayo dice:

"*Otro problema general del proyecto que podría originar una potencial acción de inconstitucional, lo anterior debido a que en todo su contexto no se hace referencia de manera explícita o implícita a la protección al consumidor, ni estipula excepción alguna en la protección o hace apelativo a norma superior o de igual rango que proteja los intereses de los consumidores.*

(...)

Es necesario que en la ley resultante se proteja de manera explícita este interés, lo anterior con el fin de que los esquemas típicos de desigualdad del mundo físico no trasciendan al mundo virtual."

No es necesario incorporar una norma que haga mención a la protección del consumidor. En Costa Rica ya tenemos una ley de Protección al Consumidor, debemos recordar que el derecho es un sistema donde todas las normas están relacionadas, aunque no se estipule expresamente la protección al consumidor en la ley de firma digital, no implica que el consumidor no tenga protección en este sentido, además que la firma digital es simplemente un producto más por lo cual quedaría cubierto bajo la mencionada ley.

El proyecto de Ley de Firma Digital y Certificados Digitales es un excelente esfuerzo en conjunto del Poder Ejecutivo y Poder Legislativo. Cumple plenamente con el principio de neutralidad tecnológica y de compatibilidad internacional, recomendados por las Leyes Modelos de la UNCITRAL y la Unión

Europea. El proyecto expresa las garantías mínimas que debe otorgar la firma digital, a saber: autoría, integridad y no repudio en origen y destino. Además, está en concordancia con las disposiciones constitucionales y legales. En efecto, ya en muchos casos están previstas situaciones en el ordenamiento jurídico, en las que se podría o incluso debería usar la firma digital que, por razones prácticas, estos mecanismos deben ser establecidos como facultativos. Es necesario que el Estado paulatinamente vaya tomando los pasos necesarios para generalizar estas prácticas.

A parte de las reformas sugeridas, no hay impedimento alguno para que esta ley sea aprobada lo antes posible. La firma digital es una realidad, es usada con regularidad, y es necesario brindarle protección jurídica. La laguna jurídica existente por la falta de regulación sobre este tema, es un factor que obstaculiza el progreso del país en este ámbito.

CONCLUSIONES

Es necesario, para el pleno desarrollo del comercio electrónico, dotarlo de un entorno jurídico, es decir, emitir una normativa que sea el soporte de las transacciones, e introducir el concepto de seguridad jurídica en la era digital, así como darle el empleo adecuado.

La eficacia de las leyes que regulen esta materia, radica en su uniformidad y armonización, puesto que su contenido difiere en cada país, donde su aplicación puede resultar compleja dado el uso globalizado de la red Internet.

Si bien es cierto que actualmente la firma digital es el único medio tecnológico que permite, brindando toda seguridad, usar los medios de comunicación para el intercambio de información, es conveniente que las legislaciones sean diseñadas de una forma flexible ya que, como hemos sido testigos en los últimos años, el mundo tecnológico cambia día a día.

La firma digital le da seguridad a las transacciones electrónicas. Esta firma es una herramienta tecnológica, basada en sistemas complejos de encriptación, que otorgan plena seguridad al intercambio de datos en Internet y en los sistemas de comunicación. Si bien es cierto que la firma digital no se puede definir con base en una tecnología en específico, actualmente la tecnología imperante en este campo y que otorga la mayor seguridad es la tecnología de encriptación, basada en una infraestructura de clave pública y clave privada.

A pesar del carácter técnico de la firma digital, su óptima aplicación se da cuando cuenta con el reconocimiento del ordenamiento jurídico. Para que esto se dé, es necesaria la intervención de terceras partes, como las autoridades de certificación que emiten certificados digitales y comprueban que el firmante es quién dice ser.

La confianza digital surge, por lo tanto, del reconocimiento legal de ciertas tecnologías de la información y las comunicaciones empleadas en las relaciones telemáticas, entre particulares, entre particulares y empresas, entre empresas

entre sí, o entre cualquiera de los anteriores y la Administración.

A pesar que las autoridades de certificación pueden ser públicas o privadas, y en cualquier caso cuentan con el mismo reconocimiento, los Estados han implementado sistemas de acreditación voluntaria, a través de entes estatales acreditantes. La acreditación se vuelve importante para el reconocimiento de la firma digital, ya que la firma digital avanzada, asegurada por una entidad de certificación acreditada, es la que cuenta con todos los efectos jurídicos que el ordenamiento establece.

Por medio de la firma digital se logran las garantías necesarias para equiparar la firma digital con la manuscrita. Se logra asegurar la identidad del firmante, en otras palabras, se puede comprobar que quien firma un mensaje de datos digitalmente es quién dice ser. Adicionalmente, se garantiza la integridad del mensaje, es decir, que éste no ha sido alterado con posterioridad a la firma. Además, se logra el no repudio en origen y destino de la información transmitida, esto ofrece la seguridad inquebrantable de que

el autor del documento no pueda retractarse en el futuro de las opiniones o acciones consignadas en dicho mensaje, ni de haberlo enviado. La firma digital otorga más garantías, como la imposibilidad de suplantación por otro individuo, la auditabilidad, según la cual se pueden identificar y rastrear las operaciones llevadas a cabo por el usuario, dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados, especialmente, cuando se incorpora el sellado de tiempo, que añada de forma totalmente fiable la fecha y hora a las acciones realizadas por el usuario. Igualmente, se garantiza la confidencialidad de la información intercambiada entre las partes, esté firmada o no.

Estas garantías permiten el desarrollo del principio de equivalencia funcional, que comprueba nuestra hipótesis. Sin lugar a dudas, la firma digital tiene el mismo valor jurídico que la firma manuscrita. El reconocimiento jurídico de la firma digital no crea ninguna nueva figura en el derecho, es una mera equiparación que conlleva las mismas consecuencias jurídicas de la firma manuscrita. Esta afirmación tiene importantes consecuencias para el reconocimiento del

documento electrónico como un documento en términos jurídicos asegurándole, además, plenos efectos probatorios.

El derecho comparado ha respondido a las necesidades de la sociedad de la información dando una adecuada regulación a la firma digital. En efecto, todos los países estudiados cuentan con legislación pertinente sobre este dispositivo, recogiendo varias similitudes en sus normas. La armonía y uniformidad de las normas sobre firma digital es tan importante que ha sido una de las preocupaciones centrales de las organizaciones internacionales como la UNCITRAL y la Unión Europea.

En Costa Rica todavía no se ha aprobado tan importante instrumento. El Proyecto de Ley de Firma Digital y Certificados Digitales es un proyecto que está en concordancia con los principios contenidos en las leyes modelo y guarda uniformidad con las demás normas sobre la materia. Constituye un importante esfuerzo del Poder Ejecutivo y el Legislativo por dotar a Costa Rica de una adecuada regulación de este tema. Asimismo, el proyecto está en armonía con el resto del ordenamiento costarricense, y no existen impedimentos legales para que sea aprobado a la

brevedad posible. Sobre todo porque constituye una necesidad para el país, es un deber del gobierno no dejar pasar la oportunidad de regular adecuadamente una actividad que ya se está dando a nivel mundial. La nueva economía se basa en gran medida en Internet, y la pronta aprobación de un proyecto de ley como el estudiado, pondría al país a la vanguardia en materia de regulación tecnológica, a la altura de los países más desarrollados.

BIBLIOGRAFÍA

LIBROS, REVISTAS Y TÉSIS

- AGÜERO GUIER, Esteban y ECHERVERRIA HINE, Leonor. **Comercio Electrónico: El Contrato de Intercambio Electrónico de Datos (EDI). Estudio de Derecho Comparado.** Trabajo final de graduación para optar el grado de licenciado en Derecho. Facultad de Derecho de la Universidad de Costa Rica, San José, Costa Rica, 2002.
- ANDERSON, John C. y CLOSEN, Michael L. **Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority.** The John Marshall Jorunal of Computer & Information Law. Estados Unidos de América. 1999.
- BAKER, Stewart A. **International Developments Affecting Digital Signatures.** Estados Unidos de América: Westlaw, 1998.
- BIDDLE, C. Bradford. **Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in Public**

Key Infrastructure. San Diego Law Review, California, 1996.

- BORDA, Alejandro. **La Teoría de los Actos Propios.** Segunda Edición. Buenos Aires, Argentina: Abeledo-Perot A.E, 1993.
- BRENES CÓRDOBA, Alberto. **Tratado de los Contratos.** Quinta Edición. San José, Costa Rica: Juritexto, 1998.
- BRISEÑO, Jolene Marie y ROLDÁN SAUMA, Marcelo. **La Protección del Consumidor en el Comercio Electrónico.** Primera Edición, San José, Costa Rica: IJSA. 2001.
- CABANELLAS, Guillermo. **Diccionario de Derecho Usual.** Tomo II. Buenos Aires: Ediciones ARAYÚ, 1953.
- CERTAD MAROTO, Gastón. **Temas de Derecho Comercial.** Segunda Edición. San José, Costa Rica: Juritexto, 1998.
- COUTURE, Eduardo J. **Vocabulario Jurídico**. Facultad de Derecho y Ciencias Sociales. Montevideo, 1950.
- DE TÉRAMOND PERALTA, Guy y RETANA, Álvaro. **Establecimiento de la Red Internet Avanzada y Creación de la Red Nacional de Investigación Avanzada.** Dictada en el Seminario Costa Rica en el Mundo Digital. Fotografía e Imprenta LIL, S.A., San José, Costa Rica, 2001.

- DE TÉRAMOND PERALTA, Guy y PARDO EVANS, Rogelio. La **Nueva Sociedad del Conocimiento**. San José, Costa Rica: Ministerio de Ciencia y Tecnología (2000-2006), 2002.
- DELPIAZZO, Carlos E. **Relevancia Jurídica en la Encriptación y la Firma Electrónica en el Comercio Actual**. Documento sin fecha. Documento sin numeración.
- Diccionario de la Lengua Española. Real Academia Española. Vigésima Primera Edición. Tomo I. Madrid, España: Editorial Espasa Clape, S.A., 2000.
- FARRER PEÑA, Mónica y GASPAR ESQUIVEL, Natalia. **La Adopción de Mecanismos de Seguridad como Prevención a los Conflictos Generados en los Contratos por Medios Electrónicos**. Tesis para optar por el grado de Licenciatura en Derecho. Universidad Escuela Libre de Derecho. San José, Costa Rica, 2001.
- HERNANDEZ, Edgar y GÁMEZ, Marco Vinicio. **Seguridad de la Información en la Era de los Negocios Sociales**. San José, Costa Rica: Rho-Sigma, S.A., 2001.
- JOVEL SÁNCHEZ, Carlos Alberto. **El Documento Electrónico y la Firma Digital al servicio de la Administración de Justicia**. Octubre de 2001

- KALAMA M., Liu-Kwan. **Recent Developments in Digital Signature Legislation and Electronic Commerce.** Berkeley Technology Law Journal. California, 1999.
- KNORR BRICEÑO, Jolene Marie y ROLDÁN SAUMA, Marcelo. **La protección del consumidor en el comercio electrónico.** Primera Edición. San José, Costa Rica: Editorial Investigaciones Jurídicas, SA, 2001.
- KOSSICK, Robert. **Critical Essay: The Internet in Latin America: New Opportunities, Developments, & Challenges.** American University International Law Review. Washington, 2001.
- KOZOLCHYK, Boris y TORREALBA, Octavio. **Curso de Derecho Mercantil**. Segunda Edición. San José, Costa Rica: Juritexto, 1997.
- KPMG Abogados. **E-Commerce in Costa Rica.** San José, Costa Rica: KPMG Abogados, 2001.
- LEAHY, Patrick J. **New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law.** Harvard Journal of Law and Technology, Harvard Law School. Spring, 1992
- LEAL TUPPER, Stephen. **From Seal to Cyber Notary: Uncertainty in Electronic Commerce and the Case for**

Digital Signature Law in Michigan. The Wayne Law Review. Estados Unidos de América. 1999.

- MARTINEZ NADAL, Apolónia. **Comercio Electrónico, Firma Digital y Autoridades de Certificación.** Segunda Edición. Madrid, España: Civitas Ediciones S.L. 2000.
- MÉNDEZ, Tiffany A. **Adopting the Digital Signature Guidelines in Implementing Public Key Infrastructure for Federal Procurement of Electronic Commerce.** Public Contract Law Journal. Estados Unidos de América: Westlaw, 2000.
- MILLSTEIN, Julian S., NEUBURGER, Jeffrey D., y WEINGART, Jeffrey P. **Encryption and Digital Signatures.** Estados Unidos de América: Westlaw. Sin fecha.
- MORA, Fernando. **Introducción al Estudio del Derecho Comercial.** Segunda Edición. San José, Costa Rica: Juritexto, 1991.
- Multimedia Strategist. **Digital Signatures: Legal Issues and ABA Guidelines.** Nueva York: Leader Publications, a division of the New York Law, 1995.
- PARMENTIER, Miriam A. **Directive 1999/93 on Community Framework for Electronic Signatures.** Columbia Journal of European Law. Columbia, 2000.

- PASCALE, Maricarmen. **Firma Digital**. Uruguay. Documento sin fecha. Documento sin numeración.
- PÉREZ VARGAS, Víctor. **Derecho Privado**. Tercera Edición. San José, Costa Rica: Litografía e Imprenta LIL, S.A. 1994.
- RAMOS UGARTE, Fresia María. **Consideraciones Teórico-Prácticas acerca del Precontrato de Compraventa en Costa Rica**. Trabajo final de graduación para optar al grado académico de Licenciada en Derecho. Escuela de Derecho de la Universidad Central Costarricense. San José, Costa Rica, 2002.
- RICHARDS, R. Jason. **The Utah Digital Signature Act as "Model" Legislation: a Critical Analysis**. The john Marshall Journal of Computer & Information Law. Alabama, 1999.
- RITTER, Jeffrey B. y GLINIECKI, Judith Y. **The Need form Harmonized Notional Reforms**. Harvard Journal of Law & Technology. Boston, 1993.
- SARRA, Andrea Viviana. **Comercio Electrónico y Derecho**. Primera Edición. Buenos Aires, Argentina: Editorial Astrea. 2000.

- SINGER, Anthony Martin. Digital **Signatures and the Role of the Kansas Digital Signature Act.** Washburn Law Journal. Estados Unidos de América, 1998.
- SMEDINGHOFF, Thomas J. Electronic Contracts & Digital Signatures: **Digital Signatures. The Key to Secure Internet Commerce.** Westlaw. Estados Unidos de América. 1998.
- SMEDINGHOFF, Thomas J. Electronic Contracts & Digital Signatures: **An Overview of Law and Legislation.** Westlaw. Estados Unidos de América. 1999.
- STERN, Jonathan E. **The Electronic Signatures in Global and National Commerce Act.** Berkeley Technology Law Journal. California, 2001.
- The New Enciclopædia Britannica. Volumen 18. Edición número 15. Chicago: Enciclopædia Británica, Inc. 1974.
- THOMAS, Sanu K. **The Protection and Promotion of E-Commerce: Should there be a Global Regulatory Scheme for Digital Signatures?** Fordham University School of Law. Estados Unidos de América, 1999.
- WHITE SCOVILLE, Adam. **Clear Signatures, Obscure Signs.** Cardozo Arts & Entertainment Law Journal. Boston, 1999.

SITIOS EN INTERNET

- ALAMILLO DOMINGO, Ignacio. **Confianza Digital Basada en Certificados** en Revista Electrónica de Derecho Informático. Número 13. España, 1999. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/No._13_-_Agosto_de_1999/confianza
- ALVA MATTEUCCI, Juan Mario. **La Firma Digital y su Aplicación en la Administración Tributaria Peruana** en Revista Electrónica de Derecho Informático. Perú. 2000, Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107712
- ÁLVAREZ MARAÑÓN, Gonzalo. **Los Secretos de la Firma Electrónica**. España. 2000. Documento sin numeración, disponible en: http://www.idg.es/iworld/articulo.asp?id=106760&n=25&sec=iworld
- Anónimo. **Correo Seguro**. España. Documento sin fecha. Documento sin numeración, disponible en: http://www.iec.csic.es/criptonomicon/correo/firma.html

- Anónimo. **Einführung zum Thema "Digitale Signatur".** Sin fecha, documento sin numeración, disponible en http://www.digital-law.net/knupfer/intor.htm
- Anónimo. **España, a la vanguardia de las firmas electrónicas.** Sin fecha, documento sin numeración, disponible en: http://www.iec.csic.es/criptonomicon/susurros/susurros10.html
- Anónimo. **Introducción a la Criptografía. El Rincón de Quevedo.** Sin fecha, documento sin numeración, disponible en http://rinconquevedo.iespana.es/Criptografia/criptografia.htm
- Anónimo. **La Signature Électronique.** Sin fecha, documento sin numeración, disponible en http://www.senat.fr/lc/lc67/lc67_mono.html
- Anónimo. **Marco Jurídico para la firma digital en España.** Sin fecha, documento sin numeración, disponible en: www.zetapoplus.com/rep_documentos/Informes/Informe_Firma_Digital34.PDF

- Anónimo. **Primer sistema de votación on-line en Alemania.** Sin fecha, documento sin numeración, disponible en: file://E:\FIRMA DIGITAL\votacion on line en Alemania.htm
- Anónimo. **A Short History of Cryptography.** Sin fecha. Documento sin numeración, disponible en: http://all.net/books/ip/Chap2-1.html
- Anónimo. **Temas de derecho: El documento electrónico, sistema de autenticación y la firma digital.** Sin fecha, documento sin numeración, disponible en: http://www.it.cenit.org.ar/Seminarios/DerEconDIG2000/material/EDoc/EDoc.htm
- ARCE, Alfonso José y DÍAZ LANNES, Federico Santiago. **La Firma Digital. Aspectos Jurídicos. Su Aplicación a las Comunicaciones previstas por la Ley 22.172** en Revista Electrónica de Derecho Informático. Número 16. Sin fecha. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107423
- Asociación de Usuarios de Internet. **Preguntas más Frecuentes.** Mesena, Madrid. Documento sin fecha. Documento sin numeración, disponible en:

http://www.aui.es/biblio/documentos/consejos_seguridad/faqs-seguridad.htm

- CAMPOLL, Gabriel Andrés. **Argentina: Firma Ológrafa y Firma No Ológrafa.** Documento sin fecha ni numeración. Disponible en: http://www.alfa-redi.org/revista/data/46-11.asp
- CERF, Vint. **Computer Networking: Global Infrastructure for the 21st Century.** Estados Unidos de América. 1995. Documento sin numeración, disponible en: http://www.es.washington.edu/homes/lazowska/cra/networks.html
- COMISIÓN REDACTORA DEL ANTEPROYECTO DE LEY DE FIRMA DIGITAL (ARGENTINA). **Informe de la Comisión Redactora.** Documento sin fecha ni numeración. Disponible en http://www.pki.gov.ar/PKIdocs/Informe.html
- CORNEJO LOPEZ, Valentino. **Una Realidad Mexicana, La Firma Electrónica y la Participación del Notario Mexicano** en Revista Electrónica de Derecho Informático. Documento sin fecha. Documento sin numeración, disponible en: http://vz.vlex.com/global/redi/detalle_doctrina_redi.asp?atriculo=107899

- DEVOTO, Mauricio y LYNCH M. Horacio. **Banca, Comercio, Moneda Electrónica y La Firma Digital** en Revista Electrónica de Derecho Informático. 1998. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/No._02_-Septiembre_de_1998/devoto
- DOPHEIDE, Jan Hendrick. **La Signature Électronique en France et en Allemagne: quelles perspectives?.** Sin fecha. Documento sin numeración, disponible en: http://www.le-juriste.com/edit/al005.htm
- ESCOBAR ROZAS, Freddy. **La Firma Electrónica en la Ley Peruana** en Revista Electrónica de Derecho Informático. No 33. Perú. Sin fecha, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107888
- GARCÍA DE LAS HERAS, Diego. **España: La Persona Jurídica como Signatario de una Firma Electrónica** en Revista Electrónica de Derecho Informático. Número 45. Sin fecha, documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=146287

- GONZÁLEZ OGAZ, Cristóbal. **Aspectos sobre el Proyecto Chileno de Ley sobre Firma Electrónica y Servicios de Certificación de Firma Electrónica** en Revista Electrónica de Derecho Informático. No. 35, Chile. Sin fecha, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?aticulo=107969
- GUADIÁN ORTA, Carlos. **España: Experiencias y proyectos de voto electrónico** en Revista Electrónica de Derecho Informático. Número 45. Sin fecha, documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=146313
- Instituto de Firmas Digitales.com. **Preguntas más comunes**. Documento sin fecha. Documento sin numeración, disponible en: http://www.digitalsignatures.org/html/preguntas_mas_comunes.html.
- JIJENA LEIVA, Renato. **Firma Digital y Entidades Certificadoras. Regulación Legal en la Administración Pública Chilena** en Revista Electrónica de Derecho Informático. Chile. Documento sin fecha, disponible en

http://v2.vlex.com/global/redi/detalle_doctirna_redi.asp?articulo=10789

- JIJENA LEIVA, Renato. **Impuestos, Firmas y Certificados Digitales** en Revista Electrónica de Derecho Informático. Chile, 2001. Número 8, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107924
- LAMBERT, Ariel. **Argentina: La Ley No. 25.506 de Firma Digital** en Revista Electrónica de Derecho Informático. Número 45. Sin fecha, documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=146283
- LOBERA P., Myriam. **La Firma Digital, es Confiable**? 2000. Documento sin numeración, disponible en: http://www.solucionestributarias.com/articulos/firma%20digital.htm
- MAESTRE, Javier A. y SÁNCHEZ ALMEIDA, Carlos. **Análisis de la Directiva sobre Comercio Electrónico (Servicios de la Sociedad de la Información)** Documento actualizado a 17-05-01. Documento sin numeración, disponible en: http://comunidad.derecho.org/redi/lssi.txt

- MAESTRE A., Javier. España: **El Empleo de la Firma Electrónica en el Sistema Registral Español: Comentario a la Resolución de la Dirección General de los Registros y del Notariado, de 26 de abril de 2000** en Revista Electrónica de Derecho Informático. Número 24. España, 2000. documento sin numeración, disponible en http://publicaciones.derecho.org/redi/No._24_-_Julio_del_2000/14
- MAGLIONA MARKOVICHT, Claudio Paul. **Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico** en Revista Electrónica de Derecho Informático. Número 4. 2001, disponible en http://derecho.org/redi/
- MÁRQUEZ GONZÁLEZ, José Antonio. **México: Las preguntas más comunes en la contratación electrónica** en Revista Electrónica de Derecho Informático. Número 43. Sin fecha, documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=130326
- MARTÍN REYES, María de los Ángeles. **El Documento Electrónico y la Firma Electrónica.** Nuevas Perspectivas en la Contratación en Revista Electrónica de Derecho

Informático. España. Sin fecha. Número 14. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107395

- MARTÍN REYES, María de los Ángeles. **Las Entidades de Certificación** en Revista Electrónica de Derecho Informático. Número 35. Sin fecha, documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107936
- MATAMOROS, Sonia, MARTÍNEZ, Jesús y MAÑA, Antonio. **Entorno de Firma Confiable basado en PDA**. Universidad de Málaga. España. Sin fecha. Documento sin numeración, disponible en: http://www.criptored.upm.es/guiateoria/gt-m034a.htm
- MORENO, Luciano. **Criptografía**. España. Documento sin fecha. Documento sin numeración, disponible en: http://www.terra.es/personal6/morenocerro2/seguridad/cripto/cripto_5.html
- MUÑOZ ESQUIVEL, Oliver. Actividad de las Entidades de Certificación frente la Función Notarial en Revista Electrónica de Derecho Informático. Número 35. Sin

fecha. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107945

- Noticias Vlex. España. **La Agencia Tributaria presenta el Nuevo procedimiento de subastas por la Red.** España, 2002, Documento sin numeración, disponible en: http://v2.vlex.com/es/asp/noticias_detalle.asp?articulo=157784
- PATRONI VIZQUERRA, Úrsula. **Perú: Pago electrónico, privacidad y seguridad en el pago** en Revista Electrónica de Derecho Informático. Número 47. Sin fecha, documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=157695
- PÉREZ MERAYO, Guillermo Augusto. **Comentario acerca de las deficiencias que presenta el Proyecto de Ley sobre la Firma Digital.** En Revista Electrónica, Instituto de Investigaciones Jurídicas de la Facultad de Derecho de la Universidad de Costa Rica, No. 1, junio 2001 documento disponible en http//:www.iij.derecho.ucr.ac.cr/revista/rev1/firmadigital/index3.htm

- PÉREZ PEREIRA, María. **Apuntes al anteproyecto de Ley sobre Firma Electrónica** en Revista Electrónica de Derecho Informático. Número 14. España, 1999. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/No._14_-_Septiembre_de_1999/1
- PÉREZ PEREIRA, María. **La Situación de los Proveedores de Servicios de Certificación en el Real Decreto-Ley 14/1999, Sobre Firma Electrónica** en Revista Electrónica de Derecho Informático. Número 17. España, 1999. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina?redi.asp?articulo=107445
- PÉREZ PEREIRA, María. **España: Establecimiento y Ley Aplicable al Prestador de Servicios de Certificación en España** en Revista Electrónica de Derecho Informático. Número 26. España, 2000. Documento sin numeración, disponible en: http://publicaciones.derecho.org/redi/No._26_-_Septiembre_de_2000/11
- Periódico El País. **Sun lanza su propia firma digital, para competir con Passport de Microsoft.** Documento sin

autor, sin fecha y sin numeración. Disponible en: www.el-mundo.es/navegante/2001/09/27/esociedad/1001576103.htm

- RAMOS SUAREZ, Fernando. **La Firma Digital: Aspectos Técnicos y Legales.** 2000. Documento sin numeración, disponible en http;//www.marketingycomercio/numero14/00abr_firmadigital.htm
- RAMOS SUÁREZ, Fernando. **La Firma Digital** en Revista Electrónica de Derecho Informático. España. Sin fecha. Número 9. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107123
- RAMOS SUÁREZ, Fernando. **Como aplicar la nueva normativa sobre Firma Electrónica** en Revista Electrónica de Derecho Informático. España. 2000. Documento sin numeración, disponible en http://publicaciones.Derecho.org/redi/No._19_-_Febrero_del_2000/1
- RIBAS, Xavier. **Propuesta de Directiva sobre Firmas Electrónicas** en Revista Electrónica de Derecho Informático. Número 2. Sin fecha. Documento sin numeración, disponible en:

http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106968

- SÁNCHEZ ALMEIDA, Carlos. **España: La Criptografía como Derecho** en Revista Electrónica de Derecho Informático. Número 23. Sin fecha. Documento sin numeración, disponible en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107545
- SANDOVAL LOPEZ, Ricardo. **Chile: Comentario sobre el Proyecto de Ley relativa a documento y firma electrónicos** en Revista Electrónica de Derecho Informático Chile. Sin fecha. Documentos sin numeración, disponible en: http://publicaciones.derecho.org/redi/No_24_-_Julio_del_2000/11
- SILVA BOGGIANO, Macarena. **Chile: El Comercio Electrónico: La Firma Electrónica** en Revista Electrónica de Derecho Informático. Número 40. Universidad Católica de Valparaíso. Sin fecha. Documento sin numeración, disponible en: http:v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=115622

- Société de l'Information. **La Signature Électronique. Francia**. Sin fecha. Documento sin numeración, disponible en:
http://internet.gouv.fr/francais/textesref/signnum.htm
- Yupi Internet Inc. **Primer Sistema de votación on-line en Alemania**. 2001, Documento sin numeración, disponible en://E:\FIRMA DIGITAL/votación online en Alemania.htm

LEYES, REGLAMENTOS, DECRETOS Y DICTAMENES

- Ley de Sistema Nacional de Calidad, número 8279.
- Ley Modelo de la UNCITRAL sobre Arbitraje Comercial Internacional.
- Ley Modelo de la CNUDMI sobre Comercio Electrónico.
- Dictamen número C-283-98 de la Procuraduría General de la República. San José, Costa Rica, 1998.
- Electronic Signatures in Global and National Commerce Act. Estados Unidos de América, 2000.
- Ley de Firmas y Certificados Digitales. Número 27269. Perú, 2000
- Proyecto de Ley de Comunicaciones y Comercio Electrónico. El Salvador.

- Ley 527 de 1999, por medio de la cual se define y reglamenta el Acceso y Uso de los Mensajes de Datos, del Comercio Electrónico y de las Firmas Digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Colombia, 1999.
- Ley sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma.
- Ley número 25.506. Ley de Firma Digital. Argentina, 2001.
- Proyecto de Ley de Firma Digital y Certificados Digitales. Número 14.276. Costa Rica, 2001.
- Código Civil. Cuarta Edición. San José, Costa Rica: IJSA, 1997.
- Código de Comercio. Onceava Edición. San José, Costa Rica: IJSA, 1999.
- Código Procesal Civil. Séptima Edición. San José, Costa Rica: Editorial Porvenir, S.A., 1997.
- Código Procesal Penal. Segunda Edición. San José, Costa Rica: Editorial Porvenir, S.A., 1998.
- Constitución Política de la República de Costa Rica. Octava Edición. San José, Costa Rica: Investigaciones Jurídicas, S.A., 1997.

- Ley de Notificaciones, Citaciones y otras Comunicaciones Oficiales. Segunda Edición. San José, Costa Rica: EDITEC Editores,1999.
- Ley General de la Administración Pública. Sexta Edición. San José, Costa Rica: Investigaciones Jurídicas, S.A., 1997.
- Ley Orgánica del Poder Judicial. Quinta Edición. San José, Costa Rica: Investigaciones Jurídicas, S.A., 1999.
- Reglamento para el Uso del Fax como Medio de Notificación en los Despachos Judiciales. Segunda Edición. San José, Costa Rica: EDITEC Editores, 1999.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un Marco Comunitario para la Firma Electrónica.
- Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Gazz. Uff. n. 60 del 13 marzo 1998) Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59.

- Décret No. 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civill et relatif à la signature électronique.
- Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) in der Fassung des Beschlusses des Deutschen Bundestages vom 13. Juni 1997.
- Legge 15 marzo 1997, n. 59 (in suppl. ordinario n. 56/L, alla Gazz. Uff. n. 63, del 17 marzo) Delega al Governo per il conferimento di funzioni e compiti alle región ed enti locali, per la riforma della Pubblica Administrazione e per la semplificazione amministrativa.
- Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001
- Loi No. 2000-230 du 13mars 2000 portant adaptation du droit de la preuve aux technologies de 1'information et relative à la signature électronique.
- Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica

- Verordnung zur digitalen Signatur (Signaturverordnung - SigV) in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997
- **Informe sobre el proyecto de "Ley de Firma Digital y Certificados Digitales".** 033-AJ-2001. Poder Judicial - Departamento de Planificación

ANEXO I

LEY FEDERAL DE ESTADOS UNIDOS DE AMÉRICA

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

106TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 106-_____

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

_____

_____, 2000.—ORDERED TO BE PRINTED

_____

Mr. BLILEY, from the committee of conference, submitted the following

CONFERENCE REPORT

[To accompany S. 761]

The committee of conference on the disagreeing votes of the two Houses on the amendments of the House to the bill (S. 761), to regulate interstate commerce by electronic means by permitting and encouraging the continued expansion of electronic commerce through the operation of free market forces, and other purposes, having met, after full and free conference, have agreed to recommend and do recommend to their respective Houses as follows:

That the Senate recede from its disagreement to the amendment of the House to the text of the bill and agree to the same with an amendment as follows:

In lieu of the matter proposed to be inserted by the House amendment, insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Signatures in Global and National Commerce Act".

TITLE I—ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE

SEC. 101. GENERAL RULE OF VALIDITY.

(a) IN GENERAL.—Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

(b) PRESERVATION OF RIGHTS AND OBLIGATIONS.—This title does not—

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) CONSUMER DISCLOSURES.—

(1) CONSENT TO ELECTRONIC RECORDS.—Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if—

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) OTHER RIGHTS.—

(A) PRESERVATION OF CONSUMER PROTECTIONS.—Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law.

(B) VERIFICATION OR ACKNOWLEDGEMENT.—If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT.—The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) PROSPECTIVE EFFECT.—Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) PRIOR CONSENT.—This subsection does not apply to any records that are provided or made available to a consumer who

has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS.—An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

(d) RETENTION OF CONTRACTS AND RECORDS.—

(1) ACCURACY AND ACCESSIBILITY.—If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that—

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) EXCEPTION.—A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) ORIGINALS.—If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).

(4) CHECKS.—If a statute, regulation, or other rule of law requires the retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with paragraph (1).

(e) ACCURACY AND ABILITY TO RETAIN CONTRACTS AND OTHER RECORDS.—Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(f) PROXIMITY.—Nothing in this title affects the proximity required by any statute, regulation, or other rule of law with respect to any warning, notice, disclosure, or other record required to be posted, displayed, or publicly affixed.

(g) NOTARIZATION AND ACKNOWLEDGMENT.—If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be no-

tarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

(h) ELECTRONIC AGENTS.—A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

(i) INSURANCE.—It is the specific intent of the Congress that this title and title II apply to the business of insurance.

(j) INSURANCE AGENTS AND BROKERS.—An insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or electronic signature may not be held liable for any deficiency in the electronic procedures agreed to by the parties under that contract if—

(1) the agent or broker has not engaged in negligent, reckless, or intentional tortious conduct;

(2) the agent or broker was not involved in the development or establishment of such electronic procedures; and

(3) the agent or broker did not deviate from such procedures.

SEC. 102. EXEMPTION TO PREEMPTION.

(a) IN GENERAL.—A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law—

(1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection; or

(2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—

(i) such alternative procedures or requirements are consistent with this title and title II; and

(ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures; and

(B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.

(b) EXCEPTIONS FOR ACTIONS BY STATES AS MARKET PARTICIPANTS.—Subsection (a)(2)(A)(ii) shall not apply to the statutes, regu-

lations, or other rules of law governing procurement by any State, or any agency or instrumentality thereof.

(c) PREVENTION OF CIRCUMVENTION.—Subsection (a) does not permit a State to circumvent this title or title II through the imposition of nonelectronic delivery methods under section 8(b)(2) of the Uniform Electronic Transactions Act.

SEC. 103. SPECIFIC EXCEPTIONS.

(a) EXCEPTED REQUIREMENTS.—The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by—

(1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or

(3) the Uniform Commercial Code, as in effect in any State, other than sections 1–107 and 1–206 and Articles 2 and 2A.

(b) ADDITIONAL EXCEPTIONS.—The provisions of section 101 shall not apply to—

(1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;

(2) any notice of—

(A) the cancellation or termination of utility services (including water, heat, and power);

(B) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;

(C) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or

(D) recall of a product, or material failure of a product, that risks endangering health or safety; or

(3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(c) REVIEW OF EXCEPTIONS.—

(1) EVALUATION REQUIRED.—The Secretary of Commerce, acting through the Assistant Secretary for Communications and Information, shall review the operation of the exceptions in subsections (a) and (b) to evaluate, over a period of 3 years, whether such exceptions continue to be necessary for the protection of consumers. Within 3 years after the date of enactment of this Act, the Assistant Secretary shall submit a report to the Congress on the results of such evaluation.

(2) DETERMINATIONS.—If a Federal regulatory agency, with respect to matter within its jurisdiction, determines after notice and an opportunity for public comment, and publishes a finding, that one or more such exceptions are no longer necessary for the protection of consumers and eliminating such exceptions will not increase the material risk of harm to consumers, such agency may extend the application of section 101 to the exceptions identified in such finding.

SEC. 104. APPLICABILITY TO FEDERAL AND STATE GOVERNMENTS.

(a) FILING AND ACCESS REQUIREMENTS.—Subject to subsection (c)(2), nothing in this title limits or supersedes any requirement by a Federal regulatory agency, self-regulatory organization, or State regulatory agency that records be filed with such agency or organization in accordance with specified standards or formats.

(b) PRESERVATION OF EXISTING RULEMAKING AUTHORITY.—

(1) USE OF AUTHORITY TO INTERPRET.—Subject to paragraph (2) and subsection (c), a Federal regulatory agency or State regulatory agency that is responsible for rulemaking under any other statute may interpret section 101 with respect to such statute through—

(A) the issuance of regulations pursuant to a statute; or

(B) to the extent such agency is authorized by statute to issue orders or guidance, the issuance of orders or guidance of general applicability that are publicly available and published (in the Federal Register in the case of an order or guidance issued by a Federal regulatory agency).

This paragraph does not grant any Federal regulatory agency or State regulatory agency authority to issue regulations, orders, or guidance pursuant to any statute that does not authorize such issuance.

(2) LIMITATIONS ON INTERPRETATION AUTHORITY.—Notwithstanding paragraph (1), a Federal regulatory agency shall not adopt any regulation, order, or guidance described in paragraph (1), and a State regulatory agency is preempted by section 101 from adopting any regulation, order, or guidance described in paragraph (1), unless—

(A) such regulation, order, or guidance is consistent with section 101;

(B) such regulation, order, or guidance does not add to the requirements of such section; and

(C) such agency finds, in connection with the issuance of such regulation, order, or guidance, that—

(i) there is a substantial justification for the regulation, order, or guidance;

(ii) the methods selected to carry out that purpose—

(I) are substantially equivalent to the requirements imposed on records that are not electronic records; and

(II) will not impose unreasonable costs on the acceptance and use of electronic records; and

(iii) the methods selected to carry out that purpose do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

(3) PERFORMANCE STANDARDS.—

(A) ACCURACY, RECORD INTEGRITY, ACCESSIBILITY.—Notwithstanding paragraph (2)(C)(iii), a Federal regulatory agency or State regulatory agency may interpret section

101(d) to specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained. Such performance standards may be specified in a manner that imposes a requirement in violation of paragraph (2)(C)(iii) if the requirement (i) serves an important governmental objective; and (ii) is substantially related to the achievement of that objective. Nothing in this paragraph shall be construed to grant any Federal regulatory agency or State regulatory agency authority to require use of a particular type of software or hardware in order to comply with section 101(d).

(B) PAPER OR PRINTED FORM.—Notwithstanding subsection (c)(1), a Federal regulatory agency or State regulatory agency may interpret section 101(d) to require retention of a record in a tangible printed or paper form if—

(i) there is a compelling governmental interest relating to law enforcement or national security for imposing such requirement; and

(ii) imposing such requirement is essential to attaining such interest.

(4) EXCEPTIONS FOR ACTIONS BY GOVERNMENT AS MARKET PARTICIPANT.—Paragraph (2)(C)(iii) shall not apply to the statutes, regulations, or other rules of law governing procurement by the Federal or any State government, or any agency or instrumentality thereof.

(c) ADDITIONAL LIMITATIONS.—

(1) REIMPOSING PAPER PROHIBITED.—Nothing in subsection (b) (other than paragraph (3)(B) thereof) shall be construed to grant any Federal regulatory agency or State regulatory agency authority to impose or reimpose any requirement that a record be in a tangible printed or paper form.

(2) CONTINUING OBLIGATION UNDER GOVERNMENT PAPERWORK ELIMINATION ACT.—Nothing in subsection (a) or (b) relieves any Federal regulatory agency of its obligations under the Government Paperwork Elimination Act (title XVII of Public Law 105–277).

(d) AUTHORITY TO EXEMPT FROM CONSENT PROVISION.—

(1) IN GENERAL.—A Federal regulatory agency may, with respect to matter within its jurisdiction, by regulation or order issued after notice and an opportunity for public comment, exempt without condition a specified category or type of record from the requirements relating to consent in section 101(c) if such exemption is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers.

(2) PROSPECTUSES.—Within 30 days after the date of enactment of this Act, the Securities and Exchange Commission shall issue a regulation or order pursuant to paragraph (1) exempting from section 101(c) any records that are required to be provided in order to allow advertising, sales literature, or other information concerning a security issued by an investment company that is registered under the Investment Company Act of 1940, or concerning the issuer thereof, to be excluded from the

definition of a prospectus under section 2(a)(10)(A) of the Securities Act of 1933.

(e) ELECTRONIC LETTERS OF AGENCY.—The Federal Communications Commission shall not hold any contract for telecommunications service or letter of agency for a preferred carrier change, that otherwise complies with the Commission's rules, to be legally ineffective, invalid, or unenforceable solely because an electronic record or electronic signature was used in its formation or authorization.

SEC. 105. STUDIES.

(a) DELIVERY.—Within 12 months after the date of the enactment of this Act, the Secretary of Commerce shall conduct an inquiry regarding the effectiveness of the delivery of electronic records to consumers using electronic mail as compared with delivery of written records via the United States Postal Service and private express mail services. The Secretary shall submit a report to the Congress regarding the results of such inquiry by the conclusion of such 12-month period.

(b) STUDY OF ELECTRONIC CONSENT.—Within 12 months after the date of the enactment of this Act, the Secretary of Commerce and the Federal Trade Commission shall submit a report to the Congress evaluating any benefits provided to consumers by the procedure required by section 101(c)(1)(C)(ii); any burdens imposed on electronic commerce by that provision; whether the benefits outweigh the burdens; whether the absence of the procedure required by section 101(c)(1)(C)(ii) would increase the incidence of fraud directed against consumers; and suggesting any revisions to the provision deemed appropriate by the Secretary and the Commission. In conducting this evaluation, the Secretary and the Commission shall solicit comment from the general public, consumer representatives, and electronic commerce businesses.

SEC. 106. DEFINITIONS.

For purposes of this title:

(1) CONSUMER.—The term "consumer" means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.

(2) ELECTRONIC.—The term "electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(3) ELECTRONIC AGENT.—The term "electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.

(4) ELECTRONIC RECORD.—The term "electronic record" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

(5) ELECTRONIC SIGNATURE.—The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

(6) FEDERAL REGULATORY AGENCY.—The term "Federal regulatory agency" means an agency, as that term is defined in section 552(f) of title 5, United States Code.

(7) INFORMATION.—The term "information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(8) PERSON.—The term "person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(9) RECORD.—The term "record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(10) REQUIREMENT.—The term "requirement" includes a prohibition.

(11) SELF-REGULATORY ORGANIZATION.—The term "self-regulatory organization" means an organization or entity that is not a Federal regulatory agency or a State, but that is under the supervision of a Federal regulatory agency and is authorized under Federal law to adopt and administer rules applicable to its members that are enforced by such organization or entity, by a Federal regulatory agency, or by another self-regulatory organization.

(12) STATE.—The term "State" includes the District of Columbia and the territories and possessions of the United States.

(13) TRANSACTION.—The term "transaction" means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct:

(A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and

(B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

SEC. 107. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title shall be effective on October 1, 2000.

(b) EXCEPTIONS.—

(1) RECORD RETENTION.—

(A) IN GENERAL.—Subject to subparagraph (B), this title shall be effective on March 1, 2001, with respect to a requirement that a record be retained imposed by—

(i) a Federal statute, regulation, or other rule of law, or

(ii) a State statute, regulation, or other rule of law administered or promulgated by a State regulatory agency.

(B) DELAYED EFFECT FOR PENDING RULEMAKINGS.—If on March 1, 2001, a Federal regulatory agency or State regulatory agency has announced, proposed, or initiated, but not completed, a rulemaking proceeding to prescribe a regulation under section 104(b)(3) with respect to a requirement described in subparagraph (A), this title shall be effective on June 1, 2001, with respect to such requirement.

(2) CERTAIN GUARANTEED AND INSURED LOANS.—With regard to any transaction involving a loan guarantee or loan guarantee commitment (as those terms are defined in section 502 of the Federal Credit Reform Act of 1990), or involving a program listed in the Federal Credit Supplement, Budget of the United States, FY 2001, this title applies only to such transactions entered into, and to any loan or mortgage made, insured, or guaranteed by the United States Government thereunder, on and after one year after the date of enactment of this Act.

(3) STUDENT LOANS.—With respect to any records that are provided or made available to a consumer pursuant to an application for a loan, or a loan made, pursuant to title IV of the Higher Education Act of 1965, section 101(c) of this Act shall not apply until the earlier of—

(A) such time as the Secretary of Education publishes revised promissory notes under section 432(m) of the Higher Education Act of 1965; or

(B) one year after the date of enactment of this Act.

TITLE II—TRANSFERABLE RECORDS

SEC. 201. TRANSFERABLE RECORDS.

(a) DEFINITIONS.—For purposes of this section:

(1) TRANSFERABLE RECORD.—The term "transferable record" means an electronic record that—

(A) would be a note under Article 3 of the Uniform Commercial Code if the electronic record were in writing;

(B) the issuer of the electronic record expressly has agreed is a transferable record; and

(C) relates to a loan secured by real property.

A transferable record may be executed using an electronic signature.

(2) OTHER DEFINITIONS.—The terms "electronic record", "electronic signature", and "person" have the same meanings provided in section 106 of this Act.

(b) CONTROL.—A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(c) CONDITIONS.—A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that—

(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as—

(A) the person to which the transferable record was issued; or

(B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(d) STATUS AS HOLDER.—Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in section 1–201(20) of the Uniform Commercial Code, of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under the Uniform Commercial Code, including, if the applicable statutory requirements under section 3–302(a), 9–308, or revised section 9–330 of the Uniform Commercial Code are satisfied, the rights and defenses of a holder in due course or a purchaser, respectively. Delivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection.

(e) OBLIGOR RIGHTS.—Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under the Uniform Commercial Code.

(f) PROOF OF CONTROL.—If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

(g) UCC REFERENCES.—For purposes of this subsection, all references to the Uniform Commercial Code are to the Uniform Commercial Code as in effect in the jurisdiction the law of which governs the transferable record.

SEC. 202. EFFECTIVE DATE.

This title shall be effective 90 days after the date of enactment of this Act.

TITLE III—PROMOTION OF INTERNATIONAL ELECTRONIC COMMERCE

SEC. 301. PRINCIPLES GOVERNING THE USE OF ELECTRONIC SIGNATURES IN INTERNATIONAL TRANSACTIONS.

(a) PROMOTION OF ELECTRONIC SIGNATURES.—

(1) REQUIRED ACTIONS.—The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions

necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.

(2) PRINCIPLES.—The principles specified in this paragraph are the following:

(A) Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law.

(B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.

(C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.

(D) Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions.

(b) CONSULTATION.—In conducting the activities required by this section, the Secretary shall consult with users and providers of electronic signature products and services and other interested persons.

(c) DEFINITIONS.—As used in this section, the terms "electronic record" and "electronic signature" have the same meanings provided in section 106 of this Act.

TITLE IV—COMMISSION ON ONLINE CHILD PROTECTION

SECTION 401. AUTHORITY TO ACCEPT GIFTS.

Section 1405 of the Child Online Protection Act (47 U.S.C. 231 note) is amended by inserting after subsection (g) the following new subsection:

"(h) GIFTS, BEQUESTS, AND DEVISES.—The Commission may accept, use, and dispose of gifts, bequests, or devises of services or property, both real (including the use of office space) and personal, for the purpose of aiding or facilitating the work of the Commission. Gifts or grants not used at the termination of the Commission shall be returned to the donor or grantee.".

And the House agree to the same.

That the Senate recede from its disagreement to the amendment of the House to the title of the bill and agree to the same.

ANEXO II

LEY DEL ESTADO DE UTAH

UTAH DIGITAL SIGNATURE ACT

Utah Digital Signature Act

Utah Code §§ 46-3-101 to 46-3-504

Enacted by L. 1995, ch. 61

PART 1. Title, interpretation, and definitions

PART 2. Licensing and regulation of certification authorities

PART 3. Duties of certification authority and subscriber

PART 4. Effect of a digital signature

PART 5. State services and reorganized repositories

For more current information, including amendments and regulations promulgated under this statute, consult Thomas J. Smedinghoff's Summary of Electronic Commerce and Digital Signature Legislation or the Utah Digital Signature Development Program web site.

Utah Digital Signature Act

PART 1. Title, interpretation, and definitions

Utah Code §§ 46-3-101 to 46-3-104

46-3-101 Title.

This chapter is known as the "Utah Digital Signature Act."

46-3-102 Purposes and construction.

This chapter shall be construed liberally to effectuate the following purposes:
(1) to minimize the incidence of forged digital signatures and enable the reliable authentication of computer-based information;
(2) to enable and foster the verification of digital signatures on computer-based documents;
(3) to facilitate commerce by means of computerized communications; and
(4) to give legal effect to the general import of the following and other similar standards:
(a) Standard X.509 of the International Telecommunication Union (formerly CCITT or International Telegraph and Telephone Consultative Committee);
(b) Standard X.9.30 of the American National Standards Institute (ANSI); and
(c) RFC 1421 through 1424 of the Internet Activities Board (IAB).

46-3-103 Definitions.

As used in this chapter:
(1) "Accept a certificate" means to either:
(a) take physical delivery of a certificate; or
(b) apply for a certificate without cancelling or revoking the application by delivering notice of the cancellation or revocation to the certification authority, and obtaining a signed, written receipt from the certification authority.
(2) "Asymmetric cryptosystem" means a computer algorithm or series of algorithms which utilize two different keys with the following characteristics:
(a) one key encrypts a given message;
(b) one key decrypts a given message; and
(c) the keys have the property that, knowing one key, it is computationally infeasible to discover the other key.

(3) "Bit" means a binary digit, or a number, often encoded in a computer- readable form, which has a value of either 0 or 1.

(4) "Certificate" means:

(a) a computer-based record identifying a subscriber and containing the subscriber's public key; or

(b) if the certificate is issued by a licensed certification authority, a computer-based record identifying a subscriber containing the subscriber's public key, and additional data about the subscriber as specified in Section 46-3-104.

(5) "Certification authority" means a person who issues one or more certificates.

(6) "Certification authority disclosure record" means an on-line, publicly accessible computer record concerning a licensed certification authority maintained by the division in accordance with Section 46-3-203.

(7) "Certify" means to declare with reference to a certificate, that all material facts in the certificate are true.

(8) "Confirm" means to ascertain through inquiry and investigation carried out with all the effort and resources commercially reasonable under the circumstances.

(9) "Correspond" means, when referring to keys, that one key belongs to the same key pair as the other.

(10) "Digital signature" is a sequence of bits which a person intending to sign creates in relation to a clearly delimited message by running the message through a one-way function, then encrypting the resulting message digest using an asymmetrical cryptosystem and the person's private key.

(11) "Division" refers to the Division of Corporations and Commercial Code within Department of Commerce.

(12) "Distinguished name" means a sequence of alphanumeric characters uniquely identifying the person bearing the name.

(13) "Forge a digital signature" means to create an apparent digital signature without the authorization of the rightful holder of the private key.

(14) "Issue a certificate" means to create and digitally sign a certificate and to deliver a copy of the certificate to the subscriber named in the certificate.

(15) "Key pair" means a private key and its corresponding public key which are the keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.

(16) "Licensed certification authority" means a certification authority to whom a license has been issued by the division.

(17) "Material" means germane to and having substantial consequences for an actual transaction involving a digital signature.

(18) (a) "Message" means a writing or recording recorded by means of any medium and intended to be signed.

(b) For purposes of this subsection, "writings" and "recordings" consist of letters, words, numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

(19) "One-way function" means an algorithm mapping or translating one set of bits into another set in such a way that:

(a) a message yields the same result every time it is passed through the one-way function;

(b) it is computationally infeasible that a message passed through the one-way function can be derived or reconstituted from the results of the function; and

(c) there is at most only a negligible probability that two

messages passing through the same one-way function will produce the same result.

(20) "Operative personnel" means one or more persons:

(a) acting as a certification authority or its agent;

(b) having managerial or policymaking responsibilities for the certification authority; or

(c) having duties directly involving the issuance of certificates, creation of keys, or administration of computing facilities.

(21) "Person" means a natural person, corporation, partnership, governmental body, or any other entity capable of signing a document.

(22) "Private key" means a sequence of bits in an asymmetric cryptosystem used to affix a digital signature to a message. A private key is intended to be known only by the rightful holder of the key.

(23) "Public key" means a sequence of bits in an asymmetric cryptosystem used to verify a digital signature. A public key may be known and used by anyone in order to verify a signature.

(24) "Publish" means to record or place on file in a repository accessible by multiple persons in the ordinary course of business.

(25) "Recognized repository" means a repository recognized by the division pursuant to Section 46-3-502.

(26) "Recommended reliance limit" means the limit of an issuing certification authority's liability and financial responsibility specified in a certificate.

(27) "Record address" means:

(a) the address on file with the division for a Utah corporation or foreign corporation authorized to do business in Utah; or

(b) the principal, official, or record address on file with any other government entity if no address is on file with the division; or

(c) if no address is reasonably ascertainable with a government entity, the last-known address of the subscriber ascertained, whenever possible, independently of any representations made in applying for a certificate.

(28) "Record leaders" are:

(a) the officers and directors or trustees listed for a corporation on the most recent report to the division or its counterpart in another state;

(b) the general partners listed for a limited partnership in the records of the division or its counterpart in another state; and

(c) the natural persons having authority to manage or direct the affairs of the subscriber, ascertained whenever possible from information sources other than representations made in applying for a certificate.

(29) "Repository" means a database of certificates accessible on-line.

(30) "Repository operator" means the person operating and responsible for the repository.

(31) (a) "Revoke a certificate" means to make a certificate ineffective from a specified time and forward perpetually.

(b) Revocation is effected by notation or inclusion in a set of revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible.

(32) "Rightfully hold a private key" means to know or be able to readily ascertain a private key:

(a) for which a corresponding public key has not been published in a certificate on file in the repository provided by the division or in a recognized repository;

(b) which the holder or the holder's agent has not revealed to any person in violation of Subsection 46-3-303(1); and

(c) which the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

(33) "Subscriber" means a person holding a private key which corresponds to a public key listed in a certificate identifying the subscriber.

(34) (a) "Suitable guaranty" means either a surety bond executed by a surety firm authorized by the Insurance Department to do business in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state by the Department of Financial Institutions, which satisfies all of the following requirements:

(i) it is issued for the benefit of claimants under this chapter and is conditioned upon the certification authority conducting business as required by this chapter;

(ii) it is in an amount equal to or exceeding the greater of either:

(A) 100% of the largest recommended reliance limit of a certificate to be issued or published by the filing certification authority during the term of the certification authority's license; or

(B) at least 35% of the recommended reliance limits of all certificates published by the filing certification authority which have not expired or been revoked;

(iii) it states that it is issued for filing pursuant to this chapter;

(iv) it specifies a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority; and

(v) it is in a form approved by division rule.

(b) A suitable guaranty may provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty.

(35) (a) "Suspend" means to make the certificate ineffective or void temporarily from a specified time forward.

(b) "Suspend" does not imply that the certificate is destroyed or made illegible.

(36) "Time-stamp" means either:

(a) to append to a message a digitally signed notation indicating the date, time, and identity of the person appending the notation; or

(b) the notation appended according to Subsection (a).

(37) "Verify a digital signature" means:

(a) to decrypt a digital signature using the public key listed in a valid certificate;

(b) to pass the message through the one-way function used in affixing the digital signature; and

(c) to then correctly determine that the results of passing the message through the one-way function and the decrypted digital signature are identical.

46-3-104 Contents of a certificate -- Effective date.

(1) A certificate issued by a licensed certification authority shall contain:

(a) the name by which the subscriber is generally known;

(b) the distinguished name of the subscriber;

(c) a public key corresponding to a private key held by the subscriber;

(d) a brief description of any algorithms with which the subscriber's public key was intended to be used in a form prescribed

by the division;

(e) the serial number of the certificate which must be unique among the certificates issued by the issuing certification authority;

(f) the date and time on which the certificate was issued and accepted which is the date on which the certificate takes effect;

(g) the date and time on which the certificate expires;

(h) the distinguished name of the certification authority issuing the certificate;

(i) a brief description of the algorithm used to sign the certificate, in a form prescribed by the division;

(j) the recommended reliance limit for transactions relying on the certificate; and

(k) other items the division requires by rule.

(2) A certificate issued by a licensed certification authority may, at the option of the subscriber and certification authority, contain any of the following:

(a) a secondary public key and its identifier or usage indicator;

(b) information material to the certificate's reliability and to any claims based on it;

(c) references incorporating specified and available documents material to the certificate, the issuing certification authority, or the accepting subscriber; and

(d) other items permitted by division rule.

(3) (a) The division may by rule require additional information in a certificate, so long as the certificate conforms to generally accepted standards for digital signature certificates and nothing in the certificate disclaims or limits the representations of the subscriber and the certification authority implied in Part 3 of this chapter.

(b) The certificate shall be in a database form specified by division rule.

(4) (a) The division may, at the joint request of a subscriber and licensed certification authority, create a secret field in its database. The division may disclose the contents of the secret field in its database only to:

(i) the licensed certification authority publishing the certificate;

(ii) authorized personnel of the division; and

(iii) a court clerk or county clerk who has received a request for suspension of the pertinent certificate.

(b) The contents of the secret field should be a password or fact likely to be known only by the subscriber, and may, in the discretion of the entity processing a request for suspension, be used to determine the identity of the requester.

Utah Digital Signature Act

PART 2. Licensing and regulation of certification authorities

Utah Code §§ 46-3-201 to 46-3-207

46-3-201 Licensure and qualifications of certification authorities.

(1) To obtain or retain a license as a certification authority by the division, a certification authority must:

(a) be either:

(i) an attorney admitted to practice before the courts of this state, that attorney's partnership which engages principally in the practice of law if the attorney is a partner, or a professional corporation in which the attorney named in the license is a shareholder;

(ii) a financial institution, a corporation authorized to conduct a trust business, or an insurance company, if authorized to do business in this state;

(iii) any title insurance or abstract company authorized to do business in this state; or

(iv) the governor, a department or division of state government, other than the Digital Signature Agency, the attorney general, the Utah Judicial Council, a state court, a city, a county, or the Legislature provided that:

(A) each of the governmental entities acts through designated officials authorized by ordinance, rule, or statute to perform certification authority functions; and

(B) the state or one of the governmental entities is the subscriber of all certificates issued by the certification authority;

(b) be the subscriber of a certificate published in the repository provided by the division or in a recognized repository;

(c) qualify and hold an appointment as a notary public or employ at least one notary public;

(d) employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception;

(e) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;

(f) file with the division a suitable guaranty, unless the certification authority is a governmental entity listed in Subsection

(1)(a)(iv);

(g) have access to hardware and software suitable for fulfilling the requirements of this chapter according to division rules;

(h) maintain an office in Utah or have established a registered agent for service of process in Utah; and

(i) comply with all licensing requirements established by division rule.

(2) The division shall issue a license to a certification authority which:

(a) is qualified under Subsection (1);

(b) applies in writing to the division for a license; and

(c) pays the required filing fee.

(3) (a) A license may specify that its scope is limited to:

(i) a specified number of certificates; or

(ii) a specified cumulative maximum of recommended reliance limits in certificates issued by the certification authority.

(b) If the scope of a license is limited, a certification authority acts as an unlicensed certification authority when issuing a certificate exceeding the limits of the license.

(4) (a) The division may revoke or suspend a certification authority's license for failure to comply with this chapter, or for failure to remain qualified pursuant to Subsection (1).

(b) The division's actions under this subsection are subject to the procedures for adjudicative proceedings in Title 63, Chapter 46b, Administrative Procedures Act.

(5) Unless the parties provide otherwise by contract between themselves, the licensing requirements in this section do not affect the validity of any certificate or digital signature issued by an unlicensed certification authority, except that:

(a) the presumptions created in Part 4 of this chapter do not apply to a certificate issued by an unlicensed certification authority; and

(b) the limitation of liability created in Section 46-3-308 does not apply to a certificate issued by an unlicensed certification authority.

46-3-202 Performance audits and investigations.

(1) A certified public accountant approved by division rule shall audit the operations of each licensed certification authority at least once each year to evaluate compliance with this chapter.

(2) (a) Based on information gathered in the audit, the auditor shall categorize the licensed certification authority's compliance as one of the following:

(i) full compliance: the certification authority appears to conform to all applicable statutory and regulatory requirements;

(ii) substantial compliance: the certification authority generally appears to comply with all applicable statutory and regulatory requirements; however, some instances of noncompliance or inability to demonstrate compliance were found in the audited sample which were likely to be inconsequential;

(iii) partial compliance: the certification authority appears to comply with some statutory and regulatory requirements, but was found not to have complied or not able to demonstrate compliance with one or more statutory or regulatory requirements;

(iv) noncompliance: the certification authority complies with few or none of the statutory and regulatory requirements, or fails to keep adequate records to demonstrate compliance with more than a few

requirements, or refused to submit to an audit.

(b) The division shall publish in the certification authority disclosure record the date of the audit and the resulting categorization of the certification authority.

(3) (a) A licensed certification authority is exempt from the requirements of Subsection (1) if:

(i) the certification authority requests exemption in writing;

(ii) the most recent performance audit, if any, of the certification authority resulted in a finding of full or substantial compliance; and

(iii) the certification authority states under oath or affirmation that one or more of the following is true with respect to the certification authority:

(A) the certification authority has issued fewer than six certificates during the past year and the recommended reliance limits of all such certificates do not exceed $10,000;

(B) the aggregate lifetime of all certificates issued by the certification authority during the past year is less than 30 days and the recommended reliance limits of all such certificates do not exceed $10,000; or

(C) the recommended reliance limits of all certificates outstanding and issued by the certification authority total less than $1,000.

(b) If a licensed certification authority is exempt under this subsection, the division shall publish in the certification authority disclosure record that the certification authority is exempt from the performance audit requirement.

46-3-203 Contents of a certification authority disclosure record.

(1) A certification authority disclosure record shall contain:

(a) the name, address, and telephone number of the certification authority;

(b) the distinguished name of the certification authority;

(c) the current public key of the certification authority;

(d) the categorization of the certification authority based on the most recent performance audit of the certification authority's activities, and the date of the most recent performance audit;

(e) if the certification authority's certificate has been revoked since licensure, the public key contained in the revoked certificate, date of revocation, and grounds for revocation;

(f) the amount of the certification authority's suitable guaranty;

(g) if the certification authority's license has been revoked or is currently suspended, the date of revocation or suspension and the grounds for revocation or suspension;

(h) the limits, if any, placed on the certification authority's license;

(i) any event or activity which substantially affects the certification authority's ability to conduct its business, or the validity of more than ten of the certificates listed in the repository provided by the division or in a recognized repository;

(j) if the certificate containing the public key required to verify one or more certificates issued by the certification authority has been revoked or is currently suspended, the date of its revocation or suspension;

(k) a statement dated within one year of the current date, containing additional rules or policies, and not exceeding two

kilobytes in length, if the certification authority submits such a statement in a form prescribed by division rule; and

(1) other information required by division rule.

(2) The division shall maintain an electronic database in its repository containing the disclosure record described in this section for each licensed certification authority.

46-3-204 Enforcement of requirements for licensed certification authorities.

(1) Division actions under this section must be made in accordance with the procedures for adjudicative proceedings in Title 63, Chapter 46b, Administrative Procedures Act.

(2) The division may:

(a) investigate the activities of a licensed certification authority material to the requirements of this chapter; and

(b) issue orders to a certification authority to secure compliance with this chapter.

(3) Nothing in this section restricts local law enforcement authorities from investigating and prosecuting violations of criminal laws.

(4) The division may suspend or revoke the license of a certification authority for serious noncompliance with an order of the division.

(5) A person may obtain punitive damages against a certification authority in a civil action against the certification authority if:

(a) the division has issued an order in accordance with Subsection (2) expressly permitting punitive damages to be assessed against the certification authority;

(b) the certification authority has not complied with the order;

(c) the person has suffered a loss caused by noncompliance with the order; and

(d) the division has granted permission for punitive damages.

(6) The division may order a certification authority which it has found to have violated a requirement of this chapter to pay the costs incurred by the division in prosecuting and adjudicating proceedings related to the enforcement of the order.

(7) (a) A licensed certification authority may obtain judicial review of the division's actions.

(b) The division may seek an injunction to compel compliance with any of its orders.

46-3-205 Record-keeping by certification authorities.

(1) A licensed certification authority shall maintain detailed records documenting compliance with this chapter and all actions taken with respect to each certificate issued by the certification authority. The records shall include evidence supporting the identification of the person named in a certificate with the distinguished name and public key set forth in the certificate. Except for requests for suspension of a certificate, the licensed certification authority may require a subscriber or agent of a subscriber to submit reasonable documentation sufficient to enable the certification authority to comply with this chapter.

(2) (a) A licensed certification authority shall retain its records of the issuance, and any suspension or revocation of a certificate, for a period of not less than 40 years after the

certificate is issued.

(b) The licensed certification authority may:

(i) contract with another licensed certification authority for the record retention required by this section; or

(ii) place the records required by this section into the custody of the Department of Commerce upon ceasing to act as a certification authority.

(c) A licensed certification authority shall secure its records in a manner that is commercially reasonable in light of the recommended reliance limits of the certificates.

46-3-206 Cessation of certification authority activities.

(1) Before ceasing to act as a certification authority, a licensed certification authority shall:

(a) give to the subscriber of each unrevoked or unexpired certificate 90 days' written notice of the certification authority's intention to discontinue acting as a certification authority;

(b) 90 days after the notice required in Subsection (1)(a), revoke all certificates which then remain unrevoked or unexpired, regardless of whether the subscriber has requested revocation;

(c) give written notice of revocation to the subscriber of each certificate revoked pursuant to Subsection (1)(b); and

(d) unless the contract between the certification authority and the subscriber provides otherwise, pay reasonable restitution to the subscriber for revoking the certificate before its expiration date.

(2) (a) To provide uninterrupted certification authority services, the discontinuing certification authority may arrange with another certification authority, including the division, for reissuance of the remaining certificates under the succeeding certification authority's digital signature for the unexpired term of the remaining certificates or one year, whichever is less.

(b) In reissuing a certificate pursuant to this subsection, the succeeding certification authority becomes subrogated to the rights and defenses of the discontinuing certification authority.

(3) The requirements of this section may be varied by contract, except that the contract may not permit the licensed certification authority to discontinue its certification authority activities without first:

(a) giving each subscriber of an unexpired or unrevoked certificate at least ten days' written notice; and

(b) revoking all outstanding certificates upon cessation of certification authority activities.

(4) (a) A licensed certification authority shall notify the division of its intention to terminate acting as a certification authority.

(b) The notice shall be in a form specified by division rule and shall be submitted to the division at least two months, but not more than six months, before the date of termination.

(c) The division may by rule or by order in a specific case require additional statements to be filed in order to track compliance with this section.

(5) (a) If a certification authority dies while licensed, the estate of the certification authority shall comply with the procedures of this section for termination of the deceased certification authority's activities.

(b) If a certification authority becomes incapacitated within the meaning of Subsection 75-1-201(18), a court may either appoint a

guardian as provided in Title 75, Chapter 5, Part 3, Utah Uniform Probate Code, or, on the petition of an interested party, appoint a receiver to terminate the incapacitated certification authority's business as provided in this section.

(c) The division may promulgate rules to facilitate termination of certification authority activities or to protect subscribers and others in cases where the certification authority dies or becomes incapacitated.

46-3-207 Hazardous activities by any certification authority prohibited.

(1) A certification authority, whether licensed or not, may not conduct its business in a manner that creates a commercially unreasonable risk of loss to:

(a) subscribers of the certification authority;

(b) persons relying on certificates issued by certification authority; or

(c) any repository recognized pursuant to Section 46-3-502.

(2) (a) The division may publish in the repository it provides or elsewhere statements advising subscribers, persons relying on digital signatures, or public repositories about activities of a certification authority, whether licensed or not, that create a risk prohibited by Subsection (1).

(b) The certification authority named in a statement as creating or causing a risk may protest the publication of the statement.

(c) Upon receipt of a protest, the division shall:

(i) include with its statement a comment that a protest has been received; and

(ii) promptly give the protesting certification authority notice and an opportunity to be heard.

(d) Following the hearing, the division shall:

(i) rescind the advisory statement if its publication was unwarranted;

(ii) cancel it if its publication is no longer warranted;

(iii) continue or amend it if it remains warranted; or

(iv) take further legal action to eliminate or reduce a risk prohibited by Subsection (1).

(e) The division shall publish its decision in the repository it provides.

(3) In the manner provided by the Administrative Procedures Act, the division may issue orders and obtain injunctions or other civil relief to prevent or restrain a certification authority from violating this section, regardless of whether the certification authority is licensed. This section does not create a right of action in any person other than the division.

Utah Digital Signature Act

PART 3. Duties of certification authority and subscriber

Utah Code §§ 46-3-301 to 46-3-309

46-3-301 Issuing a certificate.

(1) (a) A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(i) the certification authority has received a signed request for issuance of a certificate by the prospective subscriber;

(ii) the certification authority confirms that:

(A) the prospective subscriber is the person identified in the request and the person to be identified in the certificate to be issued;

(B) if the prospective subscriber is acting through an agent, the subscriber duly authorized the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(C) the prospective subscriber bears a distinguished name; and

(D) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(iii) the certification authority confirms that the prospective subscriber holds a key pair capable of:

(A) affixing a digital signature by the private key corresponding to the public key to be listed in the certificate; and

(B) verifying that a digital signature has been affixed by the corresponding private key through the use of the public key.

(b) The requirements of this subsection may not be waived or disclaimed by the licensed certification authority or the subscriber.

(2) (a) If a certificate is requested by an agent or an apparent agent of the subscriber, the certification authority may not issue the certificate until after the certification authority has given ten days' written notice to the prospective subscriber through all of its record leaders at its record address.

(b) The notice shall express the certification authority's intent to issue a certificate for the prospective subscriber to the requesting agent and the date on which the certificate is to be issued.

(c) The requirement of notice in this subsection may be waived or disclaimed only by:

(i) a writing signed by all of the record leaders of the prospective subscriber; and

(ii) confirmation of the authenticity of the waiver by the certification authority.

(3) (a) If the subscriber accepts the certificate, the certification authority shall publish a signed copy of the certificate in the repository provided by the division or in one or more recognized repositories agreed upon by the certification authority and the subscriber named in the certificate.

(b) The contract between the certification authority and the subscriber may provide that the certificate may not be published.

(c) If the subscriber does not accept the certificate, a licensed certification authority may not publish the certificate in the repository provided by the division.

(4) Nothing in this section precludes a licensed certification authority from conforming to standards, security policies, or contractual requirements more rigorous than, but consistent with, this section.

(5) (a) If a licensed certification authority confirms that a certificate was not issued as required by this section, the certification authority:

(i) shall immediately revoke the certificate; or

(ii) may suspend the certificate while investigating to confirm grounds for revocation.

(b) The certification authority shall give notice as soon as practicable to the subscriber of a certificate revoked or suspended pursuant to this subsection.

(6) The division may order the licensed certification authority to suspend or revoke a certificate which the certification authority issued if, after notice and an opportunity for the certification authority and subscriber to be heard in accordance with the Administrative Procedures Act, the division determines that:

(a) a certificate was issued without substantial compliance to this section; and

(b) the noncompliance poses a significant hazard to parties relying on the certificate.

46-3-302 Representations by the subscriber accepting a certificate.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate certifies to all who justifiably rely on the information contained in the certificate that:

(a) each digital signature affixed by means of the private key corresponding to the public key listed in the certificate is a legally valid signature of the subscriber, unless the certificate:

(i) is suspended;

(ii) is revoked by the certification authority; or

(iii) has expired;

(b) no unauthorized person has access to the private key corresponding to the public key listed in the certificate;

(c) all representations made by the subscriber to the certification authority which are material to information contained in the certificate are true; and

(d) the information contained in the certificate is true.

(2) By requesting on behalf of a principal the issuance of a

certificate naming the principal as subscriber, a person certifies to all who justifiably rely on the information contained in the certificate that:

(a) the person holds all authority legally required for issuance of a certificate naming the principal as subscriber; and

(b) the person has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

(3) A person may not disclaim or rebut the representations implied in this section or obtain indemnity for them, if the effect of the disclaimer or indemnity is to limit liability for wrongful issuance of a certificate as against persons justifiably relying on the certificate.

(4) (a) If a subscriber makes a false, material and written representation of fact, or fails to disclose a material fact, with either the intent to deceive the certification authority or a person relying on the certificate, or with negligence, the subscriber, by accepting a certificate, becomes obligated to indemnify the issuing certification authority for any loss or damage caused by the misrepresentation or negligence.

(b) If the certification authority issued the certificate at the request of agents of the subscriber, both the agents and the subscriber shall indemnify the certification authority in accordance with this subsection.

(c) The indemnity provided in this subsection may not be disclaimed or superseded by contract between the certification authority and the subscriber.

(5) To obtain information required for issuance of a certificate, the certification authority may require a subscriber to testify under oath or an affirmation of truthfulness.

46-3-303 Control of the private key.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care in retaining control of the private key and keeping it confidential.

(2) A private key is the property of the subscriber who rightfully holds it.

(3) (a) If a certification authority holds the private key corresponding to a public key listed in a certificate which it issued, it holds the private key as a fiduciary of the subscriber named in the certificate, regardless of any provision to the contrary in a contract between the subscriber and the certification authority.

(b) A certification authority holding the subscriber's private key may use it only upon the prior written consent of the subscriber.

46-3-304 Duties of a licensed certification authority in issuing a certificate.

(1) (a) By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:

(i) the certificate contains no information known to the certification authority to be false;

(ii) the certificate satisfies the requirements of this chapter and does not exceed any limitations of the certification authority's

license; and

(iii) the certification authority has not exceeded any limitation of its license in issuing the certificate.

(b) The warranties described in this subsection may not be limited or disclaimed by contract.

(2) Unless the parties otherwise agree, a certification authority, by issuing a certificate, promises to the subscriber:

(a) to notify the subscriber within a reasonable time of any facts known to the certification authority which affect the validity or reliability of the certificate once it is issued; and

(b) to act promptly to suspend or revoke a certificate in accordance with Section 46-3-305.

(3) By issuing a certificate, a licensed certification authority certifies to all who justifiably rely on the information contained in the certificate that the certification authority has complied with all applicable requirements for issuance of the certificate.

(4) By publishing a certificate, a licensed certification authority certifies to the repository and to all who justifiably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

46-3-305 Suspension of a certificate.

(1) (a) Unless the certification authority and the subscriber otherwise agree, the licensed certification authority which issued a certificate shall suspend the certificate for a period of 48 hours:

(i) upon request by a person identifying himself as:

(A) the subscriber named in the certificate;

(B) an agent of the subscriber;

(C) a business associate of the subscriber;

(D) an employee of the subscriber; or

(E) a member of the immediate family of the subscriber; or

(ii) upon order of the division pursuant to Subsection 46-3-301(6).

(b) The certification authority need not confirm the identity or division of the person requesting suspension.

(2) (a) Unless the certificate or other records in the repository indicate otherwise, the division, a court clerk, or a county clerk may suspend a certificate issued by a licensed certification authority for a period of 48 hours, if:

(i) a person identifying himself as the subscriber named in the certificate, or as an agent, business associate, employee, or member of the immediate family of the subscriber requests suspension; and

(ii) the requester represents that the certification authority which issued the certificate is unavailable.

(b) The division or clerk may:

(i) require the requester to provide evidence of his identity, authorization, and the unavailability of the issuing certification authority;

(ii) inquire of the contents of the certificate and the secret field described in Subsection 46-3-104(4); and

(iii) decline to suspend the certificate with or without cause.

(c) The division or law enforcement agencies may investigate multiple suspensions by the division, court clerk, or county clerks for possible wrongdoing.

(3) (a) Immediately upon suspension of a certificate, the suspending certification authority, court clerk, or county clerk shall publish signed notice of the suspension in all repositories in which

the certificate was published.

(b) If the repository described in Subsection (a) no longer exists, or if the person suspending the certificate does not know all the repositories in which the certificate was published, the certification authority shall publish the notice of suspension in the repository provided by the division.

(4) (a) A certification authority shall terminate the suspension of a certificate that was suspended by request if:

(i) the subscriber named in the suspended certificate requests that the suspension be terminated and, the certification authority confirms the identity of the person making the request, and when the requester is acting as agent, the agent's authorization by the subscriber; or

(ii) the certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber.

(b) This subsection does not obligate the certification authority to confirm a request for suspension.

(5) The contract between a subscriber and a licensed certification authority may:

(a) limit or eliminate suspension by the certification authority upon request; or

(b) provide for termination of a suspension or disclosure of information about a suspension that varies from the requirements of Subsections (1), (2), (4), and (5), except that if the contract varies from the requirements of this section, the certificate must indicate the differences for the contractual variation to be valid.

(6) (a) No person may knowingly or intentionally misrepresent to a certification authority his identity, name, distinguished name, or authorization when requesting suspension of a certificate.

(b) Violation of this subsection is a class B misdemeanor.

(7) The subscriber is released from the duty to keep the private key secure pursuant to Section 46-3-303 during the period the certificate is suspended.

46-3-306 Revocation of a certificate.

(1) (a) A licensed certification authority shall revoke a certificate which it issued after receiving and confirming a request for revocation by the subscriber named in the certificate in accordance with Subsection (b).

(b) A licensed certification authority shall confirm a request for revocation and revoke a certificate within one business day after:

(i) receiving a subscriber's written request accompanied by evidence reasonably sufficient to confirm the request; and

(ii) receiving any required fee.

(2) A licensed certification authority shall revoke a certificate which it issued upon receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead.

(3) (a) A licensed certification authority may revoke one or more certificates which it issued if the certificates are or become unreliable regardless of whether the subscriber consents to the revocation.

(b) Unless the contract between the certification authority and the subscriber provides otherwise, the certification authority shall pay reasonable restitution to the subscriber and compensate the subscriber for any interruption to the subscriber's business due to

the revocation of the certificate under the circumstances described in Subsection (3)(a).

(4) (a) Immediately upon revocation of a certificate, the revoking certification authority shall publish signed notice of the revocation in all repositories in which the certification authority published the certificate.

(b) If the repositories described in Subsection (a) no longer exist, or if all are unrecognized repositories, the certification authority shall publish the notice in the repository provided by the division.

(5) A subscriber ceases to certify as provided in Section 46-3-302, and has no further duty to keep the private key secure as required by Section 46-3-303 when either:

(a) notice of the revocation is published as required in Subsection (4); or

(b) the certification authority is required to revoke under Subsection (1).

(6) Upon publication as required by Subsection 46-3-305(3), a licensed certification authority is:

(a) discharged of its warranties based on issuance of the revoked certificate; and

(b) ceases to certify as provided in Subsection 46-3-304(2) and (3) in relation to the revoked certificate.

46-3-307 Expiration of a certificate.

(1) (a) A certificate shall indicate the date on which it expires.

(b) A certificate's expiration date may be no later than three years after its issuance.

(2) When a certificate expires:

(a) the subscriber and certification authority cease as provided in Sections 46-3-302 and 46-3-304; and

(b) the certification authority is discharged of its duties based on issuance, in relation to the expired certificate.

46-3-308 Liability of a licensed certification authority.

(1) By specifying a recommended reliance limit in a certificate, the issuing certification authority and accepting subscriber recommend that persons rely on the certificate only in transactions in which the total amount at risk does not exceed the recommended reliance limit.

(2) Except as designated in Subsection 46-3-201(5):

(a) a licensed certification authority is not liable for any loss caused by a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with the requirements of this chapter;

(b) a licensed certification authority is not liable for a misrepresentation in the certificate, or for error in issuing the certificate in excess of the amount specified in the certificate as the recommended reliance limit; and

(c) a licensed certification authority is not liable for punitive or exemplary damages, except as provided in Section 46-3-204.

46-3-309 Collection based on suitable guaranty.

(1) (a) Notwithstanding any provision in the suitable guaranty to the contrary:

(i) if the suitable guaranty is a surety bond, a person may recover from the bond surety the full amount of a claim against the bond principal or, if there is more than one such claim during the term of the bond, a ratable share, up to a maximum total liability of the surety equal to the face amount of the bond; or

(ii) if the suitable guaranty is a letter of credit, a person may recover from the issuing financial institution a claim against the customer named in the credit, or, if there is more than one claim during the term of the letter of credit, a ratable share, up to a maximum total liability of the issuer equal to the face amount of the credit.

(b) Claimants may recover successively on the same suitable guaranty, provided that the total liability on the guaranty to all persons making claims during its term may not exceed the face amount of the guaranty.

(2) In addition to the actual damages suffered by the claimant, the claimant may recover from the proceeds of a suitable guaranty, until depleted, reasonable attorney fees, and court costs incurred by the claimant in collecting the claim.

(3) (a) A claim against a surety or issuer of a suitable guaranty must be filed in writing with the division and the surety or issuer, within one year after the claim arose.

(b) A claim must include a statement of the amount claimed and the basis for the claim.

(c) An action or suit against the surety or issuer of the suitable guaranty must be filed with the court within one year after the claim is filed with the division.

(d) Except as prohibited by division rule, a suitable guaranty may, by contract, alter the obligations under this subsection.

Utah Digital Signature Act

PART 4. Effect of a digital signature

Utah Code §§ 46-3-401 to 46-3-403

46-3-401 Presumptions established by a digital signature.

(1) The presumptions established in this section, Section 46-3-402, and Section 46-3-403 do not apply to a certificate issued by an unlicensed certification authority.

(2) A certificate is presumed to be an acknowledgment of any digital signature verified using the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature in any document, or in relation to the message if:

(a) the certificate is in the repository provided by the division or in a recognized repository; and

(b) the certificate was not revoked, suspended, or expired at the time of signature.

(3) A digital signature verified using a public key is presumed to have been affixed with the intention of the subscriber to authenticate the message and to be bound by the contents of the message if:

(a) the public key is listed in a certificate that is in the repository provided by the division, or a recognized repository; and

(b) the certificate was not revoked, suspended, or expired at the time of signature.

(4) (a) If a signature is time-stamped by the division or a recognized repository, and unless the message otherwise provides, the time-stamp is prima facie evidence that the time-stamped signature took effect as of the date and time indicated in the time-stamp.

(b) This subsection does not preclude a finder of fact from concluding, based on other evidence, that the date and time of signature are other than as shown in a time-stamp of the division or a recognized repository.

(5) The presumptions established in this section may be rebutted:

(a) by evidence indicating that a digital signature cannot be verified by reference to a certificate issued by a licensed certification authority;

(b) by evidence that the rightful holder of the private key by which the digital signature was affixed had lost exclusive control of the private key, without violating any duty imposed by this chapter, at the time when the digital signature was affixed;

(c) by evidence showing a lack of a signature at common law; or

(d) by a showing that reliance on the presumption was not commercially reasonable under the circumstances.

46-3-402 Effect of digital signature.

(1) A digitally signed document is as valid as if it had been written on paper.

(2) This section does not limit the authority of the State Tax Commission to prescribe the form of tax returns or other documents filed with the State Tax Commission.

46-3-403 Digital signatures making instruments payable to bearer.

Notwithstanding any other provisions of this chapter, a digital signature which would make a negotiable instrument payable to bearer is void, unless the digital signature effectuates either a funds transfer within the meaning of Section 70A-4a-104, or a transaction between banks or other financial institutions.

Utah Digital Signature Act

PART 5. State services and reorganized repositories

Utah Code §§ 46-3-501 to 46-3-504

46-3-501 Division duties -- Rulemaking -- Fees.

(1) (a) The division shall be a certification authority, and may issue, suspend, and revoke certificates in the manner prescribed for licensed certification authorities.

(b) The provisions of Part 4 apply to the division with respect to the certificates it issues.

(2) The division shall provide for an on-line, publicly accessible database as a repository containing:

(a) certificates published in the repository by licensed certification authorities;

(b) all orders and advisory statements designated for publication by the division;

(c) certification authority disclosure records for all currently or formerly licensed certification authorities;

(d) notices of suspended or revoked certificates published by licensed certification authorities;

(e) references to recognized repositories;

(f) information required to be kept by a recognized repository; and

(g) other information as determined by division rule.

(3) In conjunction with the repository it provides, the division shall make available a system for reliably time-stamping digital signatures.

(4) The division may promulgate rules consistent with this chapter in order to:

(a) govern licensed certification authorities and their licensure;

(b) approve asymmetric cryptosystems for use in signing certificates issued by licensed certification authorities; and

(c) maintain the database required by Section 46-3-203.

(5) The division's rules shall address at least the following:

(a) design and implementation requirements limiting the equipment and software to fulfill the requirements of this chapter;

(b) validating that the hardware and software to be used are limited to those determined to meet the design and implementation requirements;

(c) suitability of algorithms for use in fulfilling the requirements of this chapter;

(d) the form of suitable guarantees in accordance with Subsection 46-3- 103(34);

(e) items included in certificates issued by licensed certification authorities in accordance with Subsection 46-3-104(2);

(f) approval of persons authorized to audit licensed certification authorities under Section 46-3-202;

(g) the contents of a certification authority disclosure record required in Section 46-3-203;

(h) the termination of certification authority activities under Section 46- 3-206, including the form of notice and required statements; and

(i) prohibitions against altering obligations under Subsection 46-3-309(3).

(6) The division may establish fees for the use of the repository provided for in Subsection (2), for licensing certification authorities, for publishing certificates and other records, and for its other activities required by this chapter.

46-3-502 Recognition of repositories.

(1) The division shall recognize a repository kept by a licensed certification authority, if the division concludes that:

(a) the repository includes a database of certificates substantially similar in content and operation to the repository kept by the division;

(b) the information in the repository appears to be true, accurate, and reasonably reliable;

(c) the repository, its operator, and the certification authorities issuing the certificates in the repository conform to legally binding rules which the division finds to be substantially similar to, or more stringent toward the certificate authorities than those of Utah;

(d) the repository provides a time-stamping service which the division finds to be reasonably trustworthy;

(e) the repository keeps an archive of suspended, revoked, or expired certificates; and

(f) the repository has expressed in writing its intention to continue acting as a repository for the foreseeable future and is able to do so as indicated from its managerial and financial capabilities.

(2) A repository may apply to the division for recognition by filing a written request and providing evidence to the division that the conditions for recognition are satisfied.

(3) The division may withdraw or discontinue recognition of a repository in accordance with the procedures for adjudicative proceedings prescribed by Title 63, Chapter 46b, Administrative Procedures Act, if it concludes that the repository no longer satisfies the conditions for recognition listed in this section.

(4) The division shall publish in its repository the names, addresses, and public keys of all recognized repositories.

46-3-503 Liability of repositories limited.

A recognized repository, the division in providing for a repository, or the division's repository operator is not liable for any loss arising from:

(1) misrepresentation in a certificate published by a licensed certification authority;

(2) accurately recording or reporting information which a licensed certification authority, a county or court clerk, or the

division has published as required by this chapter, including information about suspension or revocation of a certificate;

(3) reporting information about a certification authority, a certificate, or a subscriber, if the information is published as required by this chapter or by division rule, or is published by order of the division in the performance of its licensing and regulatory duties under this chapter; and

(4) failure to record publication of a certificate, suspension, or revocation, unless the repository has received notice of publication and a commercially reasonable time of not more than one business day has elapsed for processing of the publication.

46-3-504 Exemptions.

(1) The following governmental entity records are exempt from Title 63, Chapter 2, Government Records Access and Management Act:

(a) records containing information that would disclose, or might lead to the disclosure of private keys, asymmetric cryptosystems, or algorithms; or

(b) records, the disclosure of which might jeopardize the security of an issued certificate or a certificate to be issued.

(2) For purposes of this section, "record" has the meaning described in Section 63-2-103.

ANEXO III

LEY DE COLOMBIA

LEY 527 DE 1999, POR MEDIO DE LA CUAL SE DEFINE Y REGLAMENTA EL ACCESO Y USO DE LOS MENSAJES DE DATOS, DEL COMERCIO ELECTRÓNICO Y DE LAS FIRMAS DIGITALES, Y SE ESTABLECEN LAS ENTIDADES DE CERTIFICACIÓN Y SE DICTAN OTRAS DISPOSICIONES

Poder Público - Rama Legislativa

LEY 527 DE 1999

(agosto 18)

por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

El Congreso de Colombia

DECRETA:

PARTE I

PARTE GENERAL

CAPITULO I

Disposiciones generales

Artículo 1°. *Ambito de aplicación.* La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Artículo 2°. *Definiciones.* Para los efectos de la presente ley se entenderá por:

a) **Mensaje de datos.** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

b) **Comercio electrónico.** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de

suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

c) **Firma digital.** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) **Entidad de Certificación.** Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

e) **Intercambio Electrónico de Datos (EDI).** La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

f) **Sistema de Información.** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3°. *Interpretación.* En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4°. *Modificación mediante acuerdo.* Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

Artículo 5°. *Reconocimiento jurídico de los mensajes de datos.* No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

CAPITULO II

Aplicación de los requisitos jurídicos de los mensajes de datos

Artículo 6°. *Escrito.* Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Artículo 7°. *Firma.* Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

Artículo 8°. *Original.* Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

Artículo 9°. *Integridad de un mensaje de datos.* Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 10. *Admisibilidad y fuerza probatoria de los mensajes de datos.* Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en

las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

Artículo 11. *Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 12. *Conservación de los mensajes de datos y documentos.* Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y

3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

Artículo 13. *Conservación de mensajes de datos y archivo de documentos a través de terceros.* El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPITULO III

Comunicación de los mensajes de datos

Artículo 14. *Formación y validez de los contratos.* En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Artículo 15. *Reconocimiento de los mensajes de datos por las partes.* En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Artículo 16. *Atribución de un mensaje de datos.* Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador.

2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o

3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 17. *Presunción del origen de un mensaje de datos.* Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o

2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

Artículo 18. *Concordancia del mensaje de datos enviado con el mensaje de datos recibido.* Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, este último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Artículo 19. *Mensajes de datos duplicados.* Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la

debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

Artículo 20. *Acuse de recibo.* Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

Artículo 21. *Presunción de recepción de un mensaje de datos.* Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Artículo 22. *Efectos jurídicos.* Los artículos 20 y 21 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Artículo 23. *Tiempo del envío de un mensaje de datos.* De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

Artículo 24. *Tiempo de la recepción de un mensaje de datos.* De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar:

1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o

2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

Artículo 25. *Lugar del envío y recepción del mensaje de datos.* De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

PARTE II

COMERCIO ELECTRONICO EN MATERIA DE TRANSPORTE DE MERCANCIAS

Artículo 26. *Actos relacionados con los contratos de transporte de mercancías.* Sin perjuicio de lo dispuesto en la parte I de la presente ley, este capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea taxativa:

a) I. Indicación de las marcas, el número, la cantidad o el peso de las mercancías.

II. Declaración de la naturaleza o valor de las mercancías.

III. Emisión de un recibo por las mercancías.

IV. Confirmación de haberse completado el embarque de las mercancías;

b) I. Notificación a alguna persona de las cláusulas y condiciones del contrato.

II. Comunicación de instrucciones al transportador;

c) I. Reclamación de la entrega de las mercancías.

II. Autorización para proceder a la entrega de las mercancías.

III. Notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;

e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;

f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;

g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 27. *Documentos de transporte.* Con sujeción a lo dispuesto en el inciso 3° del presente artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 26 se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El inciso anterior será aplicable, tanto si el requisito en él previsto está expresado en forma de obligación o si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o utilización de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del inciso tercero, el nivel de confiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 26, no será válido ningún documento emitido en papel para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos emitidos en papel. Todo documento con soporte en papel que se emita en esas circunstancias deberá contener una declaración en tal sentido. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento emitido en papel, esa norma no dejará de aplicarse, a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en documentos emitidos en papel.

PARTE III

FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACION

CAPITULO I

Firmas digitales

Artículo 28. *Atributos jurídicos de una firma digital.* Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.

2. Es susceptible de ser verificada.

3. Está bajo el control exclusivo de la persona que la usa.

4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.

5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

CAPITULO II

Entidades de certificación

Artículo 29. *Características y requerimientos de las entidades de certificación.* Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;

b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;

c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

Artículo 30. *Actividades de las entidades de certificación.* Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.

3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.

4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

Artículo 31. *Remuneración por la prestación de servicios.* La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

Artículo 32. *Deberes de las entidades de certificación.* Las entidades de certificación tendrán, entre otros, los siguientes deberes:

a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;

c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;

d) Garantizar la prestación permanente del servicio de entidad de certificación;

e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;

f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;

g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

h) Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;

i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio;

j) Llevar un registro de los certificados.

Artículo 33. *Terminación unilateral.* Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

Artículo 34. *Cesación de actividades por parte de las entidades de certificación.* Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte de la Superintendencia de Industria y Comercio.

CAPITULO III

Certificados

Artículo 35. *Contenido de los certificados.* Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.

2. Identificación del suscriptor nombrado en el certificado.

3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.

4. La clave pública del usuario.

5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.

6. El número de serie del certificado.

7. Fecha de emisión y expiración del certificado.

Artículo 36. *Aceptación de un certificado.* Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

Artículo 37. *Revocación de certificados.* El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

1. Por pérdida de la clave privada.

2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

1. A petición del suscriptor o un tercero en su nombre y representación.

2. Por muerte del suscriptor.

3. Por liquidación del suscriptor en el caso de las personas jurídicas.

4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.

5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.

6. Por el cese de actividades de la entidad de certificación, y

7. Por orden judicial o de entidad administrativa competente.

Artículo 38. *Término de conservación de los registros.* Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

CAPITULO IV

Suscriptores de firmas digitales

Artículo 39. *Deberes de los suscriptores.* Son deberes de los suscriptores:

1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.

2. Suministrar la información que requiera la entidad de certificación.

3. Mantener el control de la firma digital.

4. Solicitar oportunamente la revocación de los certificados.

Artículo 40. *Responsabilidad de los suscriptores.* Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

CAPITULO V

Superintendencia de Industria y Comercio

Artículo 41. *Funciones de la Superintendencia.* La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones:

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.

2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.

3. Realizar visitas de auditoría a las entidades de certificación.

4. Revocar o suspender la autorización para operar como entidad de certificación.

5. Solicitar la información pertinente para el ejercicio de sus funciones.

6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.

8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.

9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.

10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.

11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

Artículo 42. *Sanciones.* La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

1. Amonestación.

2. Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora.

4. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.

5. Revocar definitivamente la autorización para operar como entidad de certificación.

CAPITULO VI

Disposiciones varias

Artículo 43. *Certificaciones recíprocas.* Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Artículo 44. *Incorporación por remisión.* Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

PARTE IV

REGLAMENTACION Y VIGENCIA

Artículo 45. La Superintendencia de Industria y Comercio contará con un término adicional de doce (12) meses, contados a partir de la publicación de la presente ley, para organizar y asignar a una de sus dependencias la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella para tal efecto.

Artículo 46. *Prevalencia de las leyes de protección al consumidor.* La presente ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

Artículo 47. *Vigencia y derogatoria.* La presente ley rige desde la fecha de su publicación y deroga las disposiciones que le sean contrarias.

El Presidente del honorable Senado de la República,

Fabio Valencia Cossio.

El Secretario General del honorable Senado de la República,

Manuel Enríquez Rosero.

El Presidente de la honorable Cámara de Representantes,

Emilio Martínez Rosales.

El Secretario General de la honorable Cámara de Representantes,

Gustavo Bustamante Moratto.

REPUBLICA DE COLOMBIA – GOBIERNO NACIONAL

Publíquese y ejecútese.

Dada en Santa Fe de Bogotá, D. C., a 18 de agosto de 1999.

ANDRES PASTRANA ARANGO

El Ministro de Desarrollo Económico,

Fernando Araújo Perdomo.

La Ministra de Comercio Exterior,

Martha Lucía Ramírez de Rincón.

La Ministra de Comunicaciones,

Claudia De Francisco Zambrano.

El Ministro de Transporte,

Mauricio Cárdenas Santamaría.

ANEXO IV

LEY DE PERÚ

LEY No. 27269, LEY DE FIRMAS Y CERTIFICADOS DIGITALES

LEY Nº 27269

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE FIRMAS Y CERTIFICADOS DIGITALES

Artículo 1°.- Objeto de la ley
La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 2°.- Ámbito de aplicación
La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

DE LA FIRMA DIGITAL

Artículo 3°.- Firma digital
La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

DEL TITULAR DE LA FIRMA DIGITAL

Artículo 4°.- Titular de la firma digital
El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5°.- Obligaciones del titular de la firma digital
El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

DE LOS CERTIFICADOS DIGITALES

Artículo 6°.- Certificado digital
El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Artículo 7°.- Contenido del certificado digital
Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación.

Artículo 8°.- Confidencialidad de la información
La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley.

Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9°.- Cancelación del certificado digital
La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital.
2. Por revocatoria de la entidad certificante.
3. Por expiración del plazo de vigencia.
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10°.- Revocación del certificado digital
La Entidad de Certificación revocará el certificado digital en los siguientes casos:

1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

Artículo 11°.- Reconocimiento de certificados emitidos por entidades extranjeras
Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

DE LAS ENTIDADES DE CERTIFICACIÓN Y DE REGISTRO

Artículo 12°.- Entidad de Certificación
La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.

Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.

Artículo 13°.- Entidad de Registro o Verificación
La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14°.- Depósito de los Certificados Digitales

Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley.

El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización.

A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.

Artículo 15°.- Inscripción de Entidades de Certificación y de Registro o Verificación

El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.

La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales.

Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

Artículo 16°.- Reglamentación

El Poder Ejecutivo reglamentará la presente ley en un plazo de 60 (sesenta) días calendario, contados a partir de la vigencia de la presente ley.

DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES

Primera.- Mientras se cree el Registro señalado en el Artículo 15°, la validez de los actos celebrados por Entidades de Certificación y Entidades de Registro o Verificación, en el ámbito de la presente ley, está condicionada a la inscripción respectiva dentro de los 45 (cuarenta y cinco) días siguientes a la creación el referido Registro.

Segunda.- El Reglamento de la presente ley incluirá un glosario de términos referidos a esta ley y a las firmas electrónicas en general, observando las definiciones establecidas por los organismos internacionales de los que el Perú es parte.

Tercera.- La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los ocho días del mes de mayo del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO
Presidenta del Congreso de la República

RICARDO MARCENARO FRERS
Primer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL
DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de mayo del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y
Ministro de Justicia

LEY Nº 27310

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;
Ha dado la Ley siguiente:

LEY QUE MODIFICA EL ARTÍCULO 11º DE LA LEY Nº 27269

Artículo Único.- Objeto de la ley
Modifícase el Artículo 11° de la Ley N° 27269, el mismo que quedará redactado de la siguiente manera:

"**Artículo 11°.-** Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente."

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiséis días del mes de junio del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO
Presidenta del Congreso de la República

LUIS DELGADO APARICIO
Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los quince días del mes de julio del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y
Ministro de Justicia

ANEXO V

LEY DE CHILE

LEY SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LOS SERVICIOS DE DICHA FIRMA

Chile.

"Ley sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma."

TITULO I DISPOSICIONES GENERALES

Artículo 1°.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.

Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel. Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.

Artículo 2°.- Para los efectos de esta ley se entenderá por:

a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;

c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;

d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;

e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción;

f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;

g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y

h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica.

Artículo 3°.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los

mismos consten por escrito, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan por escrito. Lo dispuesto en el inciso anterior no será aplicable a los actos y contratos otorgados o celebrados en los casos siguientes:

a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;

b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes; y,

c) Aquellos relativos al derecho de familia.

La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en el artículo siguiente.
Artículo 4°.- Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.
Artículo 5°.- Los documentos electrónicos podrán presentarse en juicio y, en el evento de que sean usados como medio de prueba, habrán de seguirse las reglas siguientes:

1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales; y

2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el numeral anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.
TITULO II USO DE FIRMAS ELECTRÓNICAS POR LOS ORGANOS DEL ESTADO
Artículo 6°.- Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. Se exceptúan aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

Lo dispuesto en este título no se aplicará a las empresas públicas creadas por ley, las que se regirán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares.
Artículo 7°.- Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel. Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada.
Artículo 8°.- Las personas podrán relacionarse con los órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos.

Los órganos del Estado deberán evitar, al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias.
Artículo 9°.- La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos del Estado se realizará por los respectivos ministros de fe. Si éste

no se encontrare establecido en la ley, el reglamento a que se refiere el artículo 10 indicará la forma en que se designará un funcionario para estos efectos. Dicha certificación deberá contener, además de las menciones que corresponda, la fecha y hora de la emisión del documento. Los efectos probatorios de la certificación practicada por el ministro de fe competente serán equivalentes a los de la certificación realizadas por un prestador acreditado de servicios de certificación. Sin perjuicio de lo dispuesto en el inciso primero, los órganos del Estado podrán contratar los servicios de certificación de firmas electrónicas con entidades certificadoras acreditadas, si ello resultare más conveniente, técnica o económicamente, en las condiciones que señale el respectivo reglamento.
Artículo 10.- Los reglamentos aplicables a los correspondientes órganos del Estado regularán la forma cómo se garantizará la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas de este Título.".
TITULO III DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN
Artículo 11.- Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Asimismo, son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad al Título V de esta ley, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.
Artículo 12.- Son obligaciones del prestador de servicios de certificación de firma electrónica:

a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano;

b) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N° 19.628, sobre Protección de la Vida Privada;

c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;

d) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

e) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente,

ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;

f) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos, y

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes N° 19.496, sobre Protección de los Derechos de los Consumidores y N° 19.628, sobre Protección de la Vida Privada.

Artículo 13.- El cumplimiento, por parte de los prestadores no acreditados de servicios de certificación de firma electrónica, de las obligaciones señaladas en las letras a), b), c) y j) del artículo anterior, será considerado por el juez como un antecedente para determinar si existió la debida diligencia, para los efectos previstos en el inciso primero del artículo siguiente

Artículo 14.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia. Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica. Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquéllos homologados en virtud de lo dispuesto en el inciso final del artículo 15. El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado. En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.

TITULO IV DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Artículo 15.- Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:

a) Un código de identificación único del certificado;

b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;

c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y

d) Su plazo de vigencia. Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente.
Artículo 16.- Los certificados de firma electrónica quedarán sin efecto, en los siguientes casos:

1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;

2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:

a) A solicitud del titular del certificado;

b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;

c) Por resolución judicial ejecutoriada, o d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 24;

3) Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados que señala el artículo 18, en razón de lo dispuesto en el artículo 19 o del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) y h) del artículo 12; y,

4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 12.

La revocación de un certificado en las circunstancias de la letra d) del número 2) de este artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador. El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.
TITULO V DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 17.- La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento, permitiendo su inscripción en el registro que se señala en el artículo 18. Para ser acreditado, el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:

a) Demostrar la fiabilidad necesaria de sus servicios;

b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;

c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;

d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;

e) Haber contratado un seguro apropiado en los términos que señala el artículo 14; y,

f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

Artículo 18.- El procedimiento de acreditación se iniciará mediante solicitud ante la Entidad Acreditadora, a la que se deberá acompañar los antecedentes relativos a los requisitos del artículo 17 que señale el reglamento y el comprobante de pago de los costos de la acreditación. La Entidad Acreditadora deberá resolver fundadamente sobre la solicitud en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse. Si el interesado denunciare el incumplimiento de ese plazo ante la propia autoridad y ésta no se pronunciare dentro del mes siguiente, la solicitud se entenderá aceptada. La Entidad Acreditadora podrá contratar expertos con el fin de verificar el cumplimiento de los requisitos señalados en el artículo 17.

Otorgada la acreditación, el prestador será inscrito en un registro público que a tal efecto llevará la Entidad Acreditadora, al que se podrá acceder por medios electrónicos. Durante la vigencia de su inscripción en el registro, el prestador acreditado deberá informar a la Entidad Acreditadora cualquier modificación de las condiciones que permitieron su acreditación.

Artículo 19 .- Mediante resolución fundada de la Entidad Acreditadora se podrá dejar sin efecto la acreditación y cancelar la inscripción en el registro señalado en el artículo 18, por alguna de las siguientes causas:

a) Solicitud del prestador acreditado;

b) Pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o peritos que la Entidad Acreditadora ocupe en la inspección a que se refiere el artículo 20; y,

c) Incumplimiento grave o reiterado de las obligaciones que establece esta ley y su reglamento. En los casos de las letras b) y c), la resolución será adoptada previa audiencia del afectado y se podrá reclamar de ella ante el Ministro de Economía, Fomento y Reconstrucción, dentro del plazo de cinco días contados desde su notificación. El Ministro

tendrá un plazo de treinta días para resolver. Dentro de los diez días siguientes a la fecha en que se notifique la resolución que éste dicte o, en su caso, desde que se certifique que la reclamación administrativa no fue resuelta dentro de plazo, el interesado podrá interponer reclamación jurisdiccional, para ante la Corte de Apelaciones de su domicilio. La reclamación deberá ser fundada y para su agregación a la tabla, vista y fallo, se regirá por las normas aplicables al recurso de protección. La resolución de la Corte de Apelaciones no será susceptible de recurso alguno.

Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de firmas electrónicas certificadas por ellos. Sin perjuicio de ello, la Entidad Acreditadora publicará un aviso dando cuenta de la cancelación, a costa del certificador. A partir de la fecha de esta publicación, quedarán sin efecto los certificados, a menos que los datos de los titulares sean transferidos a otro certificador acreditado, en conformidad con lo dispuesto en la letra h) del artículo 12. Los perjuicios que pueda causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador.
Artículo 20.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Entidad Acreditadora ejercerá la facultad inspectora sobre los mismos y podrá, a tal efecto, requerir información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados, de conformidad al reglamento.
Artículo 21.- La Entidad Acreditadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los certificadores acreditados.
Artículo 22.- Los recursos que perciba la Entidad Acreditadora por parte de los prestadores acreditados de servicios de certificación constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.
TITULO VI DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE FIRMAS ELECTRÓNICAS
Artículo 23.- Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:

1°. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar;

2°.A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos;

3°. A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se convinieren;

4°. A que el prestador de servicios o quien homologue sus certificados le proporcionen la información sobre sus domicilios en Chile y sobre todos los medios a los que el usuario pueda

acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

5°. A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 4) del artículo 16 de la presente ley, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

6°. A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 3) del artículo 16 de la presente ley, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

7°. A traspasar sus datos a otro prestador de servicios de certificación;

8°. A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;

9°. A acceder, por medios electrónicos, al registro de prestadores acreditados que mantendrá la Entidad Acreditadora, y

10°. A ser indemnizado y hacer valer los seguros comprometidos, en conformidad con el artículo 15 de la presente ley. Los usuarios gozarán de estos derechos, sin perjuicio de aquellos que deriven de la Ley N° 19.628, sobre Protección de la Vida Privada y de la Ley N° 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10° de este artículo, ejercerlos conforme al procedimiento establecido en esa última normativa.

Artículo 24.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

TITULO VII REGLAMENTOS

Artículo 25.- El Presidente de la República reglamentará esta ley en el plazo de noventa días contados desde su publicación, mediante uno o más decretos supremos del Ministerio de Economía, Fomento y Reconstrucción, suscritos también por los Ministros de Transportes y Telecomunicaciones y Secretario General de la Presidencia. Lo anterior es sin perjuicio de los demás reglamentos que corresponda aprobar, para dar cumplimiento a lo previsto en el artículo 10.

Artículo transitorio.- El mayor gasto que irrogue a la Subsecretaría de Economía, Fomento y Reconstrucción las funciones que le asigna esta ley, durante el año 2002, se financiará con los recursos consultados en su presupuesto.

ANEXO VI

LEY DE ARGENTINA

LEY FIRMA DIGITAL

A.1.1.1. Ley 25.506. B.O. 14/12/01.
Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoria. Comisión Asesora para la infraestructura de firma digital. Responsabilidad. Sanciones. Disposiciones complementarias.
Sancionada: Noviembre 14 de 2001.
Promulgada de Hecho: Diciembre 11 de 2001.

LEY FIRMA DIGITAL

CAPITULO I
CONSIDERACIONES GENERALES

ARTICULO 1°.- Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTICULO 2°.- Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.
Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3°.- Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4°.- Exclusiones. Las disposiciones de esta ley no son aplicables:
a) a las disposiciones por causa de muerte;
b) a los actos jurídicos del derecho de familia;
c) a los actos personalísimos en general;
d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTICULO 5°.- Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6°.- Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7°.- Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8°.- Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9°.- Validez. Una firma digital es válida si cumple con los siguientes requisitos:
a) haber sido creada durante el periodo de vigencia del certificado digital válido del firmante;
b) ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
c) que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTICULO 10°.- Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11.- Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12.- Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permita determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/ o recepción.

CAPITULO II
DE LOS CERTIFICADOS DIGITALES

ARTICULO 13.- Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14.- Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:
a) Ser emitidos por un certificador licenciado por el Ente Licenciante;
b) Responder a formatos estándares reconocidos internacionalmente fijados por la Autoridad de Aplicación y contener, como mínimo, los datos que permitan:
1. identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
2. ser susceptible de verificación respecto de su estado de revocación;
3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
4. contemplar la información necesaria para la verificación de la firma;

5. identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15.- Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o con su revocación si fuere revocado.
La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.
La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16.- Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:
a) reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República argentina y el país de origen del certificador extranjero, o;
b) tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la Autoridad de Aplicación.

CAPITULO III
DEL CERTIFICADOR LICENCIADO

ARTICULO 17.- Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados y presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.
La actividad de los certificadores licenciados no pertenecientes al Sector Público se prestará en régimen de competencia. El arancel de los servicios prestados por los Certificadores Licenciados será establecido libremente por éstos.

ARTÍCULO 18.- Certificados por profesión. Las entidades que controlan la matricula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19.- Funciones. El certificador licenciado tiene las siguientes funciones:
a) recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;
b) emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la Autoridad de Aplicación indique en la reglamentación de la presente ley;
c) identificar inequívocamente los certificados digitales emitidos;
d) mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;
e) revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1. a solicitud del titular del certificado digital
2. si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación;
3. si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguro;
4. por condiciones especiales definidas en su política de certificación.
5. por resolución judicial o de la Autoridad de Aplicación.
f) informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20.- Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el Ente Licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21.- Obligaciones. Son obligaciones del certificador licenciado:
a) informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el Ente Licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;
c) mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
d) operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la Autoridad de Aplicación;
e) notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable y de las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
f) recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
g) mantener la confidencialidad de toda información que no figure en el certificado digital;
h) poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
i) mantener la documentación respaldatoria de los certificados digitales emitidos, por DIEZ (10) años a partir de su fecha de vencimiento o revocación;
j) incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la Autoridad de Aplicación;
k) publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la Autoridad de Aplicación;

l) publicar en el Boletín Oficial aquellos datos que la Autoridad de Aplicación determine;
m) registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
n) informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
o) verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
p) solicitar inmediatamente al Ente Licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenida haya dejado de ser seguro;
q) informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos relativos a su licencia;
r) permitir el ingreso de los funcionarios autorizados de la Autoridad de Aplicación, del Ente Licenciante o de los auditores, a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
s) emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
t) someter a aprobación del Ente Licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
u) constituir domicilio legal en la República Argentina;
v) disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
w) cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el Ente Licenciante.

ARTICULO 22.- Cese del certificador. El certificador licenciado cesa en tal calidad:
a) por decisión unilateral comunicada al Ente Licenciante;
b) por cancelación de su personería jurídica;
c) por cancelación de su licencia dispuesta por el Ente Licenciante.
La Autoridad de Aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23.- Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:
a) para alguna finalidad diferente a los fines para los cuales fue extendido;
b) para operaciones que superen el valor máximo autorizado cuando corresponda;
c) una vez revocado.

CAPITULO IV
DEL TITULAR DE UN CERTIFICADO DIGITAL

ARTICULO 24.- Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

a) a ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) a que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
c) a ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;
d) a que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;
e) a que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25.- Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:
a) mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) utilizar un dispositivo de creación de firma digital técnicamente confiable;
c) solicitar la revocación de su certificado al Certificador Licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V
DE LA ORGANIZACIÓN INSTITUCIONAL

ARTICULO 26- Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocido, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27.- Sistema de Auditoria. La Autoridad de Aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoria para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciante.

ARTICULO 28.- Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

CAPÍTULO VI
DE LA AUTORIDAD DE APLICACIÓN

ARTICULO 29.- Autoridad de Aplicación. La Autoridad de Aplicación de la presente ley será la JEFATURA DE GABINETE DE MINISTROS

ARTICULO 30.- Funciones. La Autoridad de Aplicación tiene las siguientes funciones:
a) dictar las normas reglamentarias y de aplicación de la presente;
b) establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;
c) determinar los efectos de la revocación de los certificados de los certificadores licenciados o del Ente Licenciante;
d) instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;
e) determinar las pautas de auditoria, incluyendo los dictámenes tipo que deba emitirse como conclusión de las revisiones;
f) actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;
g) determinar los niveles de licenciamiento.
h) otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;
i) fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;
j) homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;
k) aplicar las sanciones previstas en la presente ley;

ARTICULO 31.- Obligaciones. En su calidad de titular de certificado digital, la Autoridad de Aplicación tiene las mismas obligaciones que los titulares de certificados y que los Certificadores Licenciados. En especial y en particular debe:
a) abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los Certificadores Licenciados;
b) mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;
c) revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;
d) publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;
e) supervisar la ejecución del plan de cese de actividades de los Certificadores Licenciados que discontinúan sus funciones;

ARTICULO 32.- Arancelamiento. La Autoridad de Aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y de las auditorias realizadas por sí o por terceros contratados a tal efecto.

CAPÍTULO VII
DEL SISTEMA DE AUDITORÍA

ARTICULO 33.- Sujetos a auditar. El Ente Licenciante y los Certificadores Licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoria que diseñe y apruebe la Autoridad de Aplicación.

La Autoridad de Aplicación podrá implementar el sistema de auditoria por sí o por terceros habilitados a tal efecto. Las auditorias deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciante.

ARTICULO 34.- Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorias las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia.

CAPÍTULO VIII
DE LA COMISIÓN ASESORA PARA
LA INFRAESTRUCTURA DE FIRMA DIGITAL

ARTICULO 35.- Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado Nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de Profesionales.
Los integrantes serán designados por el Poder Ejecutivo Nacional por un período de cinco (5) años renovables por única vez.
Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la Autoridad de Aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.
Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la Autoridad de Aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36.- Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la Autoridad de Aplicación, sobre los siguientes aspectos:
a) estándares tecnológicos;
b) sistema de registro de toda la información relativa a la emisión de certificados digitales;
c) requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
d) metodología y requerimiento del resguardo físico de la información;
e) otros que le sean requeridos por la Autoridad de Aplicación.

CAPITULO IX
RESPONSABILIDAD

ARTICULO 37.- Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley y demás legislación vigente.

ARTICULO 38.- Responsabilidad de los certificadores licenciados ante terceros.
El Certificador que emita un Certificado Digital, o lo reconozca en los términos del art. 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de la ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma cuando así

correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio, demostrar que actuó con la debida diligencia.

ARTICULO 39.- Limitaciones de responsabilidad. Los Certificadores Licenciados no son responsables en los siguientes casos:
a) por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;
b) por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X
SANCIONES

ARTICULO 40.- Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley será realizada por el Ente Licenciante. Es aplicable la Ley de Procedimientos Administrativos N° 19.549 y sus normas reglamentarias.

ARTICULO 41.- Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:
a) apercibimiento;
b) multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);
c) caducidad de la licencia.
Su gradación según reincidencia y/u oportunidad será establecida por la reglamentación.
El pago de la sanción que aplique el Ente Licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42.- Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:
a) emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;
b) no facilitar los datos requeridos por el Ente Licenciante en ejercicio de sus funciones;
c) cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43.- Multa. Podrá aplicarse sanción de multa en los siguientes casos:
a) incumplimiento de las obligaciones previstas en el artículo 21;
b) si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causaren perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;
c) omisión de llevar el registro de los certificados expedidos;
d) omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

e) cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la Autoridad de Aplicación y del Ente Licenciante;
f) incumplimiento a las normas dictadas por la Autoridad de Aplicación;
g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento;

ARTICULO 44.- Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:
a) no tomar los debidos recaudos de seguridad en los servicios de certificación;
b) expedición de certificados falsos;
c) transferencia no autorizada o fraude en la titularidad de la licencia;
d) reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;
e) quiebra del titular.
La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45.- Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los tribunales federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.
La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46.- Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso Administrativo Federal.

CAPITULO XI
DISPOSICIONES COMPLEMENTARIAS

ARTICULO 47.- Utilización por el Estado Nacional. El Estado Nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus Poderes.

ARTICULO 48.- Implementación. El Estado Nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8 de la Ley N° 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.
En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley N° 24.156.

ARTICULO 49.- Reglamentación. El Poder Ejecutivo Nacional deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50.- Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTICULO 51.- Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como art. 78 (bis) del Código Penal: "Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente."

ARTICULO 52.- Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo Nacional para que por la vía del artículo 99 inciso 2 de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53.- Comuníquese al PODER EJECUTIVO NACIONAL.

ANEXO

INFORMACIÓN: conocimiento adquirido acerca de algo o alguien.

PROCEDIMIENTO DE VERIFICACIÓN: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

a) que dicha firma digital ha sido creada durante el periodo de validez del certificado digital del firmante;

b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;

c) la verificación de la autenticidad y la validez de los certificados involucrados.

DATOS DE CREACION DE FIRMA DIGITAL: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

DATOS DE VERIFICACION DE FIRMA DIGITAL: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

DISPOSITIVO DE CREACION DE FIRMA DIGITAL: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

DISPOSITIVO DE VERIFICACIÓN DE FIRMA DIGITAL: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

POLITICAS DE CERTIFICACIÓN: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

TECNICAMENTE CONFIABLE: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad, y procedimientos administrativos relacionados, que cumpla los siguientes requisitos:

1. resguardar contra la posibilidad de intrusión y/o de uso no autorizado;
2. asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
3. ser apto para el desempeño de sus funciones específicas;
4. cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;
5. cumplir con los estándares técnicos y de auditoria que establezca la Autoridad de Aplicación.

CLAVE CRIPTOGRÁFICA PRIVADA: En un criptosistema asimétrico, es aquella que se utiliza para firmar digitalmente.

CLAVE CRIPTOGRÁFICA PÚBLICA: En un criptosistema asimétrico, es aquella que se utiliza para verificar una firma digital.

INTEGRIDAD: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.
CRIPTOSISTEMA ASIMÉTRICO: Algoritmo que utiliza un "par de claves", una "clave privada" para firmar digitalmente y su correspondiente "clave pública" para verificar dicha "firma digital".

ANEXO VII

LEY DE ITALIA

LEGGE 15 MARZO 1997, N. 59 DELEGA AL GOVERNO PER IL CONFERIMENTO DI FUNZIONI E COMPITI ALLE REGIÓN ED ENTI LOCALI, PER LA RIFORMA DELLA PUBBLICA ADMINISTRAZIONE E PER LA SEMPLIFICAZIONE AMMINISTRATIVA

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 10 NOVEMBRE 1997, N. 513 REGOLAMENTO RECANTE CRITERI E MODALITÀ PER LA FORMAZIONE, L'ARCHIVIAZIONE E LA TRASMISSIONE DI DOCUMENTI CON STRUMENTI INFORMATICI E TELEMATICI, A NORMA DELL'ARTICOLO 15, COMMA 2, DELLA LEGGE 15 MARZO 1997, N.59

Legge 15 marzo 1997, n. 59 (in Suppl. ordinario n. 56/L, alla Gazz. Uff. n. 63, del 17 marzo).

Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa.

Capo II

Art. 15.

1. Al fine della realizzazione della rete unitaria delle pubbliche amministrazioni, l'Autorità per l'informatica nella pubblica amministrazione è incaricata, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, di stipulare, nel rispetto delle vigenti norme in materia di scelta del contraente, uno o più contratti-quadro con cui i prestatori dei servizi e delle forniture relativi al trasporto dei dati e all'interoperabilità si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite. Le amministrazioni di cui all'art. 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, in relazione alle proprie esigenze, sono tenute a stipulare gli atti esecutivi dei predetti contratti-quadro. Gli atti esecutivi non sono soggetti al parere dell'Autorità per l'informatica nella pubblica amministrazione e, ove previsto, del Consiglio di Stato. Le amministrazioni non ricomprese tra quelle di cui all'art. 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, hanno facoltà di stipulare gli atti esecutivi di cui al presente comma.

2. Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'art. 17, comma 2, della legge 23 agosto1988, n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni.

- Carta d'identità
- Elenco Certificatori
- Euro
- Formazione
- Monitoraggio e verifiche
- Osservatorio del mercato
- Osservatorio della spesa
- Pareri
- Pianificazione
- Progetti intersettoriali
- Protocollo informatico
- Relazioni Annuali
- Rete Unitaria
- Scenari internazionali
- Standard e Metodologie

Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Gazz. Uff. n. 60 del 13 marzo 1998)

Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59.

Normativa

- Leggi e decreti
- Circolari, delibere raccomandazioni
- T.U.documentazic amministrativa

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87 della Costituzione;

Visto l'articolo 17, comma 2, della legge 23 agosto 1988 n. 400;

Visto l'articolo 15, comma 2, della legge 15 marzo 1997 n. 59;

Visto il decreto legislativo 12 febbraio 1993, n.39;

Sentito il Garante per la protezione dei dati personali;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 5 agosto 1997;

Acquisiti i pareri delle commissioni permanenti della Camera dei deputati e del Senato della Repubblica;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 20 ottobre 1997;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 31 ottobre 1997;

Sulla proposta del Presidente del Consiglio dei Ministri e del Ministro per la funzione pubblica e gli affari regionali, di concerto con il Ministro di grazia e giustizia;

EMANA

il seguente regolamento:

Capo I - PRINCIPI GENERALI

Art. 1.

(Definizioni)

1. Ai fini del presente regolamento s'intende:

a. per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

b. per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

c. per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;

d. per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici;

e. per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.

f. per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;

g. per chiave biometrica, la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente;

h. per certificazione, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;

i. per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;

j. per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;

k. per certificatore, il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;

l. per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;

m. per sospensione del certificato, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;

n. per validità del certificato, l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti;

o. per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.

Art. 2.

(Documento informatico)

1. Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.

Art. 3

(Requisiti del documento informatico)

1. Con decreto del Presidente del Consiglio dei Ministri, da emanare entro 180 giorni dall'entrata in vigore del presente regolamento, sentita l'Autorità per l'informatica nella pubblica amministrazione sono fissate le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

2. Le regole tecniche indicate al comma 1 sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con decorrenza almeno biennale a decorrere dall'entrata in vigore del presente regolamento.

3. Con il decreto di cui al comma 1 sono altresì dettate le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all'eventuale uso di chiavi biometriche.

5. Resta fermo quanto previsto dall'articolo 15 della legge 31 dicembre 1996, n.675.

Art. 4.

(Forma scritta)

1. Il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta.

2. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro delle finanze.

Art. 5.

(Efficacia probatoria del documento informatico)

1. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.

2. Il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

Art.6.

(Copie di atti e documenti)

1. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.

2. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente regolamento.

3. Le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3.

4. La spedizione o il rilascio di copie di atti e documenti di cui al comma 2 esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

5. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai

sensi dell'articolo 3.

Art. 7

(Deposito della chiave privata)

1. Il titolare della coppia di chiavi asimmetriche può ottenere il deposito in forma segreta della chiave privata presso un notaio o altro pubblico depositario autorizzato.

2. La chiave privata di cui si richiede il deposito può essere registrata su qualsiasi tipo di supporto idoneo a cura del depositante e dev'essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni.

3. Le modalità del deposito sono regolate dalle disposizioni dell'articolo 605 del codice civile, in quanto applicabili.

Art.8.

(Certificazione)

1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti di cui all'articolo 2 deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione.

2. Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro validità, sono consultabili in forma telematica.

3. Salvo quanto previsto dall'articolo 17, le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all'articolo 3:

a. forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;

b. possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;

c. affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 3;

d. qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

4. La procedura di certificazione di cui al comma 1 può essere svolta anche da un certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione europea o dello Spazio economico europeo, sulla base di equivalenti requisiti.

Art. 9.

(Obblighi dell'utente e del certificatore)

1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

2. Il certificatore è tenuto a:

a. identificare con certezza la persona che fa richiesta della certificazione;

b. rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 3;

c. specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;

d. attenersi alle regole tecniche di cui all'articolo 3;

e. informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;

f. attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675;

g. non rendersi depositario di chiavi private;

h. procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare , di sospetti abusi o falsificazioni;

i. dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche;

j. dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento.

CAPO II

FIRMA DIGITALE

Art. 10

(Firma digitale)

1. A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale.

2. L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.

3. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

4. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata.

5. L'uso della firma digitale apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

6. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

7. Attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche definiti con il decreto di cui all'articolo 3, gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.

Art. 11

(*Contratti stipulati con strumenti informatici o per via telematica*)

1. I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge.

2. Ai contratti indicati al comma 1 si applicano le disposizioni previste dal decreto legislativo 15 gennaio 1992, n.50.

Art. 12

(Trasmissione del documento)

1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.

2. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente regolamento e alle regole tecniche di cui all'articolo 3, sono opponibili ai terzi.

3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

ART. 13

(Segretezza della corrispondenza trasmessa per via telematica)

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2. Agli effetti del presente regolamento, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

3. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dall'Autorità per l'informatica nella pubblica amministrazione, d'intesa con l'amministrazione degli archivi di Stato e, per il materiale classificato, con le Amministrazioni della difesa, dell'interno e delle finanze, rispettivamente competenti.

ART. 14

(Pagamenti informatici)

1. Il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e

tra queste e soggetti privati è effettuato secondo le regole tecniche definite col decreto di cui all'articolo 3.

Art.15

(Libri e scritture)

1. I libri, i repertori e le scritture, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente regolamento e secondo le regole tecniche definite col decreto di cui all'articolo 3.

Art.16

(Firma digitale autenticata)

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato.

2. L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, numero 1, della legge 16 febbraio 1913, n. 89 .

3. L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 6 del presente regolamento.

5. Ai fini e per gli effetti dell'articolo 3, comma 11, della legge 15 maggio 1997, n. 127, si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni.

6. La presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione sono validi a tutti gli effetti di legge se vi sono apposte la firma digitale e la validazione temporale a norma del presente regolamento.

Art. 17

(Chiavi di cifratura della pubblica amministrazione)

1. Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza.

2. Col decreto di cui all'articolo 3 sono disciplinate le modalità di formazione, di pubblicità, di conservazione, certificazione e di utilizzo delle chiavi pubbliche delle pubbliche amministrazioni.

3. Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente, in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici.

4. Le chiavi pubbliche di Ordini ed Albi professionali legalmente riconosciuti e dei

loro legali rappresentanti sono certificate e pubblicate a cura del Ministro di Grazia e Giustizia o suoi delegati.

Art. 18

(Documenti informatici delle pubbliche amministrazioni)

1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

2. Nelle operazioni riguardanti le attività di produzione, immissione, archiviazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate sia il soggetto che ha effettuato l'operazione.

3. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dall'Autorità per l'informatica nella pubblica amministrazione d'intesa con l'amministrazione degli archivi di Stato.

Art. 19

(Sottoscrizione dei documenti informatici delle pubbliche amministrazioni)

1. In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa, o la sottoscrizione comunque prevista, è sostituita dalla firma digitale, in conformità alle norme del presente regolamento.

2. L'uso della firma digitale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

CAPO III

NORME DI ATTUAZIONE

Art. 20

(Sviluppo dei sistemi informativi delle pubbliche amministrazioni)

1. Entro il 31 marzo 1998 le pubbliche amministrazioni adottano un piano di sviluppo dei sistemi informativi automatizzati in attuazione delle disposizioni del presente regolamento e secondo le norme tecniche definite dall'Autorità per l'informatica nella pubblica amministrazione.

2. Le pubbliche amministrazioni provvedono, entro 5 anni, a partire dal 1 gennaio 1998, a realizzare o revisionare sistemi informativi finalizzati alla totale automazione delle fasi di produzione, gestione, diffusione ed utilizzazione dei propri dati, documenti, procedimenti ed atti in conformità alle disposizioni del presente regolamento ed alle disposizioni di cui alle leggi 31 dicembre 1996, nn. 675 e 676.

3. Entro il 31 dicembre 1998, le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia opportuna od obbligatoria la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici.

Art.21

(Gestione informatica del flusso documentale)

1. Entro il 31 dicembre 1998 le pubbliche amministrazioni dispongono per la tenuta del protocollo amministrativo e per la gestione dei documenti con procedura informatica al fine di consentire il reperimento immediato, la disponibilità degli atti archiviati e l'accesso ai documenti amministrativi per via telematica tra pubbliche amministrazioni e tra queste ed i soggetti privati aventi diritto.

ART. 22

(Formulari, moduli e questionari.)

1. Entro il 31 dicembre 1998 le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge per l'interscambio dei dati nell'ambito della rete unitaria e con i soggetti privati.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella *Raccolta ufficiale* degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo o di farlo osservare.

ANEXO VIII

LEY DE ALEMANIA

GESETZ ZUR REGELUNG DER RAHMENBEDINGUNGEN FÜR INFORMATIONS- UND KOMMUNIKATIONSDIENSTE (INFORMATIONS- UND KOMMUNIKATIONSDIENSTE-GESETZ - IuKDG) IN DER FASSUNG DES BESCHLUSSES DES DEUTSCHEN BUNDESTAGES VOM 13. JUNI 1997

VERORDNUNG ZUR DIGITALEN SIGNATUR (SIGNATURVERORDNUNG - SigV) IN DER FASSUNG DES BESCHLUSSES DER BUNDESREGIERUNG VOM 8. OKTOBER 1997

Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste

(Informations- und Kommunikationsdienste-Gesetz - IuKDG)

in der Fassung des Beschlusses des Deutschen Bundestages vom 13. Juni 1997

Änderungen gegenüber der Fassung vom 11. Dezember 1996 sind im Text blau markiert.
Für die Vollständigkeit und Richtigkeit des Gesetzestextes wird keine Gewähr übernommen

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht:

Artikel 1
Gesetz über die Nutzung von Telediensten
(Teledienstegesetz - TDG)

§ 1 Zweck des Gesetzes

Zweck des Gesetzes ist es, einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen.

§ 2 Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

(2) Teledienste im Sinne von Absatz 1 sind insbesondere:

1. Angebote im Bereich der Individualkommunikation (zum Beispiel Telebanking, Datenaustausch),
2. Angebote zur Information oder Kommunikation soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),
3. Angebote zur Nutzung des Internets oder weiterer Netze,
4. Angebote zur Nutzung von Telespielen,
5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.

(3) Absatz 1 gilt unabhängig davon, ob die Nutzung der Teledienste ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist.

(4) Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120),
2. Rundfunk im Sinne des § 2 des Rundfunkstaatsvertrages,
3. inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des Mediendienste-Staatsvertrages in der Fassung vom 20. Januar bis 7. Februar 1997.

(5) Presserechtliche Vorschriften bleiben unberührt.

§ 3 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. "Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung
2. bereithalten oder den Zugang zur Nutzung vermitteln,
3. "Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§ 4 Zugangsfreiheit

Teledienste sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 5 Verantwortlichkeit

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung.

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

§ 6 Anbieterkennzeichnung

Diensteanbieter haben für ihre geschäftsmäßigen Angebote anzugeben:

1. Namen und Anschrift sowie
2. bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten.

Artikel 2
Gesetz über den Datenschutz bei Telediensten
(Teledienstedatenschutzgesetz - TDDSG)

§ 1 Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes.

(2) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. "Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. "Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§ 3 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Durchführung von Telediensten erhobene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(3) Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in zumutbarer Weise nicht möglich ist.

(4) Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen, auszurichten.

(5) Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren. Der Verzicht gilt nicht als Einwilligung im Sinne von Absatz 1 und 2.

(6) Der Nutzer ist vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 5 Satz 3 gilt entsprechend.

(7) Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß

1. sie nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber erkannt werden kann,
4. die Einwilligung protokolliert wird und
5. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.

§ 4 Datenschutzrechtliche Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

(2) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, daß

1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist,
3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden; eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für Abrechnungszwecke erforderlich ist.

(3) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(4) Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erstellte Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

§ 5 Bestandsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten).

(2) Eine Verarbeitung und Nutzung der Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung technischer Einrichtungen des Diensteanbieters ist nur zulässig, soweit der Nutzer in diese ausdrücklich eingewilligt hat.

(3) [gestrichen]

§ 6 Nutzungs- und Abrechnungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist,

1. um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen (Nutzungsdaten) oder
2. um die Nutzung von Telediensten abzurechnen (Abrechnungsdaten).

(2) Zu löschen hat der Diensteanbieter

1. Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt,
2. Abrechnungsdaten, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind; nutzerbezogene Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers gemäß Absatz 4 gespeichert werden, sind spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen, es sei denn, die Entgeltforderung wird innerhalb dieser Frist bestritten oder trotz Zahlungsaufforderung nicht beglichen.

(3) Die Übermittlung von Nutzungs- oder Abrechnungsdaten an andere Diensteanbieter oder Dritte ist unzulässig. Die Befugnisse der Strafverfolgungsbehörden bleiben unberührt. Der Diensteanbieter, der den Zugang zur Nutzung von Telediensten vermittelt, darf anderen Diensteanbietern, deren Teledienste der Nutzer in Anspruch genommen hat, lediglich übermitteln

1. anonymisierte Nutzungsdaten zu Zwecken deren Marktforschung,
2. Abrechnungsdaten, soweit diese zum Zwecke der Einziehung einer Forderung erforderlich sind.

(4) Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Der Dritte ist zur Wahrung des Fernmeldegeheimnisses zu verpflichten.

(5) Die Abrechnung über die Inanspruchnahme von Telediensten darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Teledienste nicht erkennen lassen, es sei denn der Nutzer verlangt einen Einzelnachweis.

§ 7 Auskunftsrecht des Nutzers

Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen. Die Auskunft ist auf Verlangen des Nutzers auch elektronisch zu erteilen. Das Auskunftsrecht ist im Falle einer kurzfristigen Speicherung im Sinne von § 33 Abs. 2 Nr. 5 Bundesdatenschutzgesetz nicht nach § 34 Abs. 4 Bundesdatenschutzgesetz ausgeschlossen.

§ 8 Datenschutzkontrolle

(1) § 38 Bundesdatenschutzgesetz findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen

werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

(2) Der Bundesbeauftragte für den Datenschutz beobachtet die Entwicklung des Datenschutzes bei Telediensten und nimmt dazu im Rahmen seines Tätigkeitsberichtes nach § 26 Abs. 1 BDSG Stellung.

Artikel 3
Gesetz zur digitalen Signatur
(Signaturgesetz - SigG)

§ 1 Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

(2) Die Anwendung anderer Verfahren für digitale Signaturen ist freigestellt, soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben sind.

§ 2 Begriffsbestimmungen

(1) Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.

(2) Eine Zertifizierungsstelle im Sinne dieses Gesetzes ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß § 4 besitzt.

(3) Ein Zertifikat im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).

(4) Ein Zeitstempel im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, daß ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

§ 3 Zuständige Behörde

Die Erteilung von Lizenzen und die Ausstellung von Zertifikaten, die zum Signieren von Zertifikaten eingesetzt werden, sowie die Überwachung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 16 obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.

§ 4 Genehmigung von Zertifizierungsstellen

(1) Der Betrieb einer Zertifizierungsstelle bedarf einer Genehmigung der zuständigen Behörde. Diese ist auf Antrag zu erteilen.

(2) Die Genehmigung ist zu versagen, wenn Tatsachen die Annahme rechtfertigen, daß der Antragsteller nicht die für den Betrieb einer Zertifizierungsstelle erforderliche Zuverlässigkeit besitzt, wenn der Antragsteller nicht nachweist, daß die für den Betrieb einer Zertifizierungsstelle erforderliche Fachkunde vorliegt, oder wenn zu erwarten ist, daß bei Aufnahme des Betriebes die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle nach diesem Gesetz und der Rechtsverordnung nach § 16 nicht vorliegen werden.

(3) Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Lizenzinhaber die für den Betrieb der Zertifizierungsstelle maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb der Zertifizierungsstelle tätigen Personen über die dafür erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen dieses Gesetzes und der Rechtsverordnung nach § 16 der zuständigen Behörde rechtzeitig in einem Sicherheitskonzept aufgezeigt und die Umsetzung durch eine von der zuständigen Behörde

anerkannten Stelle geprüft und bestätigt worden ist.

(4) Die Lizenz kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist um sicherzustellen, daß die Zertifizierungsstelle bei Aufnahme des Betriebes und im Betrieb die Voraussetzungen dieses Gesetzes und der Rechtsverordnung nach § 16 erfüllt.

(5) Die zuständige Behörde stellt für Signaturschlüssel, die zum Signieren von Zertifikaten eingesetzt werden, die Zertifikate aus. Die Vorschriften für die Vergabe von Zertifikaten durch Zertifizierungsstellen gelten für die zuständige Behörde entsprechend. Diese hat die von ihr ausgestellten Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und abrufbar zu halten. Dies gilt auch für Informationen über Anschriften und Rufnummern der Zertifizierungsstellen, die Sperrung von von ihr ausgestellten Zertifikaten, die Einstellung und die Untersagung des Betriebs einer Zertifizierungsstelle sowie die Rücknahme oder den Widerruf von Genehmigungen.

(6) Für öffentliche Leistungen nach diesem Gesetz und der Rechtsverordnung nach § 16 werden Kosten (Gebühren und Auslagen) erhoben.

§ 5 Vergabe von Zertifikaten

(1) Die Zertifizierungsstelle hat Personen, die ein Zertifikat beantragen, zuverlässig zu identifizieren. Sie hat die Zuordnung eines öffentlichen Signaturschlüssels zu einer identifizierten Person durch ein Signaturschlüssel-Zertifikat zu bestätigen und dieses sowie Attribut-Zertifikate jederzeit für jedermann über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und mit Zustimmung des Signaturschlüssel-Inhabers abrufbar zu halten.

(2) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung in das Signaturschlüssel-Zertifikat oder ein Attribut-Zertifikat aufzunehmen, soweit ihr die Einwilligung des Dritten zur Aufnahme dieser Vertretungsmacht oder die Zulassung zuverlässig nachgewiesen wird.

(3) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers im Zertifikat anstelle seines Namens ein Pseudonym aufzuführen.

(4) Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Sie hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig.

(5) Die Zertifizierungsstelle hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal einzusetzen. Für das Bereitstellen von Signaturschlüsseln sowie das Erstellen von Zertifikaten hat sie technische Komponenten gemäß § 14 einzusetzen. Dies gilt auch für technische Komponenten, die ein Nachprüfen von Zertifikaten nach Absatz 1 Satz 2 ermöglichen.

§ 6 Unterrichtungspflicht

Die Zertifizierungsstelle hat die Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zu sicheren digitalen Signaturen und deren zuverlässiger Prüfung beizutragen. Sie hat die Antragsteller darüber zu unterrichten, welche technischen Komponenten die Anforderungen nach § 14 Abs. 1 und 2 erfüllen, sowie über die Zuordnung der mit einem privaten Signaturschlüssel erzeugten digitalen Signaturen. Sie hat die Antragsteller darauf hinzuweisen, daß Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

§ 7 Inhalt von Zertifikaten

(1) Das Signaturschlüssel-Zertifikat muß mindestens folgende Angaben enthalten:

1. Den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,

2. den zugeordneten öffentlichen Signaturschlüssel,

3. die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,

4. die laufende Nummer des Zertifikates,

5. Beginn und Ende der Gültigkeit des Zertifikates,

6. den Namen der Zertifizierungsstelle und

7. Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

(2) Angaben zur Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung können sowohl in das Signaturschlüssel-Zertifikat als auch in ein Attribut-Zertifikat aufgenommen werden.

§ 8 Sperrung von Zertifikaten

(1) Die Zertifizierungsstelle hat ein Zertifikat zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zertifikat auf Grund falscher Angaben zu § 7 erwirkt wurde, sie ihre Tätigkeit beendet und diese nicht von einer anderen Zertifizierungsstelle fortgeführt wird oder die zuständige Behörde gemäß § 13 Abs. 5 Satz 2 eine Sperrung anordnet. Die Sperrung muß den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig.

(2) Enthält ein Zertifikat Angaben einer dritten Person, so kann auch diese eine Sperrung dieses Zertifikates verlangen.

(3) Die zuständige Behörde sperrt von ihr nach § 4 Abs. 5 ausgestellte Zertifikate, wenn eine Zertifizierungsstelle ihre Tätigkeit einstellt oder wenn die Genehmigung zurückgenommen oder widerrufen wird.

§ 9 Zeitstempel

Die Zertifizierungsstelle hat digitale Daten auf Verlangen mit einem Zeitstempel zu versehen. § 5 Abs. 5 Satz 1 und 2 gilt entsprechend.

§ 10 Dokumentation

Die Zertifizierungsstelle hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 16 sowie die ausgestellten Zertifikate so zu dokumentieren, daß die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind.

§ 11 Einstellung der Tätigkeit

(1) Die Zertifizierungsstelle hat, wenn sie ihre Tätigkeit einstellt, dies zum frühestmöglichen Zeitpunkt der zuständigen Behörde anzuzeigen und dafür zu sorgen, daß die bei Einstellung der Tätigkeit gültigen Zertifikate durch eine andere Zertifizierungsstelle übernommen werden, oder diese zu sperren.

(2) Sie hat die Dokumentation nach § 10 an die Zertifizierungsstelle, welche die Zertifikate übernimmt, oder andernfalls an die zuständige Behörde zu übergeben.

(3) Sie hat einen Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 12 Datenschutz

(1) Die Zertifizierungsstelle darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.

(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat die Zertifizierungsstelle die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Zollkriminalamtes erforderlich ist. Die Auskünfte sind zu dokumentieren.

(3) § 38 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

§ 13 Kontrolle und Durchsetzung von Verpflichtungen

(1) Die zuständige Behörde kann gegenüber Zertifizierungsstellen Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung treffen. Dazu kann sie insbesondere die Benutzung ungeeigneter technischer Komponenten untersagen und den Betrieb der Zertifizierungsstelle vorübergehend ganz oder teilweise untersagen. Personen, die den Anschein erwecken, über eine Genehmigung nach § 4 zu verfügen, ohne daß dies der Fall ist, kann die Tätigkeit der Zertifizierung untersagt werden.

(2) Zum Zwecke der Überwachung nach Absatz 1 Satz 1 haben Zertifizierungsstellen der zuständigen Behörde das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen zur Einsicht vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der zur Auskunft Verpflichtete ist auf dieses Recht hinzuweisen.

(3) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung oder bei Entstehen eines Versagungsgrundes für eine Genehmigung hat die zuständige Behörde die erteilte Genehmigung zu widerrufen, wenn Maßnahmen nach Absatz 1 Satz 2 keinen Erfolg versprechen.

(4) Im Falle der Rücknahme oder des Widerrufs einer Lizenz oder der Einstellung der Tätigkeit einer Zertifizierungsstelle hat die zuständige Behörde eine Übernahme der Tätigkeit durch eine andere Zertifizierungsstelle oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens, wenn die genehmigte Tätigkeit nicht fortgesetzt wird.

(5) Die Gültigkeit der von einer Zertifizierungsstelle ausgestellten Zertifikate bleibt vom Widerruf einer Lizenz unberührt. Die zuständige Behörde kann eine Sperrung von Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, daß Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder daß zur Anwendung der Signaturschlüssel eingesetzte technische Komponenten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung digitaler Signaturen oder eine unbemerkte Verfälschung signierter Daten zulassen.

§ 14 Technische Komponenten

(1) Für die Erzeugung und Speicherung von Signaturschlüsseln sowie die Erzeugung und Prüfung digitaler Signaturen sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die Fälschungen digitaler Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung privater Signaturschlüssel schützen.

(2) Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die die Erzeugung einer digitalen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten die digitale Signatur sich bezieht. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, ob die signierten Daten unverändert sind, auf welche Daten die digitale Signatur sich bezieht und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist.

(3) Bei technischen Komponenten, mit denen Signaturschlüssel-Zertifikate gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, sind Vorkehrungen erforderlich, um die Zertifikatverzeichnisse vor unbefugter Veränderung und unbefugtem Abruf zu schützen.

(4) Bei technischen Komponenten nach Absatz 1 bis 3 ist es erforderlich, daß sie nach dem Stand der Technik hinreichend geprüft sind und die Erfüllung der Anforderungen durch eine von der zuständigen Behörde anerkannten Stelle bestätigt ist.

(5) Bei technischen Komponenten, die nach den in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum geltenden Regelungen oder Anforderungen rechtmäßig hergestellt oder in den Verkehr gebracht werden und die gleiche Sicherheit gewährleisten, ist davon auszugehen, daß die die sicherheitstechnische Beschaffenheit betreffenden Anforderungen nach Absatz 1 bis 3 erfüllt sind. In begründeten Einzelfällen ist auf Verlangen der zuständigen Behörde nachzuweisen, daß die Anforderungen nach Satz 1 erfüllt sind. Soweit zum Nachweis der die sicherheitstechnische Beschaffenheit betreffenden Anforderungen im Sinne der Absätze 1 bis 3 die Vorlage einer Bestätigung einer von der zuständigen Behörde anerkannten Stelle vorgesehen ist, werden auch Bestätigungen von in anderen Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zugelassenen Stellen berücksichtigt, wenn die den Prüfberichten dieser Stellen zugrundeliegenden technischen Anforderungen, Prüfungen und Prüfverfahren denen der durch die zuständige Behörde anerkannten Stellen gleichwertig sind.

§ 15 Ausländische Zertifikate

(1) Digitale Signaturen, die mit einem öffentlichen Signaturschlüssel überprüft werden können, für den ein ausländisches Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie gleichwertige Sicherheit aufweisen, digitalen Signaturen nach diesem Gesetz gleichgestellt.

(2) Absatz 1 gilt auch für andere Staaten, soweit überstaatliche oder zwischenstaatliche Vereinbarungen über die Anerkennung der Zertifikate getroffen sind.

§ 16 Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 15 erforderlichen Rechtsvorschriften zu erlassen über

1. die näheren Einzelheiten des Verfahrens der Erteilung, Rüchnahme und des Widerrufs einer Lizenz sowie des Verfahrens bei Einstellung lizenzierter Tätigkeit,
2. die gebührenpflichtigen Tatbestände nach § 4 Abs. 6 und die Höhe der Gebühr,
3. die nähere Ausgestaltung der Pflichten der Zertifizierungsstellen,
4. die Gültigkeitsdauer von Signaturschlüssel-Zertifikaten,
5. die nähere Ausgestaltung der Kontrolle der Zertifizierungsstellen,
6. die näheren Anforderungen an die technischen Komponenten sowie die Prüfung technischer Komponenten und die Bestätigung, daß die Anforderungen erfüllt sind,
7. den Zeitraum sowie das Verfahren, nach dem eine neue digitale Signatur angebracht werden sollte.

Artikel 4
Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 10. März 1987 (BGBl. I S. 945, 1160), zuletzt geändert durch ..... (BGBl.....), wird wie folgt geändert:

1. § 11 Abs. 3 StGB wird wie folgt gefaßt:

"(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen."

2. § 74 d wird wie folgt geändert:

a) In Absatz 3 wird nach dem Wort "Schriften" die Angabe "(§ 11 Abs. 3)" eingefügt.
b) In Absatz 4 werden nach dem Wort "wenn" die Wörter "die Schrift (§ 11 Abs. 3) oder" eingefügt.

3. In § 86 Abs. 1 werden nach dem Wort "ausführt" die Wörter "oder in Datenspeichern öffentlich zugänglich macht" eingefügt.

4. § 184 wird wie folgt geändert:

a) In Absatz 4 werden nach dem Wort "tatsächliches" die Wörter "oder wirklichkeitsnahes" eingefügt,

b) In Absatz 5 Satz 1 werden nach dem Wort "tatsächliches" die Wörter "oder wirklichkeitsnahes" eingefügt.

Artikel 5
Änderung des Gesetzes über Ordnungswidrigkeiten

Das Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch ..... (BGBl.....), wird wie folgt geändert:

1. In § 116 Abs. 1, § 120 Abs. 1 Nr. 2 und § 123 Abs. 2 Satz 1 werden jeweils nach dem Wort "Bildträgern" ein Komma und das Wort "Datenspeichern" eingefügt.

2. § 119 wird wie folgt geändert:

a) In Absatz 1 Nr. 2 werden nach dem Wort "Darstellungen" die Wörter "oder durch das öffentliche Zugänglichmachen von Datenspeichern" eingefügt.
b) In Absatz 3 werden nach dem Wort "Bildträger" ein Komma und das Wort "Datenspeicher" eingefügt.

Artikel 6
Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften

Das Gesetz über die Verbreitung jugendgefährdender Schriften in der Fassung der Bekanntmachung vom 12. Juli 1985 (BGBl. I S. 1502), zuletzt geändert durch ..... (BGBl.....), wird wie folgt geändert:

1. Die Überschrift wird wie folgt neu gefaßt:

"Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte"

2. § 1 Abs. 3 wird wie folgt gefaßt:

"(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich. Schriften im Sinne dieses Gesetzes sind nicht Rundfunsendungen nach § 2 des Rundfunkstaatsvertrages sowie inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gesatltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des Mediendienstestaatsvertrages in der Fassung vonm 20. Januar bis 7. Februar 1997."

3. § 3 wird wie folgt geändert:

a) In Absatz 1 wird am Ende der Nummer 3 der Punkt durch ein Komma ersetzt und folgende Nummer 4 angefügt:

"4. durch Informations- und Kommunikationsdienste verbreitet, bereitgehalten oder sonst zugänglich gemacht werden."

b) Dem Absatz 2 wird folgender Satz angefügt:

"Absatz 1 Nr. 4 gilt nicht, wenn durch technische Vorkehrungen Vorsorge getroffen ist, daß das Angebot oder die Verbreitung im Inland auf volljährige Nutzer beschränkt werden kann."

4. § 5 Abs. 3 wird wie folgt gefaßt:

"(3) Absatz 2 gilt nicht,

1. wenn die Handlung im Geschäftsverkehr mit dem einschlägigen Handel erfolgt,
oder
2. wenn durch technische Vorkehrungen oder in sonstiger Weise eine Übermittlung an Kinder oder Jugendliche ausgeschlossen ist."

5. Nach § 7 wird folgender § 7a eingefügt:

"§ 7a Jugendschutzbeauftragte

Wer gewerbsmäßig elektronische Informations- und Kommunikationsdienste, denen eine Übermittlung mittels Telekommunikation zugrunde liegt, zur Nutzung bereithält, hat einen Jugendschutzbeauftragten zu bestellen, wenn diese allgemein angeboten werden und jugendgefährdende Inhalte enthalten können. Er ist Ansprechpartner für Nutzer und berät den Diensteanbieter in Fragen des Jugendschutzes. Er ist von dem Diensteanbieter bei der Angebotsplanung und der Gestaltung der Allgemeinen Nutzungsbedingungen zu beteiligen. Er kann gegenüber dem Diensteanbieter eine Beschränkung von Angeboten vorschlagen. Die Verpflichtung des Diensteanbieters nach Satz 1 kann auch dadurch erfüllt werden, daß er eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung der Aufgaben nach Satz 2 bis 4 verpflichtet."

6. Nach § 21 Abs. 1 Nr. 3 wird folgende Nummer 3a eingefügt:

"3a. entgegen § 3 Abs. 1 Nr. 4 verbreitet, bereithält oder sonst zugänglich macht,"

7. § 18 wird wie folgt gefaßt:

"(1) Eine Schrift unterliegt den Beschränkungen der §§ 3 bis 5, ohne daß es einer Aufnahme in die Liste und einer Bekanntmachung bedarf, wenn sie ganz oder im wesentlichen inhaltsgleich mit einer in die Liste aufgenommenen Schrift ist. Das gleiche gilt, wenn ein Gericht in einer rechtskräftigen Entscheidung festgestellt hat, daß eine Schrift pornographisch ist oder den in § 130 Abs. 2 oder § 131 des Strafgesetzbuches bezeichneten Inhalt hat.

(2) Ist es zweifelhaft, ob die Voraussetzungen des Absatzes 1 erfüllt sind, so führt der Vorsitzende eine Entscheidung der Bundesprüfstelle herbei. Eines Antrages (§ 11 Abs. 2 Satz 1) bedarf es nicht. § 12 gilt entsprechend.

(3) Wird die Schrift in die Liste aufgenommen, so gilt § 19 entsprechend."

8. § 18 a wird gestrichen.

9. § 2 wird wie folgt geändert:

a) Der bisherige Text wird Absatz 1.

b) Es wird folgender Absatz 2 angefügt:

"(2) Kommt eine Listenaufnahme offensichtlich nicht in Betracht, so kann der Vorsitzende das Verfahren einstellen.".

10. § 21 a Absatz 1 wird wie folgt gefaßt:

"(1) Ordnungswidrig handelt, wer

1. entgegen § 4 Abs. 2 Satz 2 einen Abnehmer nicht auf die Vertriebsbeschränkungen hinweist, oder
2. entgegen § 7 a Abs. 1 Satz 1 einen Jugendschutzbeauftragten nicht bestellt oder eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung dieser Aufgaben nicht verpflichtet."

Artikel 7
Änderung des Urheberrechtsgesetzes

Das Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch ..... (BGBl.....), wird wie folgt geändert:

1. § 4 wird wie folgt gefaßt:

"§ 4
Sammelwerke und Datenbankwerke

(1) Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die aufgrund der Auswahl oder Anordnung der Elemente eine persönliche geistige Schöpfung sind (Sammelwerke), werden, unbeschadet eines an den einzelnen Elementen gegebenenfalls bestehenden Urheberrechts oder verwandten Schutzrechts, wie selbständige Werke geschützt.

(2) Datenbankwerk im Sinne dieses Gesetzes ist ein Sammelwerk, dessen Elemente systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind. Ein zur Schaffung des Datenbankwerkes oder zur Ermöglichung des Zugangs zu dessen Elementen verwendetes Computerprogramm (§ 69 a) ist nicht Bestandteil des Datenbankwerkes."

2. § 23 Satz 2 wird wie folgt geändert:

a) Nach dem Wort "Künste" wird das Wort "oder" durch ein Komma ersetzt.

b) Nach dem Wort "Baukunst" werden die Wörter "oder um die Bearbeitung oder Umgestaltung eines Datenbankwerkes" eingefügt.

3. § 53 wird wie folgt geändert:

a) Nach Absatz 4 wird folgender Absatz 5 eingefügt:

"Absatz 1 sowie Absatz 2 Nr. 2 bis 4 finden keine Anwendung auf Datenbankwerke, deren Elemente einzeln mit Hilfe elektronischer Mittel zugänglich sind. Absatz 2 Nr. 1 findet auf solche Datenbankwerke mit der Maßgabe Anwendung, daß der wissenschaftliche Gebrauch nicht zu gewerblichen Zwecken erfolgt."

b) Die bisherigen Absätze 5 und 6 werden Absätze 6 und 7.

4. Nach § 55 wird folgender § 55 a eingefügt:

"§ 55 a
Benutzung eines Datenbankwerkes

Zulässig ist die Bearbeitung sowie die Vervielfältigung eines Datenbankwerkes durch den Eigentümer eines mit Zustimmung des Urhebers durch Veräußerung in Verkehr gebrachten Vervielfältigungsstücks des Datenbankwerkes, den in sonstiger Weise zu dessen Gebrauch Berechtigten oder denjenigen, dem ein Datenbankwerk aufgrund eines mit dem Urheber oder eines mit dessen Zustimmung mit einem Dritten geschlossenen Vertrags zugänglich gemacht wird, wenn und soweit die Bearbeitung oder Vervielfältigung für den Zugang zu den Elementen des Datenbankwerkes und für dessen übliche Benutzung erforderlich ist. Wird aufgrund eines Vertrags nach Satz 1 nur ein Teil des Datenbankwerkes zugänglich gemacht, so ist nur die Bearbeitung sowie die Vervielfältigung dieses Teils zulässig. Entgegenstehende vertragliche Vereinbarungen sind nichtig."

5. In § 63 Absatz 1 wird nach Satz 1 folgender Satz 2 eingefügt:

a) "Das gleiche gilt in den Fällen des § 53 Abs. 2 Nr. 1 und Abs. 3 Nr. 1 für die Vervielfältigung eines Datenbankwerkes."

b) Die bisherigen Sätze 2 und 3 werden Sätze 3 und 4.

6. Nach § 87 wird folgender Abschnitt eingefügt:

"Sechster Abschnitt
Schutz des Datenbankherstellers

§ 87 a
Begriffsbestimmungen

(1) Datenbank im Sinne dieses Gesetzes ist eine Sammlung von Werken, Daten oder anderen

unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Eine in ihrem Inhalt nach Art oder Umfang wesentlich geänderte Datenbank gilt als neue Datenbank, sofern die Änderung eine nach Art oder Umfang wesentliche Investition erfordert.

(2) Datenbankhersteller im Sinne dieses Gesetzes ist derjenige, der die Investition im Sinne von Absatz 1 vorgenommen hat.

§ 87 b
Rechte des Datenbankherstellers

(1) Der Datenbankhersteller hat das ausschließliche Recht, die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Der Vervielfältigung, Verbreitung oder öffentlichen Wiedergabe eines nach Art oder Umfang wesentlichen Teils der Datenbank steht die wiederholte und systematische Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank gleich, sofern diese Handlungen einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen.

(2) § 17 Abs. 2 und § 27 Abs. 2 und 3 sind entsprechend anzuwenden.

§ 87 c
Schranken des Rechts des Datenbankherstellers

(1) Die Vervielfältigung eines nach Art oder Umfang wesentlichen Teils einer Datenbank ist zulässig

1.zum privaten Gebrauch; dies gilt nicht für eine Datenbank, deren Elemente einzeln mit Hilfe elektronischer Mittel zugänglich sind,
2.zum eigenen wissenschaftlichen Gebrauch, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und der wissenschaftliche Gebrauch nicht zu gewerblichen Zwecken erfolgt,
3.zum eigenen Gebrauch im Schulunterricht, in nichtgewerblichen Einrichtungen der Aus- und Weiterbildung sowie in der Berufsbildung in der für eine Schulklasse erforderlichen Anzahl.

In den Fällen der Nummern 2 und 3 ist die Quelle deutlich anzugeben.

(2) Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe eines nach Art oder Umfang wesentlichen Teils einer Datenbank ist zulässig zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde sowie für Zwecke der öffentlichen Sicherheit.

§ 87 d
Dauer der Rechte

Die Rechte des Datenbankherstellers erlöschen fünfzehn Jahre nach der Veröffentlichung der Datenbank, jedoch bereits fünfzehn Jahre nach der Herstellung, wenn die Datenbank innerhalb dieser Frist nicht veröffentlicht worden ist. Die Frist ist nach § 69 zu berechnen.

§ 87 e
Verträge über die Benutzung einer Datenbank

Eine vertragliche Vereinbarung, durch die sich der Eigentümer eines mit Zustimmung des Datenbankherstellers durch Veräußerung in Verkehr gebrachten Vervielfältigungsstücks der Datenbank, der in sonstiger Weise zu dessen Gebrauch Berechtigte oder derjenige, dem eine Datenbank aufgrund eines mit dem Datenbankhersteller oder eines mit dessen Zustimmung mit einem Dritten geschlossenen Vertrags zugänglich gemacht wird, gegenüber dem Datenbankhersteller verpflichtet, die Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank zu unterlassen, ist insoweit unwirksam, als diese Handlungen weder einer normalen Auswertung der Datenbank zuwiderlaufen noch die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen."

7. In § 108 Abs. 1 wird nach Nr. 7 folgende Nummer angefügt:

"8. eine Datenbank entgegen § 87 b Abs. 2 verwertet,"

8. In § 119 Abs. 3 werden nach dem Wort "Lichtbilder" das Wort "und" durch ein Komma ersetzt und nach dem Wort "Tonträger" die Wörter "und die nach § 87 b Abs. 2 geschützten Datenbanken" eingefügt.

9. Nach § 127 wird folgender § 127 a eingefügt:

"§ 127 a
Schutz des Datenbankherstellers

(1) Den nach § 87 b gewährten Schutz genießen deutsche Staatsangehörige sowie juristische Personen mit Sitz im Geltungsbereich dieses Gesetzes. § 120 Abs. 2 ist anzuwenden.

(2) Die nach deutschem Recht oder dem Recht eines der in § 120 Abs. 2 Nr. 2 bezeichneten Staaten gegründeten juristischen Personen ohne Sitz im Geltungsbereich dieses Gesetzes genießen den nach § 87 b gewährten Schutz, wenn

1.ihre Hauptverwaltung oder Hauptniederlassung sich im Gebiet eines der in § 120 Abs. 2 Nr. 2 bezeichneten Staaten befindet oder 2.ihr satzungsmäßiger Sitz sich im Gebiet eines dieser Staaten befindet und ihre Tätigkeit eine tatsächliche Verbindung zur deutschen Wirtschaft oder zur Wirtschaft eines dieser Staaten aufweist.

(3) Im übrigen genießen ausländische Staatsangehörige sowie juristische Personen den Schutz nach dem Inhalt von Staatsverträgen sowie von Vereinbarungen, die die Europäische Gemeinschaft mit dritten Staaten schließt; diese Vereinbarungen werden vom Bundesministerium der Justiz im Bundesgesetzblatt bekanntgemacht."

10. Nach § 137 f wird folgender § 137 g eingefügt:

"§ 137 g
Übergangsregelung bei Umsetzung der Richtlinie 96/9/EG

(1) Die §§ 23 Satz 2, 53 Abs. 5, 55 a und 63 Abs. 1 Satz 2 sind auch auf Datenbankwerke anzuwenden, die vor dem 1. Januar 1998 geschaffen wurden.

(2) Die Vorschriften des Sechsten Abschnitts des Zweiten Teils sind auch auf Datenbanken anzuwenden, die zwischen dem 1. Januar 1983 und dem 31. Dezember 1997 hergestellt worden sind. Die Schutzfrist beginnt in diesen Fällen am 1. Januar 1998.

(3) Die §§ 55 a und 87 e sind nicht auf Verträge anzuwenden, die vor dem 1. Januar 1998 abgeschlossen worden sind."

Artikel 8
Änderung des Preisangabengesetzes

Dem § 1 des Preisangabengesetzes vom 3. Dezember 1984 (BGBl. I S. 1429) wird folgender Satz angefügt:

"Bei Leistungen der Informations- und Kommunikationsdienste können auch Bestimmungen über die Angabe des Preisstandes fortlaufender Leistungen getroffen werden."

Artikel 9
Änderung der Preisangabenverordnung

Die Preisangabenverordnung vom 14. März 1985 (BGBl. I S. 580), zuletzt geändert durch .....

(BGBl.....), wird wie folgt geändert:

1. Dem § 3 Abs. 1 werden folgende Sätze angefügt:

"Ort des Leistungsangebots ist auch die Bildschirmanzeige. Wird eine Leistung über Bildschirmanzeige erbracht und nach Einheiten berechnet, ist eine gesonderte Anzeige über den Preis der fortlaufenden Nutzung unentgeltlich anzubieten."

2. § 8 Abs. 2 Nr. 2 wird wie folgt gefaßt:

"2. des § 3 Abs. 1 Satz 1, 2 oder 4 oder Abs. 2, jeweils auch in Verbindung mit § 2 Abs. 5, über das Aufstellen, das Anbringen oder das Bereithalten von Preisverzeichnissen oder über das Anbieten einer Anzeige des Preises,".

Artikel 10
Rückkehr zum einheitlichen Verordnungsrang

Die auf Artikel 8 beruhenden Teile der Preisangabenverordnung können auf Grund der Ermächtigung des § 1 Preisangabengesetz durch Rechtsverordnung geändert werden.

Artikel 11
Inkrafttreten

Dieses Gesetz tritt mit Ausnahme des Artikels 7, der am 1. Januar 1998 in Kraft tritt, am 1. August 1997 in Kraft.

Verordnung zur digitalen Signatur
(Signaturverordnung - SigV)

Aufgrund des § 16 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872) verordnet die Bundesregierung:

Inhaltsübersicht

§ 1 Verfahren bei Erteilung, Rücknahme und Widerruf von Genehmigungen

(1) Eine Genehmigung für den Betrieb einer Zertifizierungsstelle nach § 4 Abs. 1 des Signaturgesetzes ist schriftlich bei der zuständigen Behörde zu beantragen.

(2) Zur Prüfung der Voraussetzungen für die Erteilung der Genehmigung trifft die zuständige Behörde die erforderlichen Feststellungen. Sie kann vom Antragsteller verlangen, daß dieser erforderliche Unterlagen, insbesondere einen aktuellen Handelsregisterauszug und aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für die gesetzlichen Vertreter der Zertifizierungsstelle, beibringt. Zur Feststellung der erforderlichen Fachkunde hat der Antragsteller darzulegen, daß das am Zertifizierungsverfahren oder an der Ausstellung von Zeitstempeln beteiligte Personal über die erforderlichen beruflichen Qualifikationen verfügt.

(3) Vor Ablehnung, Rücknahme oder Widerruf einer Genehmigung hat die zuständige Behörde den Antragsteller anzuhören und ihm Gelegenheit zu geben, die Gründe für die Ablehnung, die Rücknahme oder den Widerruf zu beseitigen.

§ 2 Kosten

(1) Für folgende öffentliche Leistungen werden Kosten (Gebühren und Auslagen) erhoben:

1. die Erteilung einer Genehmigung für den Betrieb einer Zertifizierungsstelle,
2. die Ablehnung eines Antrags auf Erteilung einer Genehmigung,
3. die Rücknahme oder den Widerruf einer Genehmigung,
4. die vollständige oder teilweise Zurückweisung eines Widerspruchs,
5. die Ausstellung von Zertifikaten,
6. die Überprüfung von Prüfberichten und Bestätigungen nach § 15 Abs. 1,
7. die Kontrollen nach § 15 Abs. 2, wenn im Rahmen der Kontrolle ein nicht nur unerheblicher Verstoß gegen das Signaturgesetz oder gegen diese Verordnung festgestellt wird,
8. die Übernahme einer Dokumentation nach § 11 Abs. 2 des Signaturgesetzes.

Kosten werden auch dann erhoben, wenn ein Antrag auf Erteilung einer Genehmigung oder ein Widerspruch nach Beginn der sachlichen Bearbeitung, aber vor deren Beendigung zurückgenommen wird.

(2) Bei der Berechnung der Gebühren für öffentliche Leistungen nach Absatz 1 Nr. 1, 5, 6, 7 und 8 sind folgende Stundensätze zugrunde zu legen:

1. Beamte des mittleren Dienstes oder vergleichbare Angestellte: 85 Deutsche Mark,
2. Beamte des gehobenen Dienstes oder vergleichbare Angestellte: 105 Deutsche Mark,
3. Beamte des höheren Dienstes oder vergleichbare Angestellte: 135 Deutsche Mark.

Für jede angefangene Viertelstunde ist ein Viertel dieser Stundensätze zu berechnen. Werden öffentliche Leistungen durch Angehörige der zuständigen Behörde außerhalb der Behörde erbracht, so sind Gebühren ferner zu berechnen für Reisezeiten, die innerhalb der üblichen Arbeitszeit liegen oder von der zuständigen Behörde besonders abgegolten werden, sowie für Wartezeiten, die der Kostenschuldner verursacht hat.

(3) Für die Fälle der Ablehnung oder Zurücknahme eines Antrages auf Erteilung einer Genehmigung sowie der Rücknahme oder des Widerrufs einer Genehmigung gilt § 15 des Verwaltungskostengesetzes. Für die vollständige oder teilweise Zurückweisung eines Widerspruchs kann eine Gebühr bis zur Höhe der für den angefochtenen Verwaltungsakt erhobenen Gebühr erhoben werden. Für die Zurückweisung und in den Fällen der Zurücknahme eines ausschließlich gegen eine Kostenentscheidung gerichteten Widerspruchs kann eine Gebühr bis zur Höhe von 10 vom Hundert des streitigen Betrages erhoben werden.

§ 3 Antragsverfahren bei Vergabe von Zertifikaten

(1) Die Zertifizierungsstelle hat die Identifikation des Antragstellers gemäß § 5 Abs. 1 Satz 1 des Signaturgesetzes anhand des Bundespersonalausweises oder Reisepasses oder auf andere geeignete Weise vorzunehmen. Der Antrag auf ein Zertifikat muß eigenhändig unterschrieben sein. Soweit ein Antrag auf ein Zertifikat mit einer digitalen Signatur des Antragstellers versehen ist, kann die Zertifizierungsstelle von einer erneuten Identifikation und eigenhändigen Unterschrift absehen.

(2) Sollen nach § 5 Abs. 2 des Signaturgesetzes in ein Zertifikat Angaben über die Vertretungsmacht für eine dritte Person aufgenommen werden, muß die Vertretungsmacht zuverlässig nachgewiesen sein und eine schriftliche oder mit einer digitalen Signatur versehene Einwilligung der dritten Person vorliegen. Die dritte Person ist schriftlich oder in digitaler Form mit digitaler Signatur über den Inhalt des Zertifikates zu unterrichten und auf die Möglichkeit der Sperrung nach § 9 Abs. 1 hinzuweisen. Eine berufsrechtliche oder sonstige Zulassung ist insbesondere durch Vorlage der Zulassungsurkunde nachzuweisen.

§ 4 Unterrichtung des Antragstellers

(1) Die Zertifizierungsstelle hat einen Antragsteller im Rahmen des § 6 Satz 1 und 3 des Signaturgesetzes insbesondere über folgende erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der digitalen Signatur zu unterrichten:

1. Der Datenträger mit dem privaten Signaturschlüssel ist in persönlichem Gewahrsam zu halten. Bei dessen Verlust ist unverzüglich die Sperrung des Signaturschlüssel-Zertifikates zu veranlassen. Wird der Datenträger mit dem privaten Signaturschlüssel nicht mehr benötigt, ist er unbrauchbar zu machen und die Sperrung des Signaturschlüssel-Zertifikates zu veranlassen, falls es nicht abgelaufen ist.

2. Persönliche Identifikationsnummern oder andere Daten zur Identifikation gegenüber dem Datenträger mit dem privaten Signaturschlüssel sind geheim zu halten. Bei Preisgabe oder Verdacht der Preisgabe dieser Identifikationsdaten ist unverzüglich deren Änderung vorzunehmen.

3. Für die Erzeugung und Prüfung digitaler Signaturen sowie die Darstellung von zu signierenden oder zu prüfenden signierten Daten sind technische Komponenten einzusetzen, die den Anforderungen des Signaturgesetzes und dieser Verordnung entsprechen und deren Sicherheit nach dem Signaturgesetz und dieser Verordnung bestätigt wurde. Sie sind vor unbefugtem Zugriff zu schützen.

4. Soweit ein Zertifikat Beschränkungen nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes oder Angaben nach § 7 Abs. 2 des Signaturgesetzes enthält und dies für die Aussage von signierten Daten von Bedeutung ist, ist das Zertifikat den Daten beizufügen und in die digitale Signatur einzuschließen.

5. Soweit für die Verwendung signierter Daten ein Zeitpunkt von erheblicher Bedeutung sein kann, ist ein Zeitstempel anzubringen.

6. Werden Daten über längere Zeit in signierter Form benötigt, ist gemäß § 18 erneut eine digitale Signatur anzubringen.

7. Bei der Prüfung digitaler Signaturen ist festzustellen, ob das Signaturschlüssel-Zertifikat und Attribut-Zertifikate zum Zeitpunkt der Signaturerzeugung gültig waren, das Signaturschlüssel-Zertifikat gemäß § 7 Abs. 1 Nr. 7 des Signaturgesetzes Beschränkungen enthält und gegebenenfalls die Nummern 4 und 5 beachtet wurden.

(2) Soweit ein Antragsteller bereits über ein Zertifikat verfügt, kann eine erneute Unterrichtung unterbleiben.

§ 5 Erzeugung und Speicherung von Signaturschlüsseln und Identifikationsdaten

(1) Werden Signaturschlüssel durch den Signaturschlüssel-Inhaber erzeugt, so hat sich die Zertifizierungsstelle zu überzeugen, daß er hierfür sowie für die Speicherung und Anwendung des privaten Signaturschlüssels geeignete technische Komponenten nach dem Signaturgesetz und dieser Verordnung einsetzt.

(2) Werden Signaturschlüssel durch die Zertifizierungsstelle bereitgestellt, so hat diese Vorkehrungen zu treffen, um eine Preisgabe von privaten Schlüsseln und eine Speicherung bei der Zertifizierungsstelle auszuschließen. Dies gilt auch für persönliche Identifikationsnummern oder andere Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber dem Datenträger mit dem privaten Signaturschlüssel.

§ 6 Übergabe von Signaturschlüsseln und Identifikationsdaten

Soweit die Zertifizierungsstelle Signaturschlüssel oder Identifikationsdaten nach § 5 Abs. 2 bereitstellt, hat sie den privaten Signaturschlüssel sowie die Identifikationsdaten dem Signaturschlüssel-Inhaber persönlich zu übergeben und die Übergabe von diesem schriftlich bestätigen zu lassen, es sei denn, dieser verlangt schriftlich eine andere Übergabe. Mit Übergabe des privaten Signaturschlüssels oder Signaturschlüssel-Zertifikates hat sie auch den öffentlichen Signaturschlüssel der zuständigen Behörde zu übergeben.

§ 7 Gültigkeitsdauer von Zertifikaten

Die Gültigkeitsdauer eines Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 nicht überschreiten. Die Gültigkeit eines Attribut-Zertifikates endet spätestens mit der Gültigkeit des Signaturschlüssel-Zertifikates, auf das es Bezug nimmt.

§ 8 Öffentliche Verzeichnisse von Zertifikaten

(1) Die Zertifizierungsstelle hat die von ihr ausgestellten Zertifikate mindestens solange in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen, wie der im Zertifikat aufgeführte Algorithmus mit den dazugehörigen Parametern nach § 17 Abs. 2 als geeignet beurteilt wird.

(2) Die zuständige Behörde hat die von ihr ausgestellten Zertifikate für die in Absatz 1 genannte Dauer in einem Verzeichnis gemäß den Vorgaben nach § 4 Abs. 5 Satz 3 des Signaturgesetzes zu führen. Dies gilt auch für Zertifikate für öffentliche Signaturschlüssel oberster ausländischer Zertifizie-

rungsstellen, soweit ausländische Zertifikate anerkannt werden. Bei den im Verzeichnis enthaltenen ausländischen Zertifikaten hat die zuständige Behörde die Anerkennung durch eine digitale Signatur zu bestätigen. Die zuständige Behörde hat die Telekommunikationsanschlüsse, unter denen die Zertifikate abrufbar sind, sowie ihre öffentlichen Schlüssel im Bundesanzeiger zu veröffentlichen und den Zertifizierungsstellen unmittelbar bekanntzugeben.

(3) Nach Ablauf der in Absatz 1 genannten Frist haben die Zertifizierungsstelle und die zuständige Behörde eine Nachprüfung der Zertifikate bis zum Ablauf der in § 13 Abs. 2 genannten Frist auf Antrag im Einzelfall zu ermöglichen.

§ 9 Verfahren zur Sperrung von Zertifikaten

(1) Die Zertifizierungsstelle hat den Signaturschlüssel-Inhabern und dritten Personen, von denen Angaben zur Vertretungsmacht in ein Zertifikat aufgenommen wurden, sowie der zuständigen Behörde eine Rufnummer bekanntzugeben, unter der diese jederzeit eine unverzügliche Sperrung der Zertifikate veranlassen können und dafür ein Authentisierungsverfahren anzubieten.

(2) Die Zertifizierungsstelle hat ein Zertifikat unter den Voraussetzungen des § 8 des Signaturgesetzes zu sperren, wenn ein mit einer digitalen Signatur versehener oder schriftlicher Antrag des Signaturschlüssel-Inhabers oder seines Vertreters oder einer berechtigten dritten Person nach Absatz 1 vorliegt oder wenn ein vereinbartes Authentisierungsverfahren angewandt wurde.

(3) Die Sperrung von Zertifikaten ist mit Angabe des Datums und der Uhrzeit im Verzeichnis nach § 8 des Signaturgesetzes eindeutig kenntlich zu machen und darf nicht rückgängig gemacht werden.

§ 10 Zuverlässigkeit des Personals

Die Zertifizierungsstelle hat sich von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren oder an der Ausstellung von Zeitstempeln mitwirken, zu überzeugen. Sie kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren und der Ausstellung von Zeitstempeln auszuschließen.

§ 11 Schutz der technischen Komponenten

Die Zertifizierungsstelle hat Vorkehrungen zu treffen, um private Signaturschlüssel und die zum Erstellen der Zertifikate und Zeitstempel sowie zum Nachprüfbarhalten der Zertifikate eingesetzten technischen Komponenten vor unbefugtem Zugriff zu schützen.

§ 12 Sicherheitskonzept

(1) Das Sicherheitskonzept nach § 4 Abs. 3 Satz 3 des Signaturgesetzes hat alle Sicherheitsmaßnahmen sowie insbesondere eine Übersicht über die eingesetzten technischen Komponenten und eine Darstellung der Ablauforganisation der Zertifizierungstätigkeit zu enthalten. Im Falle sicherheitserheblicher Veränderungen ist das Konzept unverzüglich anzupassen.

(2) Die zuständige Behörde führt einen Katalog von geeigneten Sicherheitsmaßnahmen, den sie im Bundesanzeiger veröffentlicht. Die Maßnahmen sollen bei der Erstellung des Sicherheitskonzeptes berücksichtigt werden. Der Katalog wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik erstellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

§ 13 Dokumentation

(1) Die Dokumentation nach § 10 des Signaturgesetzes hat sich auf das Sicherheitskonzept einschließlich der Änderungen, die Prüfberichte und Bestätigungen nach § 15 Abs. 1, die vertraglichen Vereinbarungen mit den Antragstellern und die von der zuständigen Behörde erhaltenen Zertifikate zu erstrecken. Zu den eingegangenen Anträgen auf Zertifikate und Vereinbarungen mit den Antragstellern sind eine Ablichtung des vorgelegten Ausweises oder eines anderen Identitätsnachweises, die für die Aufnahme von Angaben dritter Personen erforderlichen Unterlagen, die Vergabe eines Pseudonyms, der Nachweis über die vorgeschriebene Unterrichtung des Antragstellers und dritter Personen, die erteilten Zertifikate mit dem jeweiligen Zeitpunkt der Ausstellung und der Übergabe, die Sperrung von Zertifikaten und Auskünfte nach § 12 Abs. 2 des Signaturgesetzes zu dokumentieren. Soweit die Zertifizierungsstelle Signaturschlüssel oder Identifikationsdaten nach § 5 Abs. 2 bereitstellt, sind der Zeitpunkt der Übergabe und die Übergabebestätigung zu dokumentieren. In digitaler Form geführte Aufzeichnungen müssen digital signiert sein.

(2) Die Dokumentation nach Absatz 1 ist mindestens 35 Jahre ab dem Zeitpunkt der Ausstellung des Signaturschlüssel-Zertifikates aufzubewahren und so zu sichern, daß sie innerhalb dieses Zeitraums verfügbar bleibt. Die Dokumentation von Auskünften nach § 12 Abs. 2 Satz 2 des Signaturgesetzes ist zwölf Monate aufzubewahren.

§ 14 Einstellung der Tätigkeit

(1) Die Zertifizierungsstelle hat, wenn sie ihre Tätigkeit nach § 11 Abs. 1 des Signaturgesetzes einstellen will, dies spätestens vier Monate vorher der zuständigen Behörde mitzuteilen.

(2) Vor Beendigung ihrer Tätigkeit hat die Zertifizierungsstelle für jedes nicht gesperrte und zum Zeitpunkt der Beendigung der Tätigkeit nicht abgelaufene Zertifikat dem Signaturschlüssel-Inhaber mit

einer Frist von mindestens drei Monaten mitzuteilen, daß sie ihre Tätigkeit als Zertifizierungsstelle einstellen will und ihn zu unterrichten, ob eine andere Zertifizierungsstelle das Zertifikat übernimmt und diese zu benennen. Soweit nicht eine andere Zertifizierungsstelle die Zertifikate übernimmt, sind nach Ablauf der in Absatz 1 genannten Frist alle Zertifikate zu sperren, die zu diesem Zeitpunkt nicht bereits gesperrt oder abgelaufen sind. Die Signaturschlüssel-Inhaber der zu sperrenden Zertifikate sind darüber zu unterrichten.

(3) Die Mitteilung an die zuständige Behörde und die Unterrichtung der Signaturschlüssel-Inhaber haben in digitaler Form mit digitaler Signatur oder schriftlich zu erfolgen.

(4) Die Zertifizierungsstelle, die nach § 11 Abs. 2 des Signaturgesetzes die Dokumentation übernimmt, oder andernfalls die zuständige Behörde hat die Zertifikate in einem Verzeichnis nach § 8 Abs. 1 und 3 zu führen.

§ 15 Kontrolle der Zertifizierungsstellen

(1) Die Zertifizierungsstelle hat vor Betriebsaufnahme, nach sicherheitserheblichen Veränderungen sowie regelmäßig im Abstand von zwei Jahren eine Prüfung nach § 4 Abs. 3 Satz 3 des Signaturgesetzes zu veranlassen und der zuständigen Behörde einen Prüfbericht und eine Bestätigung darüber vorzulegen, daß sie die Vorgaben aus dem Signaturgesetz und dieser Verordnung erfüllt.

(2) Die zuständige Behörde kann in angemessenen Zeitabständen sowie bei Anhaltspunkten für eine Verletzung von Vorschriften des Signaturgesetzes oder dieser Verordnung Kontrollen durchführen.

§ 16 Anforderungen an die technischen Komponenten

(1) Die zur Erzeugung von Signaturschlüsseln erforderlichen technischen Komponenten müssen so beschaffen sein, daß ein Schlüssel mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommt und aus dem öffentlichen Schlüssel nicht der private Schlüssel errechnet werden kann. Die Geheimhaltung des privaten Schlüssels muß gewährleistet sein und er darf nicht dupliziert werden können. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(2) Die zur Erzeugung oder Prüfung digitaler Signaturen erforderlichen technischen Komponenten müssen so beschaffen sein, daß aus der Signatur nicht der private Signaturschlüssel errechnet oder die Signatur auf andere Weise gefälscht werden kann. Der private Signaturschlüssel darf erst nach Identifikation des Inhabers durch Besitz und Wissen angewendet werden können und bei der Anwendung nicht preisgegeben werden. Zur Identifikation des Signaturschlüssel-Inhabers können zusätzlich biometrische Merkmale genutzt werden. Die zum Erfassen von Identifikationsdaten erforderlichen

technischen Komponenten müssen so beschaffen sein, daß sie die Identifikationsdaten nicht preisgeben und diese nur auf dem Datenträger mit dem privaten Signaturschlüssel gespeichert werden. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(3) Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann, eine digitale Signatur nur auf ihre Veranlassung erfolgt und diese vorher eindeutig angezeigt wird. Die zum Prüfen signierter Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die prüfende Person die Daten, auf die sich die digitale Signatur erstreckt, sowie den Signaturschlüssel-Inhaber eindeutig feststellen kann und die Korrektheit der digitalen Signatur zuverlässig geprüft und zutreffend angezeigt wird. Die technischen Komponenten zum Nachprüfen von Zertifikaten müssen eindeutig erkennen lassen, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zu einem angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Die technischen Komponenten müssen nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Werden technische Komponenten nach den Sätzen 1 bis 4 geschäftsmäßig Dritten zur Nutzung angeboten, muß die eindeutige Interpretation der Daten sichergestellt sein und müssen die technischen Komponenten bei Benutzung automatisch auf ihre Echtheit überprüft werden. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(4) Die technischen Komponenten, mit denen Zertifikate nach § 4 Abs. 5 Satz 3 oder § 5 Abs. 1 Satz 2 des Signaturgesetzes nachprüfbar gehalten werden, müssen so beschaffen sein, daß nur befugte Personen Eintragungen und Veränderungen vornehmen können, die Sperrung eines Zertifikates nicht unbemerkt rückgängig gemacht werden kann und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte müssen beinhalten, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Nur nachprüfbar gehaltene Zertifikate dürfen nicht öffentlich abrufbar sein. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Betreiber erkennbar werden.

(5) Die technischen Komponenten, mit denen Zeitstempel nach § 9 des Signaturgesetzes erzeugt werden, müssen so beschaffen sein, daß die zum Zeitpunkt der Erzeugung des Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Betreiber erkennbar werden.

(6) Die zuständige Behörde führt einen Katalog von geeigneten Sicherheitsmaßnahmen, den sie im Bundesanzeiger veröffentlicht. Die Maßnahmen sollen bei den technischen Komponenten berücksichtigt werden. Der Katalog wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik erstellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

§ 17 Prüfung der technischen Komponenten

(1) Die Prüfung der technischen Komponenten nach § 14 Abs. 4 des Signaturgesetzes hat nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (GMBl. 1992, S. 545) zu erfolgen. Die Prüfung muß bei technischen Komponenten zum Erzeugen von Signaturschlüsseln oder zum Speichern oder Anwenden privater Signaturschlüssel und bei technischen Komponenten, die geschäftsmäßig Dritten zur Nutzung angeboten werden, mindestens die Prüfstufe „E 4" und im übrigen mindestens die Prüfstufe „E 2" umfassen. Die Stärke der Sicherheitsmechanismen muß mit "hoch" und die Algorithmen und zugehörigen Parameter müssen nach Absatz 2 als geeignet bewertet sein.

(2) Die zuständige Behörde veröffentlicht im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung digitaler Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen. Die Eignung ist gegeben, wenn innerhalb des bestimmten Zeitraumes nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von digitalen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

(3) In der Bestätigung der Erfüllung der Anforderungen für technische Komponenten nach § 14 Abs. 4 des Signaturgesetzes ist anzugeben, für welche Anforderungen nach § 16 die Bestätigung gilt und unter welchen Einsatzbedingungen, welche Algorithmen und zugehörigen Parameter nach Absatz 2 eingesetzt und bis zu welchem Zeitpunkt diese mindestens geeignet sind sowie nach welcher Stufe die technischen Komponenten nach Absatz 1 geprüft wurden. Eine Ausfertigung des Prüfberichtes und der Bestätigung ist bei der zuständigen Behörde zu hinterlegen. Diese kann bei Anhaltspunkten für Mängel bei Prüfungen oder bei bestätigten technischen Komponenten sowie stichprobenweise Gutachten eines unabhängigen Dritten darüber einholen, ob die technischen Komponenten gemäß Absatz 1 geprüft wurden und ob diese die Anforderungen des Signaturgesetzes und dieser Verordnung erfüllen. Betroffene Hersteller, Vertreiber und Prüfstellen haben die dafür erforderliche Unterstützung zu gewähren. Wird diese nicht gewährt oder stellt sich heraus, daß bestätigte technische Komponenten nicht ausreichend geprüft wurden oder Anforderungen nicht erfüllen, so kann die zuständige Behörde erteilte Bestätigungen für ungültig erklären.

(4) Die zuständige Behörde hat die nach § 14 Abs. 4 des Signaturgesetzes anerkannten Stellen sowie die technischen Komponenten, die von diesen eine Bestätigung nach Absatz 3 erhalten haben, im Bundesanzeiger zu veröffentlichen und den Zertifizierungsstellen unmittelbar bekannt zu geben. Zu den technischen Komponenten ist anzugeben, bis zu welchem Zeitpunkt die Bestätigung gilt. Wird eine Anerkennung entzogen oder eine Bestätigung für ungültig erklärt, so ist dies ebenfalls im Bundesanzeiger zu veröffentlichen und den Zertifizierungsstellen unmittelbar bekannt zu geben.

§ 18 Erneute digitale Signatur

Werden Daten über längere Zeit in signierter Form benötigt, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 als geeignet beurteilt sind, so sind die Daten vor Ablauf des Zeitpunktes der Eignung der Algorithmen und zugehörigen Parameter mit einer neuen digitalen Signatur zu versehen. Diese muß mit neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere digitale Signaturen einschließen und einen Zeitstempel tragen.

§ 19 Inkrafttreten

Diese Verordnung tritt am 1. November 1997 in Kraft.

ANEXO IX

LEY DE ESPAÑA

REAL DECRETO-LEY 14/1999, DE 17 DE SEPTIEMBRE, SOBRE FIRMA ELECTRÓNICA

REAL DECRETO LEY 14/1999, DE 17 DE SEPTIEMBRE, SOBRE FIRMA ELECTRÓNICA

En la sesión del Consejo de Ministros de Telecomunicaciones de la Unión Europea, celebrada el 22 de abril de 1999, se ha informado favorablemente la adopción de una posición común, respecto del proyecto de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica.

El Estado español ha tenido una participación activa en el logro de la posición común que facilita la tramitación del texto, al recoger éste los elementos suficientes para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica. En ese sentido, existen ya en España diversas normas sobre la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas por medios telemáticos, dictadas por la Administración tributaria. La Comisión Nacional del Mercado de Valores, por su parte, ha aprobado y puesto en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas.

Asimismo, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, anuncia la posibilidad de prestar, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos. La Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda actuará en colaboración con Correos y Telégrafos.

En el proyecto de Directiva se incorpora, a solicitud del Estado español, una novedad, recogida en el apartado c) del anexo II, entre los requisitos exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos. Esta novedad consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante.

Existe, además, en España un sector empresarial que podría prestar un servicio de certificación de la firma electrónica con suficiente calidad. Se considera que debe introducirse, cuanto antes, la disciplina que permita utilizar, con la adecuada seguridad jurídica, este medio tecnológico que contribuye al desarrollo de lo que se ha venido en denominar, en la Unión Europea, la sociedad de la información. La urgencia de la aprobación de esta norma deriva, también, del deseo de dar, a los usuarios de los nuevos servicios, elementos de confianza en los sistemas, permitiendo su introducción y rápida difusión.

Por ello, este Real Decreto-ley persigue, respetando el contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real Decretoley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

La presente disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio.

En su virtud, a propuesta del Ministro de Fomento, de la Ministra de Justicia y del Ministro de Industria y Energía, previo informe del Consejo General del Poder Judicial y de la Agencia de Protección de Datos, tras la deliberación del Consejo de Ministros, en su reunión celebrada el día 17 de septiembre de 1999, y en uso de la autorización concedida en el artículo 86 de la Constitución, DISPONGO:

TÍTULO I

Disposiciones generales

CAPÍTULO ÚNICO

Disposiciones generales

Artículo 1. Ámbito de aplicación.

1. Este Real Decreto-ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. Definiciones.

A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:

a) «Firma electrónica»: Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

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

c) «Signatario»: Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

d) «Datos de creación de firma»: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica.

e) «Dispositivo de creación de firma»: Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma.

f) «Dispositivo seguro de creación de firma»: Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

g) «Datos de verificación de firma»: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

h) «Dispositivo de verificación de firma»: Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma.

i) «Certificado»: Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

j) «Certificado reconocido»: Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

k) «Prestador de servicios de certificación»: Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

l) «Producto de firma electrónica»: Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

ll) «Acreditación voluntaria del prestador de servicios de certificación»: Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Artículo 3. Efectos jurídicos de la firma electrónica.

1. La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que

ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21.

2. A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

TÍTULO II

La prestación de servicios de certificación

CAPÍTULO I

Principios generales

Artículo 4. Régimen de libre competencia.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea.

2. La prestación de los servicios de certificación por las Administraciones o los organismos o sociedades de ellas dependientes se realizará con la debida separación de cuentas y con arreglo a los principios de objetividad, transparencia y no discriminación.

Artículo 5. Empleo de la firma electrónica por las Administraciones públicas.

1. Se podrá supeditar por la normativa estatal o, en su caso, autonómica el uso de la firma electrónica en el seno de las Administraciones públicas y sus entes públicos y en las relaciones que con cualesquiera de ellos mantengan los particulares, a las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento.

Las condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora, respecto de los documentos electrónicos integrados en un expediente administrativo.

El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica a las que se refiere este apartado sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y se dictarán a propuesta del Ministerio de Administraciones Públicas y previo informe del Consejo Superior de Informática.

2. Las condiciones adicionales a las que se refiere el apartado anterior deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o

extranjeras.

3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

Artículo 6. Sistemas de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica.

1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios.

2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones; en la Ley 21/1992, de 16 de julio, de Industria, y en la demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1 establecerá las condiciones que permitan coordinar los sistemas de certificación.

3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen.

4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que se haya pedido certificación. También tomarán en cuenta el cumplimiento, por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado.

5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

Artículo 7. Registro de Prestadores de Servicios de Certificación.

1. Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España.

Su regulación se desarrollará por Real Decreto.

2. La solicitud de inscripción habrá de formularse, aportando la documentación que se establezca reglamentariamente, a efectos de la identificación del prestador de servicios de certificación y de justificar que éste reúne los requisitos necesarios, en cada caso, para ejercer su actividad. También será

objeto de inscripción ulterior cualquier circunstancia relevante, a efectos de este Real Decreto-ley, relativa al prestador de servicios de certificación, como su acreditación o estar en condiciones de expedir certificados reconocidos.

La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente.

3. El Registro de Prestadores de Servicios de Certificación será público y deberá mantener permanentemente actualizada y a disposición de cualquier persona
una relación de los inscritos, en la que figurarán su nombre o razón social, la dirección de su página en Internet o de correo electrónico, los datos de verificación de su firma electrónica y, en su caso, su condición de acreditado o de tener la posibilidad de expedir certificados reconocidos. En la citada relación figurarán, también, cualesquiera otros datos complementarios que se determinen por Real Decreto.

Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral. El suministro de esta información podrá sujetarse al pago de una tasa, cuyos elementos esenciales se determinarán por ley.

CAPÍTULO II

Certificados

Artículo 8. Requisitos para la existencia de un certificado reconocido.

1. Los certificados reconocidos, definidos en el artículo 2.j) de este Real Decreto-ley, tendrán el siguiente contenido:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

g) Los datos de verificación de firma que correspondan a los datos de creación

de firma que se encuentren bajo el control del signatario h) El comienzo y el fin del período de validez del certificado.

i) Los límites de uso del certificado, si se prevén.

j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Artículo 9. Vigencia de los certificados.

1. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:

a) Expiración del período de validez del certificado.

Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro año contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.

c) Pérdida o inutilización por daños del soporte del certificado.

d) Utilización indebida por un tercero.

e) Resolución judicial o administrativa que lo ordene.

f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.

g) Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.

h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

2. La pérdida de eficacia de los certificados, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado surtirá efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11.e).

3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación.

Corresponderá al prestador de servicios la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

4. El prestador de servicios de certificación podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores.

Artículo 10. Equivalencia de certificados.

Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste, expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumplan alguna de las siguientes condiciones:

a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.

b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.

c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPÍTULO III

Condiciones exigibles a los prestadores de servicios de certificación

Artículo 11. Obligaciones de los prestadores de servicios de certificación.

Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación, los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.

b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.

c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.

d) Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su

posible responsabilidad patrimonial.

e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o perdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.

f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el apartado 1 del artículo 13, a los titulares de los certificados por ellos emitidos y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

Artículo 12. Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

a) Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

b) Demostrar la fiabilidad necesaria de sus servicios.

c) Garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.

d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

f) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.

g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de

caución.

Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 Euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.

h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.

i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información, deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.

j) Utilizar sistemas fiables para almacenar certificados, de modo tal que:

1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas.

2. Únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.

3. Pueda comprobarse la autenticidad de la información.

4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

Artículo 13. Cese de la actividad.

1. El prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos y transferir, con su consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

2. Si el prestador de servicios estuviere inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar a éste, con la antelación indicada en el anterior apartado, el cese de su actividad, y el destino que vaya a dar a los certificados especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto. Igualmente, indicará cualquier otra circunstancia relevante, que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de un procedimiento de quiebra o suspensión de pagos respecto de él.

3. La inscripción del prestador de servicios de certificación en el Registro de Prestadores de Servicios de Certificación será cancelada, de oficio, por el Ministerio de Justicia, cuando aquél cese en su actividad. El Ministerio de Justicia se hará cargo de la información relativa a los certificados que se hubieren dejado sin efecto por el prestador de servicios de certificación, a efectos de lo previsto en el artículo 12.h).

Artículo 14. Responsabilidad de los prestadores de servicios de certificación.

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

2. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

3. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.

4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Artículo 15. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación al que se refiere este Real Decreto-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2. Los prestadores de servicios de certificación que expidan certificados a los

usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre. Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

En todo caso, se estará a lo previsto en las normas sobre protección de datos indicadas en el apartado 1 de este artículo.

CAPÍTULO IV

Inspección y control de la actividad de los prestadores de servicios de certificación

Artículo 16. Supervisión y control.

1. El Ministerio de Fomento controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en este Real Decreto-ley y en sus disposiciones de desarrollo. Asimismo, vigilará el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones establecidas en el artículo 11.

2. En el ejercicio de su actividad de control, la Secretaría General de Comunicaciones actuará de oficio, mediante petición razonada del Ministerio de Justicia o de otros órganos administrativos o a instancia de persona interesada. Los funcionarios de la Secretaría General de Comunicaciones adscritos a la Inspección de las Telecomunicaciones, a efectos de cumplir las tareas de control, tendrán la consideración de autoridad pública.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, de lo dispuesto en el artículo 11.c), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Ésta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador, con arreglo a la legislación que regula su actividad.

Artículo 17. Deber de colaboración.

Los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría General de Comunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier

documentación relevante para la inspección de que se trate, referida siempre a datos que conciernan al prestador de servicios.

Artículo 18. Resoluciones del órgano de supervisión.

La Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan este Real Decreto-ley y sus disposiciones de desarrollo.

TÍTULO III

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

CAPÍTULO ÚNICO

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

Artículo 19.
Dispositivos seguros de creación de firma electrónica.

A efectos del artículo 2.f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:

1.º Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2.º Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3.º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4.º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Artículo 20. Normas técnicas.

1. Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el «Diario Oficial de las Comunidades Europeas» son conformes con lo previsto en la letra e) del artículo 12 y en el artículo 19.

2. Sin perjuicio de esta presunción, los números de referencia de esas normas se publicarán en el «Boletín Oficial del Estado».

Artículo 21. Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica.

1. Los órganos de certificación a los que se refiere el artículo 6 podrán certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de

evaluación acreditadas.

En la evaluación del cumplimiento de los requisitos previstos en el artículo 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el artículo anterior u otras que determinen los órganos de acreditación y de certificación, y cuyas referencias se publiquen en el «Boletín Oficial del Estado».

2. Se reconocerá eficacia a los certificados sobre dispositivos seguros de creación de firma que hayan sido expedidos por los organismos designados para ello por los Estados miembros de la Unión Europea, cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.

Artículo 22. Dispositivos de verificación de firma.

1. Los dispositivos de verificación de firma electrónica avanzada deben garantizar lo siguiente:

1. Que la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente.

2. Que el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

3. Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo.

4. Que se verifica de forma fiable el certificado.

5. Que puede detectarse cualquier cambio relativo a su seguridad.

2. El Real Decreto al que se refiere el artículo 6 podrá establecer los términos en los que las entidades de evaluación y los órganos de certificación podrán evaluar y certificar, respectivamente, el cumplimiento, por los dispositivos de verificación de firma electrónica avanzada, de los requisitos establecidos en este artículo.

TÍTULO IV

Tasa por el reconocimiento de acreditaciones y certificaciones

CAPÍTULO ÚNICO

Tasa por el reconocimiento de acreditaciones y certificaciones

Artículo 23. Régimen aplicable a la tasa.

1. La gestión precisa para el reconocimiento de las acreditaciones y de las certificaciones con arreglo a los artículos 6, 21 y 22, por los órganos públicos competentes, se grava con una tasa, a la que se aplicará el siguiente régimen:

a) Constituye el hecho imponible el reconocimiento por dichos órganos de la acreditación de los prestadores de servicios o de la certificación de los dispositivos de creación o de verificación de firma a que se refieren los

artículos 6, 21 y 22.

b) Es sujeto pasivo la persona natural o jurídica que se beneficie del reconocimiento de la correspondiente acreditación o certificación.

c) Su cuota es de 47.500 pesetas (285,48 Euros) por cada acreditación o certificación reconocida. Esta cantidad podrá ser actualizada por Real Decreto.

d) Se devengará cuando se presente la solicitud de reconocimiento de la correspondiente acreditación o certificación.

2. La forma de liquidación de la tasa se establecerá reglamentariamente.

TÍTULO V

Infracciones y sanciones

CAPÍTULO ÚNICO Infracciones y sanciones

Artículo 24. Clasificación de las infracciones.

Las infracciones de las normas reguladoras de la firma electrónica y los servicios de certificación se clasifican en muy graves, graves y leves.

Artículo 25. Infracciones.

1. Son infracciones muy graves:

a) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h).

b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones impuestas en las letras c) a la j) del artículo 12, siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.

c) El incumplimiento grave y reiterado por los prestadores de servicios de certificación de las resoluciones dictadas por la Secretaría General de Comunicaciones, para asegurar el respeto a este Real Decreto-ley.

2. Son infracciones graves:

a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones impuestas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h), siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.

b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones previstas en las letras a), b), y k) del artículo 12.

c) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones contempladas en las letras

c) a la j) del artículo 12, cuando no concurran las circunstancias previstas en el apartado 1.b) de este artículo.

d) La falta de comunicación por el prestador de servicios de certificación al Ministerio de Justicia, en los plazos previstos en el artículo 13, del cese de su actividad o de la iniciación, respecto de él, de un procedimiento de suspensión de pagos o de quiebra.

e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo, con arreglo a este Real Decreto-ley.

f) El incumplimiento de las resoluciones dictadas por la Secretaría General de Comunicaciones para asegurar que el prestador de servicios de certificación se ajuste a este Real Decreto-ley, cuando no deba considerarse como infracción muy grave, conforme al apartado 1.c) de este artículo.

3. Son infracciones leves:

a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, excepto la c), cuando no deba considerarse como infracción grave, de acuerdo con lo previsto en el apartado 2.a) de este artículo.

b) La expedición de certificados reconocidos que incumplan alguno de los requisitos establecidos en el artículo 8.

c) No facilitar los datos requeridos, en el ámbito de sus respectivas funciones, por el Ministerio de Justicia o la Secretaría General de Comunicaciones para comprobar el cumplimiento de este Real Decreto-ley por los prestadores de servicios de certificación.

d) Cualquier otro incumplimiento de las obligaciones impuestas a los prestadores de servicios de certificación por este Real Decreto-ley, salvo el de la recogida en el artículo 11.c) o que deba ser considerado como infracción grave o muy grave, de acuerdo con lo dispuesto en los apartados anteriores.

Artículo 26. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 1 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 5 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 100.000.000 de pesetas (601.012,10 Euros).

La reiteración de dos o más infracciones muy graves, en el plazo de cinco años,

podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años. Cuando la resolución
de imposición de esta sanción sea firme, será comunicada al Registro de Prestadores de Servicios de Certificación para que cancele la inscripción del prestador de servicios sancionado.

b) Por la comisión de infracciones graves, se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 0,5 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 2 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 50.000.000 de pesetas (300.506,04 Euros).

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 Euros).

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación de la resolución sancionadora en el «Boletín Oficial del Estado» y en dos periódicos de difusión nacional, una vez que aquélla tenga carácter firme.

3. La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El daño causado, siempre que no haya sido tomado en consideración para calificar la infracción como leve, grave o muy grave.

d) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

4. Se anotarán en el Registro de Prestadores de Servicios de Certificación las sanciones impuestas por resolución firme a éstos por la comisión de cualquier infracción grave o muy grave. Las notas relativas a las sanciones se cancelarán una vez transcurridos los plazos de prescripción de las sanciones administrativas previstos en la Ley reguladora del procedimiento administrativo común.

5. Las cuantías señaladas en este artículo serán actualizadas periódicamente por el Gobierno, mediante Real Decreto, teniendo en cuenta la variación de los índices de precios al consumo.

Artículo 27. Medidas cautelares.

En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, las medidas

cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

Estas medidas podrán consistir en la orden de cese temporal de la actividad del prestador de servicios de certificación, en la suspensión de la vigencia de los certificados por él expedidos o en la adopción de otras cautelas que se estimen precisas. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

Artículo 28. Procedimiento sancionador.

1. El ejercicio de la potestad sancionadora atribuida por este Real Decreto-ley corresponde a la Secretaría General de Comunicaciones del Ministerio de Fomento.

Para ello, la Secretaría General de Comunicaciones se sujetará al procedimiento aplicable, con carácter general, al ejercicio de la potestad sancionadora por las Administraciones públicas.

2. El Ministerio de Justicia y los demás órganos que ejercen competencias con arreglo a este Real Decreto-ley y sus normas de desarrollo podrán instar la incoación de un procedimiento sancionador, mediante petición razonada dirigida a la Secretaría General de Comunicaciones Disposición adicional única. Posibilidad de emisión por las entidades públicas de radiodifusión de una Comunidad Autónoma en el territorio de otras con las que aquélla tenga espacios radioeléctricos colindantes.

Las entidades autonómicas habilitadas, con arreglo a la Ley, para prestar el servicio de radiodifusión digital terrenal, podrán emitir en el territorio de otras Comunidades Autónomas con las que aquélla tenga espacios radioeléctricos colindantes. Para ello, será preciso que exista acuerdo entre las Comunidades Autónomas afectadas y que, en cada territorio, se empleen los bloques de frecuencias planificados en el Plan Técnico Nacional de Radiodifusión Sonora Digital Terrenal, para el ámbito autonómico.

Disposición transitoria única. Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de este Real Decreto-ley.

Los prestadores de servicios de certificación ya establecidos en España y cuya actividad se rija por una normativa específica habrán de adaptarse a este Real Decreto-ley en el plazo de un año desde su entrada en vigor.

No obstante conservarán su validez los certificados ya expedidos que hayan surtido efectos.

Disposición final primera. Fundamento constitucional.

Este Real Decreto-ley se dicta al amparo del artículo 149.1.8. a , 18. a y 21. a de la Constitución, que atribuye competencia exclusiva al Estado en materia de legislación civil, de bases del régimen jurídico de las Administraciones Públicas y de telecomunicaciones.

Disposición final segunda. Habilitación al Gobierno.

Se habilita al Gobierno para desarrollar, mediante Reglamento, lo previsto en este Real Decreto-ley.

Disposición final tercera. Entrada en vigor.

El presente Real Decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid a 17 de septiembre de 1999.

Juan Carlos Rey de España

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

ANEXO X

LEY DE FRANCIA

LOI No. 2000-230 DU 13 MARS 2000 PORTANT ADAPTATION DU DROIT DE LA PREUVE AUX TECHNOLOGIES DE L'INFORMATION ET RELATIVE À LA SIGNATURE ÉLECTRONIQUE

DÉCRET No. 2001-272 DU 30 MARS 2001 PRIS POUR L'APPLICATION DE L'ARTICLE 1316-4 DU CODE CIVIL ET RELATIF À LA SIGNATURE ÉLECTRONIQUE

Loi 2000-230 du 13 Mars 2000

LOI portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

NOR : JUSX9900020L

Article 6

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.

Nota - Loi 2001-616 2001-07-11 art 75 : Dans tous les textes législatifs et réglementaires en vigueur à Mayotte, la référence à la "collectivité territoriale de Mayotte" est remplacée par la référence à "Mayotte", et la référence à la "collectivité territoriale" est remplacée par la référence à la "collectivité départementale".

Jacques Chirac
Par le Président de la République :
Le Premier ministre,
Lionel Jospin
Le garde des sceaux, ministre de la justice,
Élisabeth Guigou
Le ministre de l'intérieur,
Jean-Pierre Chevènement
Le ministre de l'économie,
des finances et de l'industrie,
Christian Sautter
Le secrétaire d'Etat à l'outre-mer,
Jean-Jack Queyranne
Le secrétaire d'Etat à l'industrie,
Christian Pierret

Loi n° 2000-230.
- Directive communautaire :
Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
- Travaux préparatoires :
Sénat :
Projet de loi n° 488 (1998-1999) ;
Rapport de M Charles Jolibois, au nom de la commission des lois, n° 203 (1999-2000) ;
Discussion et adoption le 8 février 2000.
Assemblée nationale :
Projet de loi, adopté par le Sénat, n° 2158 ;
Rapport de M Christian Paul, au nom de la commission des lois, n° 2197 ;
Discussion et adoption le 29 février 2000.

Décret 2001-272 du 30 Mars 2001

Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

NOR : JUSC0120141D

Le Premier ministre,
Sur le rapport de la garde des sceaux, ministre de la justice,
Vu la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ;
Vu le code civil, notamment ses articles 1316 à 1316-4 ;
Vu la loi n° 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;
Le Conseil d'Etat (section de l'intérieur) entendu,

Article 1

Au sens du présent décret, on entend par :
1. Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;
2. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :
- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;
3. Signataire : toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en uvre un dispositif de création de signature électronique ;
4. Données de création de signature électronique : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;
5. Dispositif de création de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;
6. Dispositif sécurisé de création de signature électronique : un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 ;
7. Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;
8. Dispositif de vérification de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;
9. Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;
10. Certificat électronique qualifié : un certificat électronique répondant aux exigences définies à l'article 6 ;
11. Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;
12. Qualification des prestataires de services de certification électronique : l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Article 2

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en uvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation

d'un certificat électronique qualifié.

Chapitre Ier : Des dispositifs sécurisés de création de signature électronique.

Article 3

Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est certifié conforme à ces exigences dans les conditions prévues au II.
I - Un dispositif sécurisé de création de signature électronique doit :
1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :
a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.
II. - Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I :
1° Soit par les services du Premier ministre chargés de la sécurité des systèmes d'information, après une évaluation réalisée, selon des règles définies par arrêté du Premier ministre, par des organismes agréés par ces services. La délivrance par ces services du certificat de conformité est rendue publique ;
2° Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

Article 4

Le contrôle de la mise en uvre des procédures d'évaluation et de certification prévues au 1° du II de l'article 3 est assuré par un comité directeur de la certification, institué auprès du Premier ministre.
Un arrêté du Premier ministre précise les missions attribuées à ce comité, fixe sa composition, définit les procédures de certification et d'évaluation des dispositifs de création de signature électronique mentionnées à l'alinéa précédent ainsi que les procédures d'agrément des organismes d'évaluation. Il détermine, en outre, les obligations incombant à ces organismes et fixe les conditions dans lesquelles sont présentées et instruites les demandes de certification.

Chapitre II : Des dispositifs de vérification de signature électronique.

Article 5

Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies par l'arrêté mentionné à l'article 4, s'il répond aux exigences suivantes :
a) Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en uvre le dispositif et qui est dénommée vérificateur ;
b) Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;
c) Le vérificateur doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;
d) Les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;
e) L'identité du signataire doit sans subir d'altération être portée à la connaissance du vérificateur ;
f) Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement portée à la connaissance du vérificateur ;
g) Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.

Chapitre III : Des certificats électroniques qualifiés et des prestataires de services de certification électronique.

Article 6

Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II.

I - Un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

II. - Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :

a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;

b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;

c) Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;

d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;

e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;

f) Appliquer des procédures de sécurité appropriées ;

g) Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;

h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;

i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;

j) Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;

k) Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.

l) Utiliser des systèmes de conservation des certificats électroniques garantissant que :

- l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;
- l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
- toute modification de nature à compromettre la sécurité du système peut être détectée ;

m) Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;

n) S'assurer au moment de la délivrance du certificat électronique :

- que les informations qu'il contient sont exactes ;
- que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;

o) Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un

certificat électronique :
- des modalités et des conditions d'utilisation du certificat ;
- du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique mentionnée à l'article 7 ;
- des modalités de contestation et de règlement des litiges ;
p) Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au o qui leur sont utiles.

Article 7

Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés.
Cette qualification, qui vaut présomption de conformité auxdites exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de l'industrie.
Elle est précédée d'une évaluation réalisée par ces mêmes organismes selon des règles définies par arrêté du Premier ministre.
L'arrêté du ministre chargé de l'industrie prévu à l'alinéa précédent détermine la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de certification électronique.

Article 8

Un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat n'appartenant pas à la Communauté européenne a la même valeur juridique que celui délivré par un prestataire établi dans la Communauté, dès lors :
a) Que le prestataire satisfait aux exigences fixées au II de l'article 6 et a été accrédité, au sens de la directive du 13 décembre 1999 susvisée, dans un Etat membre ;
b) Ou que le certificat électronique délivré par le prestataire a été garanti par un prestataire établi dans la Communauté et satisfaisant aux exigences fixées au II de l'article 6 ;
c) Ou qu'un accord auquel la Communauté est partie l'a prévu.

Article 9

I - Au titre de la déclaration de fourniture de prestations de cryptologie effectuée conformément aux dispositions de l'article 28 de la loi du 29 décembre 1990 susvisée, le prestataire de services de certification électronique doit, quand il entend délivrer des certificats électroniques qualifiés, l'indiquer.
II. - Le contrôle des prestataires visés au I est effectué par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information.
Ce contrôle porte sur le respect des exigences définies à l'article 6. Il peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire de services de certification électronique.
Lorsque le contrôle révèle qu'un prestataire n'a pas satisfait à ces exigences, les services du Premier ministre chargés de la sécurité des systèmes d'information assurent la publicité des résultats de ce contrôle et, dans le cas où le prestataire a été reconnu comme qualifié dans les conditions fixées à l'article 7, en informent l'organisme de qualification.
Les mesures prévues à l'alinéa précédent doivent faire l'objet, préalablement à leur adoption, d'une procédure contradictoire permettant au prestataire de présenter ses observations.

Chapitre IV : Dispositions diverses.

Article 10

Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française, aux îles Wallis et Futuna et à Mayotte.

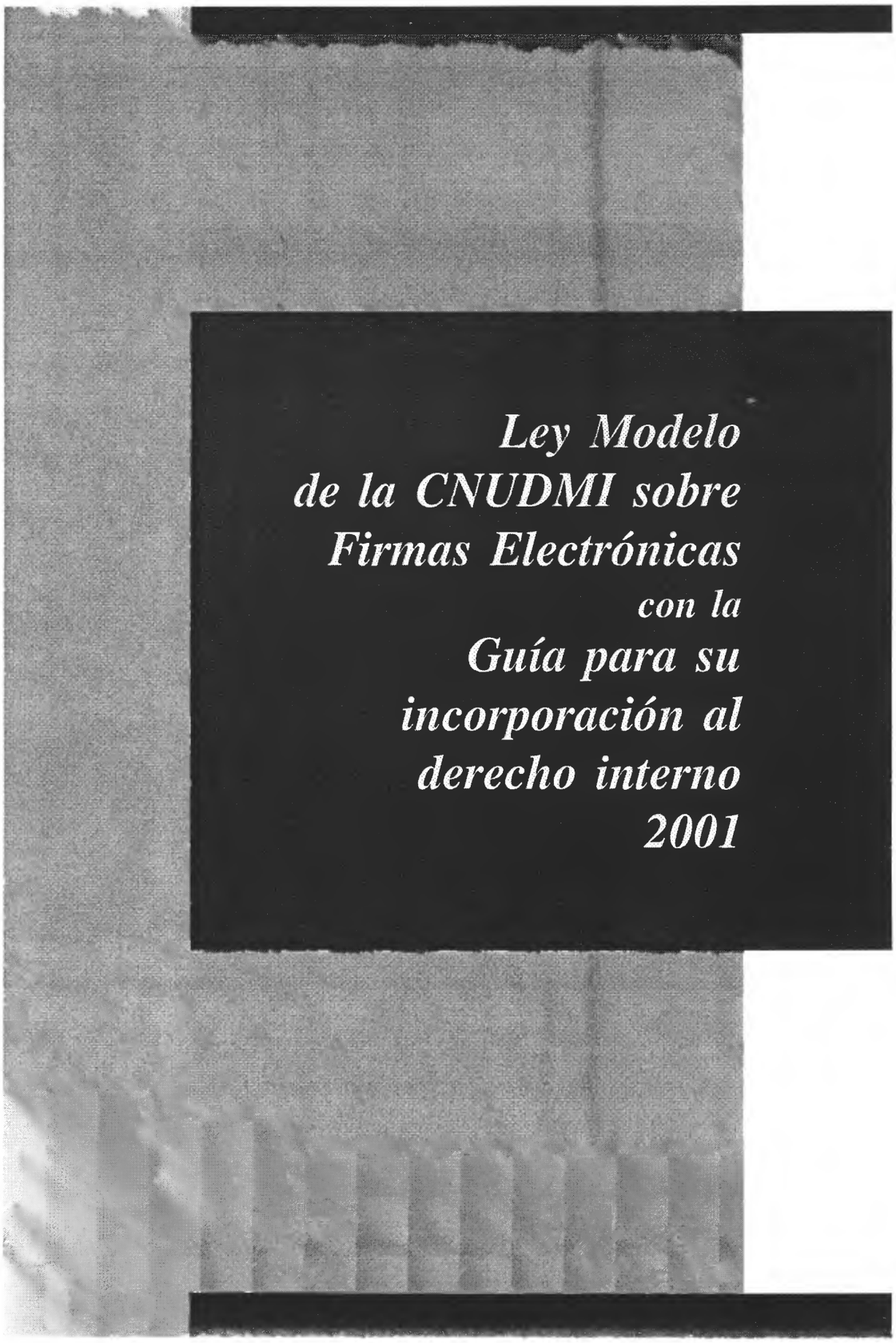
Article 11 Le ministre de l'économie, des finances et de l'industrie, la garde des sceaux, ministre de la justice, le ministre de l'intérieur, le secrétaire d'Etat à l'outre-mer et le secrétaire d'Etat à l'industrie sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Lionel Jospin
Par le Premier ministre :
La garde des sceaux, ministre de la justice,
Marylise Lebranchu
Le ministre de l'économie,
des finances et de l'industrie,
Laurent Fabius
Le ministre de l'intérieur,
Daniel Vaillant
Le secrétaire d'Etat à l'outre-mer,
Christian Paul
Le secrétaire d'Etat à l'industrie,
Christian Pierret

ANEXO XI

LEY DE LAS NACIONES UNIDAS

LEY MODELO DE LA CNUDMI SOBRE FIRMAS ELECTRÓNICAS CON LA GUÍA PARA SU INCORPORACIÓN AL DERECHO INTERNO 2001



Ley Modelo de la CNUDMI sobre Firmas Electrónicas

con la

Guía para su incorporación al derecho interno

2001

Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001

NACIONES UNIDAS
Nueva York, 2002

Publicación de las Naciones Unidas
Número de venta: S.02.V.8
ISBN 92-1-333321-8

Índice

Resolución aprobada por la Asamblea General

[sobre la base del informe de la Sexta Comisión (A/56/588)]

56/80 Ley Modelo sobre las Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

La Asamblea General,

Recordando su resolución 2205 (XXI), de 17 de diciembre de 1966, por la que estableció la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional con el mandato de fomentar la armonización y la unificación progresivas del derecho mercantil internacional y de tener presente, a ese respecto, el interés de todos los pueblos, en particular el de los países en desarrollo, en el progreso amplio del comercio internacional,

Observando que un número creciente de transacciones comerciales internacionales se realizan por el medio de comunicación habitualmente conocido como comercio electrónico, en el que se usan métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel,

Recordando la recomendación relativa al valor jurídico de los registros computadorizados aprobada por la Comisión en su 18.° período de sesiones, celebrado en 1985, y el apartado *b)* del párrafo 5 de la resolución 40/71 de la Asamblea General, de 11 de diciembre de 1985, en la que la Asamblea pidió a los gobiernos y a las organizaciones internacionales que, cuando así convenga, adopten medidas acordes con las recomendaciones de la Comisión[1] a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos en el comercio internacional,

Recordando también que la Ley Modelo sobre Comercio Electrónico fue aprobada por la Comisión en su 29.° período de sesiones, celebrado en 1996[2], y complementada por un nuevo artículo 5 *bis*, aprobado por la Comisión en su 31.° período de sesiones, celebrado en 1998[3], y recordando el párrafo 2 de la resolución 51/162 de la Asamblea General, de 16 de diciembre de 1996, en la que la Asamblea recomendaba que todos los Estados consideraran de manera favorable la Ley Modelo cuando promulgaran o revisaran sus leyes, habida cuenta de la necesidad de que el derecho aplicable a los métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel sea uniforme,

---

[1] *Documentos Oficiales de la Asamblea General, cuadragésimo período de sesiones, Suplemento núm. 17* (A/40/17), cap. VI, secc. B.

[2] Ibíd., *quincuagésimo primer período de sesiones, Suplemento núm. 17* (A/51/17), párr. 209.

[3] Ibíd., *quincuagésimo tercer período de sesiones, Suplemento núm. 17* (A/53/17), cap. III, secc. B.

Convencida de que la Ley Modelo sobre Comercio Electrónico es de considerable utilidad para los Estados al posibilitar o facilitar la utilización del comercio electrónico, como demuestra la incorporación de esta Ley Modelo al derecho interno de un cierto número de países y su reconocimiento universal como referencia esencial en lo relativo a la legislación sobre el comercio electrónico,

Consciente de la gran utilidad de las nuevas tecnologías de identificación personal utilizadas en el comercio electrónico, generalmente conocidas como firmas electrónicas,

Deseosa de desarrollar los principios fundamentales enunciados en el artículo 7 de la Ley Modelo sobre Comercio Electrónico[4] con respecto al cumplimiento de la función de la firma en las operaciones de comercio electrónico, con miras a fomentar la confianza en las firmas electrónicas para que surtan efectos jurídicos cuando sean el equivalente funcional de las firmas manuales,

Convencida de que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas y el establecimiento de un método para evaluar de un modo tecnológicamente neutral la fiabilidad práctica y la idoneidad comercial de las técnicas de firma electrónica darán una mayor certidumbre jurídica al comercio electrónico,

Estimando que la Ley Modelo sobre las Firmas Electrónicas constituirá un útil complemento de la Ley Modelo sobre Comercio Electrónico y ayudará en gran medida a los Estados a formular legislación que regule la utilización de técnicas modernas de autenticación y a mejorar la legislación ya existente,

Considerando que la elaboración de legislación modelo que facilite la utilización de las firmas electrónicas de forma que sea aceptable para Estados con distintos ordenamientos jurídicos, sociales y económicos podría contribuir al fomento de relaciones económicas armoniosas en el plano internacional,

1. *Expresa su gratitud* a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional por haber completado y aprobado la Ley Modelo sobre las Firmas Electrónicas que figura en el anexo a la presente resolución y por haber preparado la Guía para la incorporación de la Ley Modelo al derecho interno;

2. *Recomienda* que todos los Estados consideren de manera favorable la Ley Modelo sobre las Firmas Electrónicas, junto con la Ley Modelo sobre Comercio Electrónico aprobada en 1996 y complementada en 1998, cuando promulguen o revisen sus leyes, habida cuenta de la necesidad de que el derecho aplicable a los métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel sea uniforme;

3. *Recomienda también* que se haga todo lo posible por promover el conocimiento y la disponibilidad generales de la Ley Modelo sobre Comercio Electrónico y de la Ley Modelo sobre las Firmas Electrónicas, junto con sus respectivas Guías para la incorporación al derecho interno.

85ª sesión plenaria
12 de diciembre de 2001

---

[4]Resolución 51/162 de la Asamblea General, anexo.

Primera parte

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor.

Artículo 2. Definiciones

Para los fines de la presente Ley:

a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;

b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos

---

*La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]."

**El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje ("factoring"); arrendamiento con opción de compra ("leasing"); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

d) Por "firmante" se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa;

e) Por "prestador de servicios de certificación" se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por "parte que confía" se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1 del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4. Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.

2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.

Artículo 5. Modificación mediante acuerdo

Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6. Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier

acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.

2. El párrafo 1 será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1 si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4. Lo dispuesto en el párrafo 3 se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1, la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

5. Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.

2. La determinación que se haga con arreglo al párrafo 1 deberá ser compatible con las normas o criterios internacionales reconocidos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8. Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.

Artículo 9. Proceder del prestador de servicios de certificación

1. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

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

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su

control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) el método utilizado para comprobar la identidad del firmante;

ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado *b)* del párrafo 1 del artículo 8 de la presente Ley;

vi) si se ofrece un servicio para revocar oportunamente el certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado *d)*, proporcionar un medio para que el firmante dé aviso conforme al apartado *b)* del párrafo 1 del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado *d)*, cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.

Artículo 10. Fiabilidad

A los efectos del apartado *f)* del párrafo 1 del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de activos;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o

g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.

2. Todo certificado expedido fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que todo

certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2, o del párrafo 3, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2, 3 y 4, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

ANEXO XII

LEY DE LA UNIÓN EUROPEA

DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 13 DE DICIEMBRE DE 1999 POR LA QUE SE ESTABLECE UN MARCO COMUNITARIO PARA LA FIRMA ELECTRÓNICA

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica Diario Oficial nº L 013 de 19/01/2000 P. 0012-0020 Texto:

DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 2 de su artículo 47 y sus artículos 55 y 95, Vista la propuesta de la Comisión(1), Visto el dictamen del Comité Económico y Social(2), Visto el dictamen del Comité de las Regiones(3), De conformidad con el procedimiento establecido en el artículo 251 del Tratado(4), Considerando lo siguiente:

El 16 de abril de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación "Iniciativa europea de comercio electrónico".

El 8 de octubre de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación "El Fomento de la seguridad y la confianza en la comunicación electrónica: hacia un marco europeo para la firma digital y el cifrado".

El 1 de diciembre de 1997, el Consejo invitó a la Comisión a que presentara lo antes posible una propuesta de directiva del Parlamento Europeo y del Consejo sobre la firma digital.

La comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico. Por otro lado, un marco claro comunitario sobre las condiciones aplicables a la firma electrónica aumentará la confianza en las nuevas tecnologías y la aceptación general de las mismas. La legislación de los Estados miembros en este ámbito no debería obstaculizar la libre circulación de bienes y servicios en el mercado interior.

Es preciso promover la interoperabilidad de los productos de firma electrónica; de conformidad con el artículo 14 del Tratado, el mercado interior implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica, sin perjuicio de lo dispuesto en el Reglamento (CE) nº 3381/94 del Consejo, de 19 de diciembre de 1994, por el que se establece un régimen comunitario de control de las exportaciones de productos de doble uso (5) y en la Decisión 94/942/PESC del Consejo, de 19 de diciembre de 1994, relativa a la Acción común adoptada por el Consejo referente al control de las exportaciones de productos de doble uso (6).

La presente Directiva no armoniza la prestación de servicios por lo que respecta a la confidencialidad de la información cuando sean objeto de disposiciones nacionales en materia de orden público y seguridad pública.

El mercado interior garantiza también la libre circulación de personas, por lo cual es cada vez más frecuente que los ciudadanos y residentes de la Unión Europea tengan que tratar con autoridades de Estados miembros distintos de aquél en el que residen. La disponibilidad de la comunicación electrónica puede ser de gran utilidad a este respecto.

Los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.

La firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con ella o que la utilicen. La definición de dichos productos y servicios no debe limitarse a la expedición y gestión de certificados, sino incluir también cualesquiera otros servicios o productos que utilicen firmas electrónicas o se sirvan de ellas, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relacionados con la firma electrónica.

El mercado interior permite a los proveedores de servicios de certificación llevar a cabo sus actividades transfronterizas para acrecentar su competitividad y, de ese modo, ofrecer a los consumidores y a las empresas nuevas posibilidades de intercambiar información y comerciar electrónicamente de una forma segura, con independencia de las fronteras. Con objeto de estimular la prestación de servicios de certificación en toda la Comunidad a través de redes abiertas, los proveedores de servicios de certificación deben tener libertad para prestar sus servicios sin autorización previa. La autorización previa implica no sólo el permiso que ha de obtener el proveedor de servicios de certificación interesado en virtud de una decisión de las autoridades nacionales antes de que se le permita prestar sus servicios de certificación, sino también cualesquiera otras medidas que tengan ese mismo efecto.

Los sistemas voluntarios de acreditación destinados a un nivel reforzado de prestación de servicios pueden aportar a los proveedores de servicios de certificación un marco apropiado para aproximarse a los niveles de confianza, seguridad y calidad exigidos por un mercado en evolución. Dichos sistemas deben fomentar la adopción de las mejores prácticas por parte de los proveedores de servicios de certificación; debe darse a los proveedores de servicios de certificación libertad para adherirse a dichos sistemas de acreditación y disfrutar de sus ventajas.

Los servicios de certificación pueden ser prestados tanto por entidades públicas como por personas físicas o jurídicas cuando así se establezca de acuerdo con el Derecho nacional. Los Estados miembros no deben prohibir a los proveedores de servicios de certificación operar al margen de los sistemas de acreditación voluntaria; ha de velarse por que los sistemas de acreditación no supongan mengua de la competencia en el ámbito de los servicios de certificación.

Los Estados miembros pueden decidir cómo llevar a cabo la supervisión del cumplimiento de lo dispuesto en la presente Directiva. La presente Directiva no excluye el establecimiento de sistemas de supervisión basados en el sector privado. La presente Directiva no obliga a los proveedores de servicios de certificación a solicitar ser supervisados con arreglo a cualquier sistema de acreditación aplicable.

Es importante alcanzar un equilibrio entre las necesidades de los consumidores y las de las empresas.

El anexo III abarca los requisitos de los dispositivos seguros de creación de firmas electrónicas para garantizar la funcionalidad de las firmas electrónicas avanzadas; no abarca la totalidad del sistema en cuyo entorno operan dichos dispositivos. El funcionamiento del mercado interior exige que la Comisión y los Estados miembros actúen con celeridad para hacer posible la designación de los organismos encargados de evaluar la conformidad de los dispositivos seguros de firma con el anexo III. Con objeto de subvenir a las necesidades del mercado, la evaluación de la conformidad ha de producirse oportunamente y ser eficaz.

La presente Directiva contribuye al uso y al reconocimiento legal de la firma electrónica en la Comunidad; no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrados entre un número determinado de participantes. En la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común

acuerdo las condiciones en que aceptarán las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales.

La presente Directiva no pretende armonizar las legislaciones nacionales sobre contratos, en particular por lo que respecta al perfeccionamiento y eficacia de los mismos, ni tampoco otras formalidades de naturaleza no contractual relativas a la firma; por dicho motivo, las disposiciones sobre los efectos legales de la firma electrónica deberán entenderse sin perjuicio de los requisitos de forma establecidos por las legislaciones nacionales en materia de celebración de contratos, ni para las normas que determinan el lugar en que se considera celebrado un contrato.

El almacenamiento y la copia de los datos de creación de la firma pueden poner en peligro la validez jurídica de la firma electrónica.

La firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitaria y en la comunicación entre dichas administraciones y entre éstas y los ciudadanos y agentes económicos, por ejemplo en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial.

Unos criterios armonizados en relación con la eficacia jurídica de la firma electrónica mantendrán un marco jurídico coherente en toda la Comunidad. Las legislaciones nacionales establecen requisitos divergentes con respecto a la validez jurídica de las firmas manuscritas; se pueden utilizar certificados para confirmar la identidad de la persona que firma electrónicamente; las firmas electrónicas avanzadas basadas en un certificado reconocido pretenden lograr un mayor nivel de seguridad. Las firmas electrónicas avanzadas relacionadas con un certificado reconocido y creadas mediante un dispositivo seguro de creación de firma únicamente pueden considerarse jurídicamente equivalentes a las firmas manuscritas si se cumplen los requisitos aplicables a las firmas manuscritas.

Para contribuir a la aceptación general de los métodos de autenticación electrónica, debe garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales en todos los Estados miembros. El reconocimiento legal de la firma electrónica debe basarse en criterios objetivos y no estar supeditado a la autorización del proveedor de servicios de certificación de que se trate; la legislación nacional rige la determinación de los ámbitos jurídicos en los que pueden usarse los documentos electrónicos y de la firma electrónica. La presente Directiva se entiende sin perjuicio de la facultad de los tribunales nacionales para dictar resoluciones acerca de la conformidad con los requisitos de la presente Directiva y no afecta a las normas nacionales en lo que se refiere a la libertad de la valoración judicial de las pruebas.

Los proveedores de servicios de certificación al público están sujetos a la normativa nacional en materia de responsabilidad.

El desarrollo del comercio electrónico internacional requiere acuerdos transfronterizos que implican a terceros países; para garantizar la interoperabilidad a nivel mundial, podría ser beneficioso celebrar acuerdos con terceros países sobre normas multilaterales en materia de reconocimiento mutuo de servicios de certificación.

Para incrementar la confianza de los usuarios en la comunicación y el comercio electrónicos, los proveedores de servicios de certificación deben observar la normativa sobre protección de datos y el respeto de la intimidad.

Las disposiciones relativas al uso de seudónimos en los certificados no deben impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho comunitario o nacional.

Habida cuenta de que las medidas necesarias para la ejecución de la presente Directiva son medidas de gestión con arreglo al artículo 2 de la Decisión 1999/468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio

de las competencias de ejecución atribuidas a la Comisión (7), dichas medidas deben ser aprobadas con arreglo al procedimiento de gestión previsto en el artículo 4 de la citada Decisión.

Transcurridos dos años desde su aplicación, la Comisión procederá a una revisión de la presente Directiva a fin de cerciorarse de que los avances tecnológicos y los cambios del entorno jurídico no han creado obstáculos al logro de los objetivos formulados en la presente Directiva. La Comisión debe estudiar la incidencia de ámbitos técnicos afines y presentar un informe al respecto al Parlamento Europeo y al Consejo.

De conformidad con los principios de subsidiariedad y proporcionalidad recogidos en el artículo 5 del Tratado, el objetivo de crear un marco jurídico armonizado para la prestación del servicio de firma electrónica y de servicios conexos no puede ser alcanzado de manera suficiente por los Estados miembros y, por consiguiente, puede lograrse mejor a nivel comunitario. La presente Directiva no excede de lo necesario para lograr dicho objetivo,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Ámbito de aplicación

La presente Directiva tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. La presente Directiva crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior.

La presente Directiva no regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos.

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

1) "firma electrónica": los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación;

2) "firma electrónica avanzada": la firma electrónica que cumple los requisitos siguientes:

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;

d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable;

3) "firmante": la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa;

4) "datos de creación de firma": los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica;

5) "dispositivo de creación de firma": un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma;

6) "dispositivo seguro de creación de firma": un dispositivo de creación de firma que cumple los requisitos enumerados en el anexo III;

7) "datos de verificación de firma": los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica;

8) "dispositivo de verificación de firma": un programa informático configurado o un aparato informático

configurado, que sirve para aplicar los datos de verificación de firma;

9) "certificado": la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta;

10) "certificado reconocido": el certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II;

11) "proveedor de servicios de certificación": la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica;

12) "producto de firma electrónica": el programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas;

13) "acreditación voluntaria": todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, cuando el proveedor de servicios de certificación no esté habilitado para ejercer los derechos derivados del permiso hasta que haya recaído la decisión positiva de dicho organismo.

Artículo 3

Acceso al mercado

1. Los Estados miembros no condicionarán la prestación de servicios de certificación a la obtención de autorización previa.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación. Todas las condiciones relativas a tales sistemas deberán ser objetivas, transparentes, proporcionadas y no discriminatorias. Los Estados miembros no podrán limitar el número de proveedores de servicios de certificación acreditados amparándose en la presente Directiva.

3. Los Estados miembros velarán por que se establezca un sistema adecuado que permita la supervisión de los proveedores de servicios de certificación establecidos en su territorio que expiden al público certificados reconocidos.

4. La conformidad de los dispositivos seguros de creación de firma con los requisitos fijados en el anexo III será determinada por los organismos públicos o privados pertinentes, designados por los Estados miembros. La Comisión, con arreglo al procedimiento del artículo 9, establecerá criterios para que los Estados miembros determinen si procede designar un

determinado organismo. La conformidad con los requisitos del anexo III establecida por dichos organismos será reconocida por todos los Estados miembros.

5. La Comisión, con arreglo al procedimiento del artículo 9, podrá determinar, y publicar en el Diario Oficial de las Comunidades Europeas, los números de referencia de las normas que gocen de reconocimiento general para productos de firma electrónica. Los Estados miembros presumirán que los productos de firma electrónica que se ajusten a dichas normas son conformes con lo prescrito en la letra f) del anexo II y en el anexo III de la presente Directiva.

6. Los Estados miembros y la Comisión cooperarán para promover el desarrollo y la utilización de los dispositivos de creación de firma, a la luz de las recomendaciones para la verificación segura de firma que figuran en el anexo IV y en interés del consumidor.

7. Los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate.

Estas prescripciones no deberán obstaculizar los servicios transfronterizos al ciudadano.

Artículo 4

Principios del mercado interior

1. Los Estados miembros aplicarán las disposiciones nacionales que adopten en cumplimiento de la presente Directiva a los proveedores de servicios de certificación establecidos en su territorio y a los servicios prestados por ellos. Los Estados miembros no podrán restringir la prestación de servicios de certificación en los ámbitos regulados por la presente Directiva que procedan de otro Estado miembro.

2. Los Estados miembros velarán por que los productos de firma electrónica que se ajusten a lo dispuesto en la presente Directiva puedan circular libremente en el mercado interior.

Artículo 5

Efectos jurídicos de la firma electrónica

1. Los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y sea admisible como prueba en procedimientos judiciales.

2. Los Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que:

- ésta se presente en forma electrónica, o

- no se base en un certificado reconocido, o

- no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o

- no esté creada por un dispositivo seguro de creación de firma.

Artículo 6

Responsabilidad

1.- Los Estados miembros garantizarán, como mínimo, que el proveedor de servicios de certificación que expida al público un certificado presentado como certificado reconocido o que garantice al público tal certificado, será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en el certificado por lo que respecta a:

a) la veracidad, en el momento de su expedición, de toda la información contenida en el certificado reconocido y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos;

b) la garantía de que, en el momento de la expedición del certificado, obraban en poder del firmante identificado en el certificado reconocido los datos de creación de firma correspondientes a los datos de verificación de firma que constan o se identifican en el certificado;

c) la garantía de que los datos de creación y de verificación de firma pueden utilizarse complementariamente, en caso de que el proveedor de servicios de certificación genere ambos; salvo que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia.

2. Los Estados miembros garantizarán como mínimo que el proveedor de servicios de certificación que haya expedido al público un certificado presentado como certificado reconocido será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en dicho certificado por no haber registrado la revocación del certificado, salvo que el proveedor de servicios de certificación pruebe que no ha actuado con negligencia.

3. Los Estados miembros velarán por que el proveedor de servicios de certificación pueda consignar en un certificado reconocido límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles para terceros. El proveedor de servicios de certificación no deberá responder de los daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites indicados en el mismo.

4. Los Estados miembros velarán por que el proveedor de servicios de certificación pueda consignar en el certificado reconocido un valor límite de las transacciones que puedan realizarse con el mismo, siempre y cuando los límites sean reconocibles para terceros. El proveedor de servicios de certificación no será responsable por los perjuicios que pudieran derivarse de la superación de este límite máximo.

5. Las disposiciones de los apartados 1 a 4 se aplicarán sin perjuicio de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores(8).

Artículo 7

Aspectos internacionales

1. Los Estados miembros velarán por que los certificados expedidos al público como certificados reconocidos por un proveedor de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si se cumple alguna de las condiciones siguientes:

a) que el proveedor de servicios de certificación cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro;

b) que un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva, avale el certificado;

c) que el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

2. Para facilitar tanto la prestación de servicios transfronterizos de certificación con terceros países como el reconocimiento legal de las firmas electrónicas avanzadas originarias de estos últimos, la Comisión presentará, en su caso, propuestas para lograr el efectivo establecimiento de normas y acuerdos internacionales aplicables a los servicios de certificación. En particular, y en caso necesario, solicitará al Consejo mandatos para la negociación de acuerdos bilaterales y multilaterales con terceros países y organizaciones internacionales. El Consejo se pronunciará por mayoría cualificada.

3. Cuando la Comisión sea informada de cualquier dificultad encontrada por las empresas comunitarias en relación con el acceso al mercado en terceros países, podrá, en caso necesario, presentar propuestas al Consejo para obtener un mandato adecuado para la negociación de derechos comparables para las empresas comunitarias en dichos terceros países. El Consejo se pronunciará por mayoría cualificada. Las medidas tomadas en virtud del presente apartado se entenderán sin perjuicio de las obligaciones de la Comunidad y de los Estados miembros con arreglo a los acuerdos internacionales pertinentes.

Artículo 8

Protección de datos

1. Los Estados miembros velarán por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos(9).

2. Los Estados miembros velarán por que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales directamente del titular de los datos o previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado. Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento explícito de su titular.

3. Sin perjuicio de los efectos jurídicos concedidos a los seudónimos con arreglo al Derecho nacional, los Estados miembros no impedirán al proveedor de servicios de certificación que consigne en el certificado un seudónimo del firmante en lugar de su verdadero nombre.

Artículo 9

Comité

1. La Comisión estará asistida por el Comité de firma electrónica (denominado en lo sucesivo "el Comité"), compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. En los casos en que se haga referencia al presente apartado, se aplicará el procedimiento de gestión previsto en el artículo 4 de la Decisión 1999/468/CE observando lo dispuesto en el artículo 8 de la misma. El plazo previsto en el apartado 3 del artículo 4 de la Decisión 1999/468/CE será de tres meses.

3. El Comité aprobará su Reglamento interno.

Artículo 10

Funciones del Comité

El Comité procederá a la clarificación de los requisitos establecidos en los anexos, los criterios a que se refiere el apartado 4 del artículo 3 y las normas para los productos de firma electrónica que gocen de reconocimiento general establecidas y publicadas con arreglo a lo dispuesto en el apartado 5 del artículo 3, conforme al procedimiento establecido en el apartado 2 del artículo 9.

Artículo 11

Notificación

1. Los Estados miembros interesados notificarán a la Comisión y a los demás Estados miembros lo siguiente:

a) información sobre los sistemas voluntarios de acreditación de ámbito nacional, incluidos cualesquiera requisitos adicionales con arreglo al apartado 7 del artículo 3;

b) el nombre y dirección de los organismos nacionales competentes en materia de acreditación y supervisión, así como de los organismos a que se refiere el apartado 4 del artículo 3; y c) el nombre y dirección de todos los proveedores nacionales de servicios de certificación acreditados.

2. Toda la información facilitada en virtud del apartado 1 y cualquier modificación de su contenido serán notificadas por los Estados miembros a la mayor brevedad.

Artículo 12

Revisión

1. La Comisión procederá al examen de la aplicación de la presente Directiva y presentará el oportuno informe al Parlamento Europeo y al Consejo a más tardar el 19 de julio de 2003.

2. Dicho examen permitirá, entre otras cosas, determinar si conviene modificar el ámbito de aplicación de la presente Directiva en vista de la evolución tecnológica y comercial y del contexto jurídico. El informe incluirá, en particular, una valoración de los aspectos de armonización, basada en la experiencia adquirida. El informe irá acompañado, en su caso, de propuestas legislativas.

Artículo 13

Aplicación

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva antes del 19 de julio de 2001. Informarán inmediatamente de ello a la Comisión. Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 14

Entrada en vigor

La presente Directiva entrará en vigor el día de su publicación en el Diario Oficial de las Comunidades Europeas.

Artículo 15

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el 13 de diciembre de 1999.

Por el Parlamento Europeo

La Presidenta

N. FONTAINE

Por el Consejo

El Presidente

S. HASSI

(1) DO C 325 de 23.10.1998, p. 5.

(2) DO C 40 de 15.2.1999, p. 29.

(3) DO C 93 de 6.4.1999, p. 33.

(4) Dictamen del Parlamento Europeo de 13 de enero de 1999 (DO C 104 de 14.4.1999, p. 49), Posición común del Consejo de 28 de junio de 1999 (DO C 243 de 27.8.1999, p. 83) y Decisión del Parlamento Europeo de 27 de octubre de 1999 (no publicada aún en el Diario Oficial), Decisión del Consejo de 30 de noviembre de 1999.

(5) DO L 367 de 31.12.1994, p. 1; Reglamento modificado por el Reglamento (CE) n° 837/95 (DO L 90 de 21.4.1995, p. 1).

(6) DO L 367 de 31.12.1994, p. 8; Decisión cuya última modificación la constituye la Decisión 1999/193/CE (DO L 73 de 19.3.1999, p. 1).

(7) DO L 184 de 17.7.1999, p. 23.

(8) DO L 95 de 21.4.1993, p. 29.

(9) DO L 281 de 23.11.1995, p. 31.

ANEXO I

Requisitos de los certificados reconocidos

Los certificados reconocidos habrán de contener:

a) la indicación de que el certificado se expide como certificado reconocido;

b) la identificación del proveedor de servicios de certificación y el Estado en que está establecido;

c) el nombre y los apellidos del firmante o un seudónimo que conste como tal;

d) un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado;

e) los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del firmante;

f) una indicación relativa al comienzo y fin del período de validez del certificado;

g) el código indentificativo del certificado;

h) la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado;

i) los límites de uso del certificado, si procede; y

j) los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

ANEXO II

Requisitos de los proveedores de servicios de certificación que expiden certificados reconocidos

Los proveedores de servicios de certificación deberán:

a) demostrar la fiabilidad necesaria para prestar servicios de certificación;

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

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

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

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

f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

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

h) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado;

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

j) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves;

k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado;

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

- sólo personas autorizadas puedan hacer anotaciones y modificaciones,

- pueda comprobarse la autenticidad de la información,

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

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

ANEXO III

Requisitos de los dispositivos seguros de creación de firma electrónica

1. Los dispositivos seguros de creación de firma garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

a) los datos utilizados para la generación de firma sólo pueden producirse una vez en la práctica y se garantiza razonablemente su secreto;

b) existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad;

c) los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.

2. Los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma.

ANEXO IV

Recomendaciones para la verificación segura de firma

Durante el proceso de verificación de firma, deberá garantizarse, con suficiente certeza, que:

a) los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador;

b) la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente;

c) el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados;

d) se verifican de forma fiable la autenticidad y la validez del certificado exigido al verificarse la firma;

e) figuran correctamente el resultado de la verificación y la identidad del firmante;

f) consta claramente la utilización de un seudónimo; y

g) puede detectarse cualquier cambio pertinente relativo a la seguridad.

ANEXO XIII

LEY DE COSTA RICA

PROYECTO DE LEY No. 14.276 "LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES"

Ley de Firma Digital y Certificados Digitales

CAPITULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- La presente Ley tiene por objetivo reconocer y regular el uso de la Firma Digital y los Certificados Digitales, otorgándole a los documentos firmados digitalmente la misma validez y eficacia jurídica que aquellos con firma manuscrita que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización.

ARTÍCULO 2.- Para los propósitos de la presente Ley se establecen las siguientes definiciones:

1.- **Acreditación:** Es el procedimiento mediante el cual la Autoridad de Acreditación, creada en esta ley, reconoce formalmente que una entidad o empresa es competente para realizar las tareas de certificación digital, de acuerdo a normas nacionales e internacionales.
2.- **Acreditación voluntaria del prestador de servicios de certificación:** Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se emite, a petición del interesado, por la Autoridad de Acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa internacional aplicable.
3.- **Certificado Digital:** Es la estructura de datos que vincula unos datos de verificación de firma a un signatario y confirma su identidad, vinculándola con su firma digital.
4.- **Certificado Digital Reconocido:** Es el certificado digital que cumple con los requisitos establecidos en la presente Ley y su reglamento, y que vincula una firma digital con determinada entidad como su signatario, mediante un proceso seguro de certificación y verificación; es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la Autoridad de Acreditación.
5.- **Datos de creación de firma:** Son los datos únicos, como códigos, atributos biométricos o claves criptográficas privadas, que el signatario utiliza para crear su Firma Digital. Estos datos quedan en entredicho si se ha perdido su secretividad o control exclusivo por parte del signatario.

6.- **Documento electrónico:** es toda representación electrónica de actos, hechos, datos o descripciones, y que se puede recuperar o reproducir en una forma perceptible e inteligible

7.- **Documento digital:** es un documento electrónico cuyo contenido está codificado en dígitos binarios. En la presente Ley se utilizará el término digital entendido como cualquier información codificada en dígitos binarios.

8.- **Firma Digital:** Es el conjunto de datos asociados funcionalmente a un documento electrónico, utilizados como medio para identificar formalmente al firmante e indicar que este aprueba el contenido del documento.

9.- **Firma Digital Acreditada:** Es la Firma Digital certificada por un prestador de servicios de certificación debidamente acreditado ante la Autoridad de Acreditación.

10.- **Información Íntegra:** aquella información que haya permanecido completa e inalterada, sin menoscabo de cualquier adición o cambio accesorio, inherente al proceso de comunicación, almacenamiento, archivo o presentación.

11.- **Mensaje de datos:** Es la información generada, enviada, recibida, almacenada, o comunicada por medios digitales, electrónicos, ópticos o similares.

12.- **Prestador de servicios de certificación o entidad certificadora:** Es la persona física o jurídica que expide certificados.

13.- **Dispositivo o Procedimiento de verificación:** Es el proceso empleado con el propósito de verificar que una Firma Digital es atribuible a determinada persona como su signatario, o para detectar cambios y errores en un documento digital.

14.- **Parte que confía:** persona que puede actuar sobre la base de un certificado o de una firma digital.

15.- **Signatario:** Es la persona física o jurídica que cuenta con un mecanismo de creación de firma, que actúa en nombre propio o con poderes de representación de otra persona física o jurídica.

ARTÍCULO 3.-Ninguna de las disposiciones de la presente Ley, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear, de forma segura, una firma digital acreditada, que cumpla los requisitos de esta ley.

ARTÍCULO 4.- La Firma Digital, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá

respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel.

Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento digital, si el mismo ha sido firmado mediante una Firma Digital Acreditada.

Se presumirá que la Firma Digital y el medio de creación de firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en esta Ley cuando el certificado digital reconocido es emitido por un prestador de servicios de certificación acreditado ante la Autoridad de Acreditación.

ARTÍCULO 5.- Cuando una ley requiere que un documento o firma esté certificado o de cualquier otra forma reconocida, verificado tal requisito se tendrá por cumplido si una firma digital acreditada de un funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma Digital acreditada.

ARTÍCULO 6.- Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales y cualquier dependencia del sector público, incluso en las estructuras según modelos organizacionales del Derecho Privado para la utilización de la firma Digital acreditada en los documentos electrónicos en sus relaciones internas, entre ellos y con las particulares, así como para poder actuar como entidades certificadoras siempre que cumplan todos los requisitos que para ese efecto se establezcan, de conformidad con las previsiones de esta Ley y su reglamento. En lo atinente a los documentos electrónicos firmados digitalmente se deberá cumplir en los que sea aplicable con lo que establece la Ley 7202, Ley del Sistema Nacional de Archivos.

ARTÍCULO 7.- Los dispositivos seguros de creación de Firma Digital para considerarse como tales deberán cumplir con:

1.- Garantizar que los datos utilizados para la generación de firma puedan producirse sólo una vez y corresponden exclusivamente al firmante, asegurando razonablemente su secreto, dentro de las posibilidades o limitaciones tecnológicas.
2.- Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado y que es posible detectar cualquier alteración de la firma hecha con posterioridad al momento de firmar.
3.- Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros y que en el momento de firmar están bajo su control.
4.- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.
5.- Que sea posible detectar cualquier alteración de esa información, hecha con posterioridad al momento de firmar.

ARTÍCULO 8 Los dispositivos de verificación de Firma Digital Acreditada deben garantizar al menos lo siguiente:
1.- Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.
2.- Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.
3.- Que aparezca correctamente la identidad del signatario.
4.- Que se verifique de forma fiable el certificado.
5.- Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.
6.- Los demás que el reglamento establezca.

ARTÍCULO 9.- Las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte.

CAPITULO II
DEL ÓRGANO RECTOR Y
LA AUTORIDAD ACREDITADORA

ARTÍCULO 10.- El Ministerio de Ciencia y Tecnología será el Órgano Rector en todo lo concerniente a esta Ley.

Toda interpretación técnica estará bajo el mejor criterio del Órgano Rector tomando en cuenta los avances tecnológicos, así como los requerimientos y realidades del país.

ARTICULO 11.- Créase la Autoridad Acreditadora como órgano subordinado al Ministro de Ciencia y Tecnología y entre sus funciones estarán:

a) Autorizar la actividad de las entidades de certificación en el territorio nacional otorgando licencias de operación.
b) Fiscalizar el funcionamiento y la eficiente prestación del servicio por parte de las Entidades de Certificación.
c) Imponer sanciones a las Entidades de Certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.
d) Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las Entidades de Certificación.
e) Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en la presente ley.
f) Mantener, procesar, clasificar, resguardar y custodiar el Registro de las Entidades de Certificación de acuerdo a lo dispuesto en los reglamentos respectivos.
g) Recaudar multas de acuerdo a lo dispuesto en los reglamentos respectivos.
h) Actuar como mediador en la solución de conflictos que se susciten entre las Entidades de Certificación y sus usuarios, cuando ello sea solicitado por al menos una de las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el

usuario, conforme a esta ley y los reglamentos respectivos.

i) La demás que le asigne el reglamento.

ARTÍCULO 12.- Mediante la Autoridad de Acreditación, las empresas que emitan certificados de firma digital deberán someterse al proceso de acreditación que se defina en el reglamento.

Serán funciones de las empresas certificadoras las de emitir, suspender, cancelar o revocar certificados digitales, así como brindar otros servicios inherentes al propio certificado

ARTÍCULO 13.- La Autoridad de Acreditación así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen las empresas certificadoras.

ARTÍCULO 14- El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizará un sistema de acreditación, en el ámbito de los prestadores de servicios de certificación de Firma Digital, coordinando para ello con la Autoridad de Acreditación.

La Autoridad de Acreditación mediante la función de acreditación, reconoce formalmente que una organización es competente para llevar a cabo tareas específicas de certificación digital, de acuerdo a los requisitos de normas nacionales e internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente los derechos de los usuarios.

Para ello deberá llevar a cabo el proceso de evaluación correspondiente, llevar un registro de las entidades acreditadas y velar por que se cumplan los requisitos establecidos por esta Ley y su reglamento mediante prácticas de supervisión y auditorías de seguridad informática.

CAPÍTULO III
DE LOS CERTIFICADOS DIGITALES

ARTÍCULO 15.- Los certificados digitales se vinculan con una persona, confirmando su identidad, los cuales deberán contener al menos:

1. Los datos que identifiquen individualmente al firmante.
2. Las normas utilizados para la creación de la firma.
3. Los datos que identifiquen a la entidad de certificación.
4. Número de serie del certificado.
5. Fecha de emisión y plazo de vigencia.
6. Los demás que el reglamento establezca.

ARTÍCULO 16.- Los certificados digitales se suscriben mediante un contrato de servicios de certificación digital entre el suscriptor, que será el titular de la firma, y el prestador de servicios de certificación digital acreditado ante la Autoridad de Acreditación.

ARTÍCULO 17.- Los certificados digitales se podrán suspender, cancelar y revocar, según el caso, en las siguientes circunstancias:

1. A solicitud del titular de la firma.
2. Por expiración del plazo de vigencia del certificado.
3. Por cese de operaciones de la entidad de certificación.
4. Por muerte del titular de la Firma Digital.
5. Por incumplimiento contractual con la entidad de certificación.
6. Por orden de un juez.
7. Las demás que el reglamento establezca.

ARTÍCULO 18.- Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por prestadores establecidos y acreditados en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y reconocidos por la autoridad de acreditación competente y cumpliendo con los requisitos fijados en esta Ley, su reglamento y normas internacionales correspondientes.

CAPÍTULO IV
DEBERES DE LAS PARTES INTERVINIENTES

Artículo 19. - Para crear una firma digital el firmante deberá:

1. Actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

2. Sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación o esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma digital o prestar servicios que la apoyen si:
    - **a)** El firmante sabe que los datos de creación de la firma han quedado en entredicho; o
    - **b)** Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

3. Actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado que refrende su firma o que hayan de consignarse en él, son exactas y completas.

Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los deberes anteriores.

Artículo 20. - El prestador de servicios de certificación, que preste servicios para apoyar una firma digital que pueda utilizarse con efectos jurídicos, deberá:

1. Actuar de conformidad con las declaraciones que hizo ante la Autoridad de Acreditación respecto de sus normas, políticas y prácticas;
2. Actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado que emite o que estén consignadas en él, son exactas y completas;
3. proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:
    - **a)** La identidad del prestador de servicios de certificación.
    - **b)** Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;
    - **c)** Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

4. Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda,

permitan a ésta determinar mediante el certificado o de otra manera:

a) El método utilizado para comprobar la identidad del firmante;

b) Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

c) Si los datos de creación de la firma son válidos y no están en entredicho;

d) Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

e) Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho; en caso afirmativo, el prestador de servicios de certificación debe efectivamente proporcionar ese medio al firmante para que dé aviso;

f) Si se ofrece un servicio para revocar oportunamente el certificado; en caso afirmativo, el prestador de servicios de certificación debe cerciorarse de que existe un servicio efectivo para revocar oportunamente el certificado;

5. Al prestar sus servicios, utilizar sistemas, procedimientos y recursos humanos fiables.

Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los deberes anteriores

Artículo 21. - Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

1. verificar la fiabilidad de la firma electrónica;
2. verificar la validez, suspensión o revocación del certificado;
3. tener en cuenta cualquier limitación explícita en el certificado.

ARTÍCULO 22. Para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios

de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) Los recursos humanos y financieros, incluida la existencia de un activo;
b) La calidad de los sistemas de equipo y programas informáticos;
c) Los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;
d) La disponibilidad de información para los firmantes nombrados en el Certificado y para las partes que confíen en éste;
e) La periodicidad y el alcance de la auditoría por un órgano independiente;
f) La existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y
g) Cualesquiera otros factores pertinentes

CAPITULO V
SANCIONES

ARTÍCULO 23.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que, en el ejercicio de su actividad, ocasionen por la certificación u homologación de certificados de firmas digitales. En todo caso corresponderá al prestador de servicios de certificación demostrar que actuó con la debida diligencia.

Sin perjuicio de lo anterior, los prestadores de servicios de certificación no serán responsables de los daños o perjuicios que tengan en su origen el uso indebido o fraudulento de un certificado de firma digital por parte del suscriptor.

ARTÍCULO 24.- Para los efectos de la presente ley se consideran infracciones por parte de los prestadores de servicios de certificación, el incumplimiento de cualquiera de las disposiciones contenidas en esta ley y la negligencia en la prestación del servicio.

ARTÍCULO 25.- La Autoridad de Acreditación, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, según la naturaleza y la gravedad de la falta las siguientes

sanciones a los prestatarios del servicio de certificación que incumplan o violen las normas contenidas en la presente ley:

A) Amonestación por escrito
B) Multa de_5_ hasta_20_ salarios base, de acuerdo con el artículo 2 de la Ley 7333.
C) Suspensión inmediata de todas o algunas de las actividades de la entidad infractora.
D) Prohibición a la entidad infractora de prestar directa o indirectamente los servicios de entidad de certificación por el término de hasta 5 años.
E) Revocación definitiva de la acreditación y prohibición para operar en Costa Rica como entidad de certificación acreditada.

ARTÍCULO 26.- Las resoluciones de la Autoridad de Acreditación podrán ser impugnadas por los interesados cuando consideren que han sido perjudicados en sus intereses legítimos o en sus derechos.

Contra dichas resoluciones podrá ser interpuesto el recurso de reconsideración contra la propia Autoridad de Acreditación o apelación ante el Titular del Ministerio de Ciencia y Tecnología.

La Autoridad de Acreditación contará con un plazo de dos meses para decidir sobre el recurso de reconsideración interpuesto. Si en tal plazo no ha sido resuelto el recurso, la decisión se considerará favorable al recurrente.

De la misma forma, el Ministro de Ciencia y Tecnología dispondrá de dos meses para resolver el recurso de apelación. Si en tal plazo este recurso no ha sido resuelto la decisión se considerará favorable al recurrente.

CAPÍTULO VI
DISPOSICIONES FINALES

ARTÍCULO 27.- El Poder Ejecutivo deberá emitir el reglamento a la presente Ley dentro del plazo máximo de tres meses siguientes a su publicación.

Rige a partir de su publicación.