UNIVERSIDAD DE PANAMÁ

VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

MAESTRIA EN DERECHO CON ESPECIALIZACIÓN
EN CIENCIAS PENALES

EL DELITO DE FALSIFICACIÓN DE DOCUMENTO ELECTRÓNICO

GRETTEL DEL CARMEN VILLALAZ GUERRA

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA
OPTAR AL GRADO DE MAESTRO EN DERECHO CON
ESPECIALIZACIÓN EN CIENCIAS PENALES

PANAMÁ, REPÚBLICA DE PANAMÁ

2002

TM

UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

ACTA DE SUSTENTACIÓN DE TESIS
PROGRAMA DE MAESTRÍA EN

DERECHO CON ESPECIALIZACION EN CIENCIAS PENALES

Titulo del trabajo de tesis: " EL DELITO DE FALSIFICACION DE DOCUMENTOS ELECTRONICOS"

Nombre del estudiante: GRETIEL VILLALAZ GUERRA Cédula: 8-225-683

Miembros del Jurado:	***Calificaciones que otorgan:***
a DRA. AURA GUERRA DE VILLALAZ	95 - A
b DR. JOSE ACEVEDO	95 - A
c DRA. VIRGINIA ARANGO	91 - A
Nota final promedio:	93 - A

Observaciones generales del jurado:
EL TEMA SELECCIONADO ES ACTUAL, INTERESANTE Y NOVEDOSO EN EL AMBITO JURIDICO PENAL DE NUESTRO PAIS.

EL TRABAJO FUE REDACTADO Y SUSTENTADO DE CONFORMIDAD AL REGLAMENTO QUE RIGE EN ESTE TIPO DE INVESTIGACIONES, A NIVEL DE MAESTRIA.

EL ANALISIS DE LA LEY 43 DE 2001 SOBRE COMERCIO ELECTRONICO ES UNA BASE LEGAL IMPORTANTE QUE SE PUEDE COMPLEMENTAR CON LA PROTECCION PENAL A LOS DOCUMENTOS ELECTRONICOS TAL COMO LO RECOMIENDA LA AUTORA DE ESTE TRABAJO, CUYA PUBLICACION AYUDARIA A LA DIVULGACION DEL TEMA CON MIRAS A SU INCORPORACION AL CODIGO PENAL.

Firma de los miembros del jurado:

a

b

c

Firma del coordinador del programa

Firma del representante de la Vicerrectoría de Inv. y Postgrado

Firma del estudiante

Firma del decano
Facultad de Derecho y Ciencias Políticas

Fecha

10 ENE 2006

Adjuntar el cuerpo

13355

AGRADECIMIENTO

Por todo el apoyo y colaboración recibido durante la elaboración de esta tesis de grado, agradezco muy especialmente a:

Prof. Dra. Aura E. Guerra de Villalaz

Licenciado Edgardo Villalobos

Licenciada Delia Cárdenas

Licenciada Doris Vargas de Cigarruista

A mi esposo Douglas
Y a mis hijos Alexander y Brian
Por todo el tiempo permitido en este trabajo.

EL DELITO DE FALSIFICACIÓN DE DOCUMENTO ELECTRÓNICO

Página

CAPITULO TERCERO

ASPECTOS PROCESALES DEL DELITO DE FALSIFICACION DE DOCUMENTOS

CAPITULO QUINTO

ANALISIS DE ENTREVISTAS REALIZADAS

INDICE DE FIGURAS

RESUMEN

En el presente trabajo de investigación se analiza lo que debemos entender por documento electrónico, sus características y los diferentes dispositivos que pueden llegar a alterarse: cambiando, transformando o falsificando lo que se transmite en ese medio, como son ideas, conceptos, fotos, gráficos y hasta sonidos, que deben ser protegidos por el Estado, a fin que haya confianza en estos instrumentos, capaces de establecer y generar obligaciones. La metodología utilizada consiste en un análisis de la doctrina desarrollada por los autores que han investigado este tema y la legislación que contiene materias relacionadas con el tema objeto de investigación. Como parte de la metodología y con el propósito de analizar en la práctica el conocimiento que tiene nuestra sociedad sobre los daños y perjuicios que causa la falsificación de documentos electrónicos, el trabajo incluye la realización de unas entrevistas de distintos temas con profesionales y funcionarios directamente relacionados con la custodia y emisión de documentos electrónicos en nuestro medio, señalándose que la falsificación de documentos electrónicos es un medio para la comisión de otras formas delictivas tipificadas en nuestro Código Penal, lo cual causa perjuicios millonarios no sólo a la empresa o entidad afectada, sino también a los terceros que confían en los nuevos instrumentos de transmisión de información, que permiten transacciones rápidas, pero no tan seguras. Debido a estas entrevistas, se pudo diagnosticar que es posible que se dé con más frecuencia la comisión del delito de falsificación de documentos electrónicos por personal que labora o laboró en las empresas generadoras de dichos documentos y hay consenso en la necesidad que se mejore la legislación concerniente a la protección de los documentos electrónicos y la debida tipificación de las conductas que lo afecten de acuerdo a los esfuerzos de países más avanzados en esta materia.

SUMMARY

In the following research there is an analysis of the meaning of the electronic documents, theirs characteristics and how this could be altered: changing, transforming and altering the documents, that could be ideas, concepts, photos, pictures, graphics and sounds, that need the protection of the State, the Government, because the society need to believe in this instruments called electronic documents, because could be generate obligations. Also, the methodology used is the analysis of documents, according the doctrine developed by the authors who have surveyed on this specific topic. Similary, the laws containing the subject matter related to the main objective on this type of research. Likewise, the jurisprudence which it is been applied in criminal cases about the falsification of electronic documents. In addition, as part of the methodology and with the intention of analyzing within the professionals that manipulate electronic documents or people that work with the security of the electronic documents, I present the realization of interviews of diverse themes with the corresponding analysis ante the presentation of the final results. Taking into consideration these results, the principal author the crime of falsification in electronic documents could be the personal that work in the institution that emit this instrument. And all recommendation a best law or reglamentation to rule the emission of electronic documents, according the law of other countries, because the actual society need this instruments for fast and security transactions.

INTRODUCCIÓN

El presente trabajo de investigación denominado EL DELITO DE FALSIFICACION DE DOCUMENTO ELECTRÓNICO, es un estudio exploratorio, en el que se analizan diversos aspectos de la alteración, manipulación o destrucción de los documentos electrónicos, que ocasiona una lesión a la fe pública, en primera instancia y subsecuentemente a otros bienes jurídicos protegidos, dependiendo del interés del autor, como son la libertad, el patrimonio, el pudor y la libertad sexual, la seguridad colectiva y la economía nacional.

La polimórfica realidad de los delitos de falsedad de documentos electrónicos, se refleja por su relación directa con todo el sistema informático y el procesamiento automatizado de datos, que no ha terminado de desarrollarse, y sin embargo, lo hace a tal velocidad, que hoy es evidente la gran cantidad de contrataciones comerciales, operaciones en la bolsa de valores o servicios de compra y pagos integrados, que se dan todos los días, que representan una gran potencialidad lesiva para intereses personales y colectivos

Sin embargo, el principio de intervención mínima o carácter de última *ratio* del Derecho Penal, supone que a pesar de la nueva visión que debe tenerse ante la comisión de posibles conductas peligrosas por la falsificación de documentos electrónicos, sólo deberá aplicarse cuando las medidas disponibles en otros sectores del ordenamiento no resulten suficientes para la protección del bien jurídico.

El trabajo está dividido en 5 Capítulos y 1 Anexo. En el Primer Capítulo se hace un análisis del concepto y noción de los documentos electrónicos, clases de documentos y las características del mismo, señalándose las siguientes: que es una cosa material, que no posee caracteres de grafía personal directa, que tiene una finalidad representativa y que está contenido en un soporte magnético o electrónico.

El Segundo Capítulo, trata sobre las modalidades típicas de la conducta de falsificación en documento electrónico, señalando las formas de hacer, formar, suprimir, ocultar o destruir un documento electrónico y las formas activa y omisiva de la acción.

El Tercer Capítulo hace un análisis de los aspectos procesales del delito de falsificación en documento electrónico, debido a la

novedad y diferencias fundamentales con los métodos tradicionales de ejecución del delito, que hacen de la investigación y prueba del delito de falsedad de documento electrónico, algo novedoso en materia procesal. En ese mismo capítulo, se hace un análisis de la determinación en el tiempo y el espacio de la ley penal aplicable, que nos permite reconocer que le regulación de esta materia debe ser acorde a las normas que se emitan en consenso con otras latitudes.

El Cuarto Capítulo hace un análisis de las consideraciones de política criminal que se deben hacer en materia de falsificación de documentos electrónicos, debido a que los documentos electrónicos ya están siendo digitalizados, y por tanto, su forma de transmisión se está dando en forma masificada, lo cual amplía la posibilidad que se vulneren los derechos de las personas en la comisión de este delito. Se hace un análisis de los peligros y garantías que existen en el medio con las nuevas tecnologías, las políticas internacionales en materia de informática y las consideraciones que se deben hacer para poder tutelar y proteger legalmente la información y generación de datos con la nueva tecnología

El Capítulo Quinto , analiza la entrevista realizada a funcionarios y personal de empresas privadas, sobre los diferentes aspectos de esta investigación. De dicha investigación surgen interesantes resultados, que son analizados y que principalmente se refieren al conocimiento y la opinión de personas relacionadas con documentos electrónicos.

Las conclusiones expuestas se refieren, entre otros aspectos, a la ausencia de regulación jurídica, que por ahora se ha ido cubriendo con la aplicación de la ley penal castigando otras conductas igualmente tuteladas por el Derecho Penal, pero que deben necesariamente mejorarse con una nueva legislación sobre la materia, desarrollándose en la doctrina citada; así como las entrevistas aplicadas.

La investigación incluye un Anexo que contiene la Ley 43 de 31 de julio de 2001, que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos, el formato de la encuesta aplicada, artículos y noticias sobre falsedad de documentos electróncios y los cuadros utilizados para elaborar las gráficas (figuras) plasmadas en la encuesta.

La metodología desarrollada en este trabajo, consiste en el análisis de documentos jurídicos, doctrina y entrevistas, sobre las cuales se presenta unas recomendaciones y resultados.

Lo planteado en este trabajo, permite establecer ciertas cuestiones de carácter jurídico-penal, en lo relacionado con el delito de falsificación en documento electrónico y la formulación de propuestas en materia de política criminal, que no desconozcan los principios de proporcionalidad y racionalidad; y se logre además un grado de información jurídica con las nuevas tecnologías, que no tienen fronteras ni distancias geográficas.

CAPITULO PRIMERO

NOCIONES GENERALES SOBRE DOCUMENTO ELECTRONICO

I.- CONCEPTO DE DOCUMENTO ELECTRONICO

En atención a las nuevas tecnologías que dominan las formas de comunicación y atestación en los inicios del siglo XXI y que generan diariamente toneladas de documentos, transmitiendo ideas, conceptos, contratos, fotos, gráficos, planos y hasta sonidos; se hace imperante la definición y concepción de lo que hoy debemos entender por documento electrónico, que permita establecer la amplitud de protección que el Estado debe regular y hacer respetar, para que haya confianza en estos instrumentos, que son de fácil acceso a todos.

El ascendente uso común de documentos producidos por medios electrónicos, y la progresión del fenómeno informático nos permiten hablar de **documentos electrónicos** o **documentos informáticos**, con un tratamiento especial en todos los sentidos del derecho, por las diversas formas que toman dichos instrumentos. [1]

---

[1] Vease **VILLALOBOS, Edgardo.** INTRODUCCION A LA INFORMATICA INFORMATICA JURIDICA Y DERECHO INFORMATICO Alfa Omega Impresores Panama 1997 p 158

Si bien es cierto que a la fecha no existen criterios unánimes y claros entre los estudiosos del Derecho Penal en torno a la concepción de lo que debemos entender por documento electrónico, la realidad es que cada nuevo avance tecnológico que se da en el complejo sistema de redes, satélites, computadoras e impulsos eléctricos, ha demostrado que los defraudadores y falsificadores, así como cualquier persona que quiera sacar un provecho ilegal de un documento, lleva un gran tramo de ventaja en técnicas de falsificación que el resto de la sociedad, lo que hacen de una importancia extraordinaria la delimitación del concepto de documento electrónico en la tipicidad de los posibles ilícitos que el Estado quiera prevenir y evitar, para lograr la confianza en esta nueva forma de comercio de manera positiva.

a.- Noción de Documento Electrónico

Las transformaciones que se han dado a través de los siglos de los métodos utilizados por las personas para transmitir una idea, van desde los jeroglíficos en los murales egipcios, la documentación por escrito gracias a la imprenta ideada por Gutemberg, hasta la transferencia electrónica de documentos por medio de las computadoras, sistema de redes e internet.

La producción de documentos es de vital importancia en el día de hoy, especialmente en las transferencias y obligaciones comerciales, sociales y bancarias de nuestra sociedad, por medios electrónicos; ese instrumento de transferencia ha dado lugar a que se denomine este tipo de instrumento como: "documento electrónico". Sin embargo, es necesario determinar si para el tráfico jurídico, y para el derecho penal, estos instrumentos que pueden ser impresos y reproducidos se deben considerar como **documentos** y tratarlos como tales con las mismas particularidades de lo que hasta ahora se ha considerado como documento propiamente tal.

En un análisis etimológico de la palabra documento, debemos recordar que la misma proviene del latín ***docere*** , vocablo que significa enseñar o ilustrar y que en sentido amplio es "toda representación material, destinada e idónea, para reproducir una cierta manifestación de pensamiento". [2]

Igualmente nos parece adecuada la definición del Dr. JORGE FÁBREGA, cuando expresa que documento es "... todo objeto que sirve para ilustrar o comprobar algo; toda representación objetiva destinada e

---

[2] TELLEZ VALDES, Julio DERECHO INFORMATICO Universidad Nacional Autonoma de Mexico Mexico 1987 p 117

idónea para reproducir una determinada manifestación de pensamiento, de voluntad o un hecho o suceso o incluso un acto de la naturaleza" [3], concepto este que permite introducir los instrumentos electrónicos en la categoría de documento.

Esta concepción genérica nos indica que los documentos escritos no son la única objetividad material que permite la incorporación de las ideas, sino toda manifestación física, que pueda reproducir o recoger el pensamiento humano, como lo es una copia, registros, fotografías, etc., constituyéndose en última instancia en variedades de la prueba documental.

MUÑOZ CONDE señala, para aclarar el concepto de documento, que es "la incorporación de un pensamiento por signos escritos, bien usuales o convencionales, que se pueda atribuir a una persona, que esté destinado a entrar en el tráfico jurídico y que sea adecuado objetivamente para tener efecto jurídico". [4]

Dicho concepto concuerda con la definición que nos ofrece el artículo 832 del Código Judicial panameño, que da amplitud a los

---

[3] **FABREGA, Jorge.** MEDIOS DE PRUEBA 2 LA PRUEBA EN MATERIA MERCANTIL Segunda Edicion Editora Juridica Panameña Panama 1998 p 145

[4] **MUÑOZ CONDE, Francisco.** DERECHO PENAL PARTE ESPECIAL 7a ed Tirant Lo Blanch Valencia 1988 p 500-501

instrumentos y objetos que pueden ser considerados documentos y que en un momento dado puedan tener un efecto jurídico.

> *ARTICULO 832: Son documentos los escritos, escrituras, certificaciones, copias, impresos, planos, dibujos, cintas, cuadros, fotografías, radiografías, discos, grabaciones magnetofónicas, boletos, contraseñas, cupones, etiquetas, sellos, telegramas, radiogramas y en general, todo objeto mueble que tenga carácter representativo o declarativo y las inscripciones en lápidas, monumentos, edificios y similares. Los documentos son públicos o privados.*

Esta norma, dada su amplitud, también nos ofrece suficiente apoyo legal para considerar a los instrumentos electrónicos como documentos, y dentro de la misma, nos permite determinar a su vez, si se trata de un documento público o privado.

Para analizar el documento electrónico, como documento público o privado, se hace necesario recurrir al artículo 856 del Código Judicial patrio, que señala:

> *ARTICULO 856. Documento privado es el que no reúne los requisitos para ser documento público..."*

En esta materia, la Dra. GUERRA DE VILLALAZ expone diáfanamente que el documento privado es obra de particulares, quienes lo confeccionan sin la intervención de un funcionario o personal oficial, y

que sólo cuando hay un reconocimiento por quienes lo crearon o suscribieron, podrá tener autenticidad, que es la que permite certeza con respecto a dicho instrumento.[5]

Sumándose a esta concepción, se encuentra lo planteado por BREWER, quien señala "Con el nombre de instrumentos o documentos privados se comprenden todos los actos o escritos que emanan de las partes, sin intervención del Registrador, el Juez o de otro funcionario competente y que se refieren a hechos jurídicos a los cuales pueden servir de prueba".[6]

Estas consideraciones, tanto las legales, como las de los autores mencionados, nos permiten identificar con propiedad, que el documento electrónico en general es un documento de naturaleza privada, el cual deberá ser analizado conforme a las reglas y solemnidades que exige la ley en materia de documentos privados, pero en los casos que dichos documentos sean generados por los Registradores de las Propiedades, Registradores del Estado Civil de las personas, Notarios u otros

---

[5] Vease **GUERRA DE VILLALAZ, Aura E.** DELITOS CONTRA LA FE PUBLICA (Tiulo VIII del Codigo Penal) Taller Senda Panama 1989 p 11

[6] **BREWER, Allan-Randolph** CONSIDERACIONES ACERCA DE LA DISTINCION ENTRE DOCUMENTO PUBLICO O AUTENTICO DOCUMENTO PRIVADO RECONOCIDO Y AUTENTICADO Y DOCUMENTO REGISTRADO Ediciones Labreton Caracas Venezuela 1995 p 275

servidores públicos, autorizados para ello; el documento electrónico, deberá ser considerado, sólo en esas circunstancias, como documento público.

En un plano de regulación más específica del documento electrónico, la Ley No. 43 de 31 de julio de 2001, define y regula todo lo relacionado a documentos y firmas electrónicas, así como las entidades de certificación de comercio electrónico e intercambio de documentos electrónicos, y llega a definir en su artículo 2, numeral 3 lo que debemos entender por documento electrónico, señalando que es:

> *ARTICULO 2. Definiciones. ...*
> *1....*
> *2...*
> *3. Documento electrónico. Toda representación electrónica que da testimonio de un hecho, una imagen o una idea.*
> *4....*
> *5...."*

En el análisis de esa representación electrónica, que se adecúa a documento electrónico, definida por la Ley 43, citada, podemos mencionar una cinta magnetofónica, una cinta cinematográfica, disquetes, discos compactos de escritura o sonido, tarjetas con banda magnética, chips o microchip, etc , los cuales deben ser leídos por un

dispositivo electrónico, y los llamados documentos informáticos, que son generados por impulsos electrónicos en una computadora, los que a su vez pueden ser captados por los sentidos del hombre, y que en un momento dado pueden ser considerados como documentos públicos o privados, dependiendo de la persona que los emita y las firmas o formalidades que se le adhieran.

b.- Características de los documentos electrónicos

Los avances tecnológicos, que se reflejan en documentos electrónicos, se han traducido en una serie de instrumentos que hoy nos permiten realizar una gran cantidad de transacciones, mismas que agilizan el comercio y facilitan el desenvolvimiento de la vida en general.

El conocimiento y delimitación del documento electrónico es indudablemente necesario para confiar en la materialización de los actos que ellos contienen, ya que implican un riesgo permanente dada la rapidez de difusión de la información que se obtiene mediante estos instrumentos.

En ese sentido, el Derecho Penal está consciente de los efectos positivos y negativos de las actividades y consecuencias que generan los

documentos informáticos y poco a poco se han ido creando una serie de regulaciones que le garantizan al ciudadano particular la tutela o protección de la fe pública, el orden y respeto de sus derechos en las diversas y complejas actividades que requiere la vida en sociedad.

En cuanto a las características que nos permiten identificar cuando estamos frente a un documento electrónico, las señala el Licdo. VILLALOBOS, en su obra, así: "Acerca de las características del documento electrónico podemos mencionar las siguientes: 1. Es una cosa material. 2. No posee caracteres de grafía personal directa. 3. Tiene finalidad representativa. 4. Está contenido en un soporte magnético.". [7]

Examinemos cada una de esas características:

1. Es una cosa material: El señalamiento que los documentos electrónicos son una cosa material, es un hecho indubitable tanto para el derecho comercial, para el derecho procesal, como para el penal. Ello es así porque la única manera en que se pueda hacer una valoración de tipo jurídica ya sea contractual o con consecuencias penales, es que tales hechos o ideas que alcanzan valor probatorio consten en un soporte

---

[7] VILLALOBOS, Edgardo. Op Cit p 11

magnético, el cual es un objeto material, mismo que de alguna manera pueda reflejarse en un documento.

Si bien es cierto, que hay casos en que una transmisión del pensamiento, que tiene efectos jurídicos-penales, pueda verse sólo fugazmente a través de una pantalla o monitor de una computadora, o de un equipo de transmisión de datos, la realidad es que todas estas unidades poseen una unidad central de proceso, constituida por una unidad de memoria principal o de extensión, con un control y un reloj de tiempo real, el cual permitiría que la información que pudo aparecer sólo unos minutos en una pantalla y que luego se desvanezca, permita ser recapturada y retransmitida en los medios normales de almacenamiento de datos, que son entes materiales y físicos.

En un análisis pormenorizado de los bienes informáticos en los cuales puede transmitirse un documento, tenemos: " formas contínuas de papel, formas especiales de papel para impresión de rayos láser, impresión sin papel carbón, formas no contínuas de papel y formas especiales para uso manual o para uso mecanizado, suministro de papel perforado, suministros magnéticos de cintas magnéticas de cassette, discos magnéticos, cintas magnéticas para tarjetas u otros artículos,

micropelículas, microfichas y microformas, cintas de control de avance de papel, cinta entintada de impresión, cinta para impresoras de inyección, cinta para marcas magnéticas.."[8]

El documento electrónico es, pues, un elemento material, que puede en algún momento ser intangible, sin embargo, todo documento electrónico supone que puede ser leído, accesado y/o copiado por un instrumento especializado de carácter electrónico, que permite al ser humano disponer de él y leerlo u oírlo, conforme la idea de pensamiento que transmita. En otras palabras, el objeto material cuya corporeidad puede ser alterada o imitada.

2. No posee caracteres de grafía personal directa: Esta característica del documento electrónico, se debe esencialmente a que el pensamiento, idea, gráfico o sonido que contiene un instrumento electrónico sólo es generado a través de una máquina o un instrumento electrónico que lo crea.

Existe la posibilidad que un documento electrónico se genere en un documento simple de papel, que implique la firma o suscripción manual de los involucrados en lo redactado en el documento electrónico, pero la realidad es que si existe una alteración, pérdida o modificación de dicho

[8] HELLEZ VALDES, Julio Op Cit p 12

documento privado, una de las maneras más auténticas que se contaría para constatar la veracidad del documento lo sería a través del instrumento electrónico que lo contiene.

Las nuevas tecnologías contemplan la suscripción de **firmas electrónicas** a través de medios electrónicos de comunicación, que la Ley 43 de 31 de julio de 2001, define en su artículo 2 de la siguiente manera:

> *ARTICULO 2. Definiciones. Para los efectos de la presente Ley, los siguientes términos se definen así:*
> *1..*
> *2..*
> *3*
> *4...*
> *5. Firma electrónica. Todo sonido, símbolo o proceso electrónico vinculado a o lógicamente asociado con un mensaje, y otorgado o adoptado por una persona con la intención de firmar el mensaje que permite al receptor identificar a su autor.*
> *6..*
> *7..*
> *8..*
> *9..*
> *10*
> *11*
> *12*
> *13 . "*

Esta definición de la ley, coincide en las características del documento electrónico, en que la grafía de una persona en forma directa no forma parte integral de documento electrónico, sino que llegaría a ser una forma de suscripción, o autenticidad, que permitiría considerarla como prueba; sin embargo, en sus características primarias, la firma de puño y letra no forma parte del documento informático.

El desarrollo del comercio electrónico ha incorporado la firma electrónica, conocida también como firma digital, para permitir la validez y eficacia de la información emitida por los medios electrónicos, las cuales se han hecho cada vez más populares, especialmente con las licencias corporativas, seguros informáticos y contratos de banca electrónica.

La firma digital o electrónica está definida como "un sello integrado en datos digitales, creado con una clave privada, que permite, identificar al propietario de la firma y comprobar que los datos no han sido falsificados"[9]

[9] **RIBAS, Xavier** LA FIRMA DIGITAL Revista informática enero Madrid 1997 p 12

La existencia de esta firma es realmente una forma para establecer la validez y eficacia de las comunicaciones y documentos que se emiten, y que son una certificación de las transacciones.

Es importante señalar esta característica, para que no se confunda también con el hecho que en algunos medios electrónicos como las computadoras personales, se prevé la posibilidad que todo documento que se emita por e-mail, o correo electrónico a través del internet; por fax o telex, contenga la suscripción de una firma, sin que ello necesariamente quiera decir que el documento fue realmente emitido por quien firma, sino que la programación de los correos electrónicos que se hagan por esa computadora o de la máquina de telex o fax van a tener en la parte superior o inferior del documento que se emita la transcripción de una firma sin mayores seguridades.

3. Tiene finalidad representativa. El documento electrónico que debe entrar en el tráfico jurídico, y en especial, del derecho penal, debe necesariamente generar una idea, un pensamiento, una representación, que pueda ser captada por nuestros sentidos, con la intención de representar algo.

El documento electrónico debe generar una forma de mensaje de datos, que pueda representarse en el mismo soporte electrónico que lo reproduce o en un soporte de papel; ya sea con caracteres alfabético-algebraico, o en lenguaje de computadora, pero que coherentemente refleja la representación de un concepto, pensamiento, sonido o idea.

La doctrina en materia de documentos, señala que no es necesario que el documento –en este caso electrónico- posea un texto, tenor, o declaración; es suficiente que contenga una imagen, o una indicación numérica para que indique una representación del pensamiento humano.[10]

El artículo 5 de la Ley 43, señala que:

> *ARTICULO 5: Reconocimiento jurídico de los mensajes de datos. Se reconocen efectos jurídicos, validez y fuerza obligatoria a todo tipo de información, que esté en forma de mensaje de datos o que figure simplemente en el mensaje de datos en forma de remisión".*

Esta norma prevé un reconocimiento jurídico de todo tipo de información que sea generada por un instrumento electrónico, por supuesto con el cumplimiento de las normas adjetivas relacionadas a la

---

[10] Vease **CASAS BARQUERO, Enrique** EL DELITO DE FALSEDAD EN DOCUMENTO PRIVADO Bosch casa editorial Barcelona 1984 p 255 - 258

autenticación de documentos en general; por lo que se acepta en principio que todo documento electrónico debe tener una finalidad representativa.

4. Está contenido en un soporte magnético o electrónico: El documento electrónico, para que se diferencie de un documento normal, debe ser generado y contenido en un soporte magnético.

Cuando mencionamos las diferentes formas en que se puede generar un documento electrónico, en el punto 1. es cierto que pueda coincidir uno de los soportes de la información, como lo es una hoja simple de papel de 8 ½ X 11, con la de un documento normal; sin embargo, la realidad es que hoy, para simplificar, economizar y agilizar las formas de producción del comercio electrónico, de manera que todos puedan accesar a estos medios, en un momento dado puede coincidir una forma de soporte electrónico con la de un documento normal, sin por ello desvirtuar su original naturaleza electrónica.

c.- Clasificación de los documentos electrónicos

Conforme a lo señalado en este capítulo sobre los documentos electrónicos, los mismos pueden derivarse en documentos públicos o privados, dependiendo principalmente de la entidad o persona que los genere.

Sin embargo, es posible que el autor del documento electrónico sea un particular y posteriormente se considere el documento como público, por incorporación o accesión, como es el caso de un documento electrónico privado, que se incorpora a un protocolo, expediente o proceso público.

Lo relevante desde la óptica penal en los documentos electrónicos es que si bien los mismos son generalmente documentos privados, que carecen de eficacia probatoria mientras no sean reconocidos o llenen las formalidades legales para que se incorporen en un proceso, la doctrina y las últimas regulaciones en la materia, consideran a los documentos electrónicos como documentos mercantiles, que deben ser regulados en forma autónoma, representados en "...una figura intermedia entre la falsedad de documento privado y la falsedad de documento público".[11]

El artículo 5 de la Ley 43 es claro cuando le reconoce eficacia jurídica a todos los mensajes o informaciones que se emitan en forma electrónica, lo cual permite prever una forma especial de tratamiento, en

[11] **CASAS BARQUERO, Enrique.** Op Cit pp 242

relación con los demás documentos, para que tengan eficacia dentro del tráfico legal.

La especial función económico-jurídica de la mayoría de los documentos electrónicos, es de una naturaleza e importancia distinta a las del documento privado en general, que implica una consideración especial al momento de regularse, independientemente de las consideraciones jurídico-penales, que reconocen que la fe del público en general sobre estos documentos es sumamente especial, y que su ilegalidad, ineficacia o invalidez, causaría un caos socio-económico de magnitudes impredecibles.

Así vemos que la simple generación de un recibo de un servicio público, como lo son los que se expiden por los servicios del uso de agua, luz o teléfono, puede hoy ser inmediatamente pagado a través de un servicio electrónico en línea, de una computadora personal que accesa a los fondos de un banco privado, modificando así con esta modalidad todo un sistema económico en un país.

La emisión de correos electrónicos que inicialmente se pueden identificar como documentos privados, no comerciales, realmente son generados por un sistema de redes llamado internet; soporte de carácter

comercial que inmediatamente permite aplicar la especialidad que es un documento económico.

En la opinión del economista argentino JORGE CASTRO "Las ganancias que los recursos tradicionales (trabajo, tierra y capital) producen son cada vez menores y en contraposición, los principales productores de riqueza son el conocimiento y la información",[12] que se da a través de los documentos electrónicos.

Sobre las ventajas y aportes de la firma digital, coincidimos plenamente con lo afirmado por JOVANE cuando señala que el sistema informático, a través de la firma digital "hace posible implementar trámites administrativos, control de mercancía, acceso a información confidencial, o simplemente procesos de facturación de un modo mucho más rápido, eficaz menos costoso...."[13]

Como una excepción en el campo jurídico de aceptación de toda idea, concepto o pensamiento a través de un documento electrónico o un

---

[12] **CASTRO, Jorge** LA SOCIEDAD DEL CONOCIMIENTO INTERNET Y EDUCACION Revista Derecho y Economía Digital 2000 Buenos Aires 2000 p 17

[13] **JOVANE, Lissy** PROBLEMAS JURIDICOS DEL COMERCIO ELECTRONICO En Revista Lex Colegio Nacional de Abogados Editorial Mizrachi & Pujol S A Marzo 2001 p 63

mensaje de datos, tenemos lo que señala el artículo 6 de la Ley 43, que a la letra establece:

> ***ARTICULO 6.*** *"Cuando la ley requiera que la información conste por escrito, los actos y contratos otorgados o celebrados por medio de documento electrónico, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito en soporte de papel.....*
> *Lo dispuesto en el presente artículo no será aplicable a:*
> *a.) Los actos para los cuales la ley exige una solemnidad que no sea verificable mediante documento electrónico,*
> *b.) Los actos jurídicos para los que la ley requiera la concurrencia personal de alguna de las partes*
> *c.) Los actos jurídicos relativos al Derecho de Familia.*

Las consideraciones establecidas por la Ley 43 nos parecen importantes en lo relacionado a los documentos que tienen injerencia en el tráfico jurídico, de manera que existe mayor seguridad para las partes relacionadas.

Sin hacer distinciones con respecto a los aspectos procesales de los documentos electrónicos, la regla general es que si un documento informático o electrónico no es emitido por una entidad notarial o registral reconocida por el Estado, o por un funcionario público, se le

considera como un documento privado, no obstante, dadas las tendencias actuales del derecho y el comercio, han revestido de especiales cualidades, características y formalidades, a los documentos, dependiendo del tipo de soporte electrónico que contenga al documento informático y del pensamiento o idea que emita el mismo, de manera que se le tutela en forma especial.

II.- DISPOSITIVOS ELECTRONICOS E INFORMATICOS

En la elaboración, generación, emisión o copia de los documentos electrónicos, están involucrados una extensa gama de dispositivos electrónicos e informáticos, que son los que permiten la accesibilidad de dichos documentos al sujeto común, y por ende, a realizar transacciones comerciales y/o sociales que cambian el entorno de todos.

Los documentos electrónicos pueden ser generados por una máquina denominada computadora, que puede aceptar, procesar y proporcionar datos en un formato específico como es en lenguaje de computadoras, lenguaje común (no importa el idioma), imágenes o sonidos

Estas computadoras están formadas por componentes físicos, que se denominan *hardware*, y por un soporte lógico, denominado *software*, que en algunos casos llegan a confundirse con los documentos electrónicos, debido a que su protección está íntimamente ligada con el derecho de autor y de propiedad intelectual que se regula en distintos países.

a.- Componentes físicos o *hardware*

Los componentes físicos de una computadora, que facilitan la generación de los documentos electrónicos, son los "dispositivos mecánicos, electromecánicos y electrónicos; éstos permiten efectuar **físicamente** los procesos de captación de información, operaciones aritméticas y lógicas, almacenamiento de información, así como la obtención de resultados". [14]

Básicamente todos los componentes físicos contendrán una serie de circuitos, dispositivos de almacenamiento magnético, unidades

[11] TELLEZ VALDES, Julio Op Cit p 9

periféricas, terminales portátiles de video, impresión o sonido, dependiendo de lo que se requiera o se pueda construir.

b.- Soporte lógico o *software*

Es lo que constituye el soporte lógico de las computadoras, que forma parte integral de los bienes y servicios informáticos, y que lo constituyen todos los programas que se pueden utilizar en un sistema computarizado, y que gozan de la protección de "derecho de autor" en la mayoría de nuestros países.

Normalmente el soporte lógico lo constituye el conjunto de programas que produce el fabricante de la computadora y es un factor sumamente importante en el desarrollo y comercialización de las computadoras.

Gracias a la existencia del soporte lógico, el usuario puede reducir considerablemente el esfuerzo requerido para diseñar un sistema y escribir los programas necesarios para el adecuado funcionamiento de las computadoras.

El soporte lógico no debe ser confundido con los programas específicos que se escriben para resolver los problemas de un usuario en particular, así por ejemplo, un programa. que se vende con sus licencias

en el comercio local para lograr varias actividades relacionadas con el microempresario, no es propiamente el soporte lógico de una computadora. Un tipo de soporte lógico de una computadora es el programa de Microsoft-Windows, o el de las computadoras Apple que se vende con la computadora y que permite la accesibilidad de otros programas, según su capacidad.

c.- Telemática

La asociación cada vez más estrecha entre las tecnologías de la informática y de las telecomunicaciones ha creado aspectos de interés en el análisis de la producción de documentos electrónicos que están transformando de forma innegable las formas de comunicación y comercio del mundo.

Las telecomunicaciones relacionadas con la informática, han creado verdaderas "autopistas de la información" que surcan el planeta por una verdadera red de redes de la televisión, la telefonía y las computadoras, a través de líneas telefónicas, fibras ópticas, cables submarinos y enlaces satelitales.

Las connotaciones políticas, económicas, sociales y culturales de la telemática, están permitiendo que se llegue a hablar de un Derecho

Telemático en vez del Derecho Informático que conocemos hasta ahora, que involucre las formas de información que debe regular el Derecho y que en el aspecto particular del Derecho Penal, se logre cubrir la brecha existente entre la realidad y las posibilidades de violaciones a la intimidad, derecho de autor, simulación, falsificación, etc., relacionadas con conductas antisociales.[15]

En la estructura de los sistemas de redes de teleinformática, encontramos como componentes directamente vinculados con los servicios informáticos los siguientes: terminales, concentradores o dispositivos intermedios, transmisión de datos, dispositivos de la red de telecomunicaciones, acopladores o adaptadores de transmisión, los cuales en un momento dado permiten recoger una información y transmitirla en forma adecuada a los sentidos, como lo es un documento electrónico y que es sujeto de estudio en este trabajo.

III.- COMERCIO ELECTRONICO

Debido a la gran proliferación de documentos electrónicos que se generan por los cambios tecnológicos y la revolución comercial y

[15] Palabras de Bienvenida al VIII Congreso Iberoamericano de Derecho e Informática realizado en Lima Perú en marzo de 2001

económica que han causado en el medio se habla de comercio electrónico, el cual se define como "cualquier forma de transacción o intercambio de información basada en la transmisión de datos sobre redes de comunicación como Internet".[16]

El auge de la evolución de este comercio se debe a que gracias a este comercio se reducen las barreras de acceso a los mercados actuales, en especial para las pequeñas empresas y al usuario común, el consumidor puede accesar a cualquier producto a nivel mundial, la reducción o eliminación por completo de los intermediarios en la venta de productos en soporte electrónico, los cuales se pueden pagar y entregar directamente a través de la red.

Se ha calculado que desde 1994 a la fecha la economía cibernética ha crecido en una media de 174% cada año y aunque el desarrollo no es igual en todos los países. A pesar de los últimos acontecimientos políticos y económicos ocurridos en septiembre de 2001 en Nueva York por la destrucción de las Torres Gemelas y el Wall Street, sumadas a las grandes recesiones económicas en la mayoría de los países

---

[16] **JUEZ MARTEL, Pedro.** EL COMERCIO ELECTRONICO ¿HACIA UNA NUEVA REVOLUCION ECONOMICA Y JURIDICA? Ponencia en el VIII Congreso Iberoamericano de Derecho e Informatica realizado en Lima Peru. Marzo 2001 p. 1

Latinoamericanos; sólo en Estados Unidos, el comercio electrónico ha superado los 100 millones de personas. [17]

En este comercio electrónico participan los consumidores o usuarios, quienes adquieren servicios y productos a través del sistema; las empresas, que son las que ofrecen esos servicios y productos y la administración, que regula, fomenta y promueve la actividad comercial a través del internet; distinguiéndose de esta manera tres tipos básicos de comercio electrónico:

- Entre empresas, también conocido por sus siglas como B2B, que significa ***business to business.***.
- Entre empresas y consumidor o B2C que significa ***business to consumers***, y
- Entre empresas y administración, denominado por sus siglas B2A, y que representa lo denominado en el idioma inglés como ***business to administrations***. [18]

Los aspectos legales que se traducen con la proliferación de este comercio, es que se da una gran producción de contratos y transacciones legales "sin papel", que pueden derivar en inseguridades jurídicas; la

---

[17] Vease **JUEZ MARTEL, Pèdro.** Op Cit pp 4 y 5

[18] Vease lo comentado por Tissy Jovane sobre comercio electronico Op Cit p 64

generación de fraudes fiscales, quebrantamientos de la protección de los derechos de propiedad intelectual, indefensión de los consumidores o usuarios particulares.

La solución jurídica que se ha planteado para que el comercio electrónico funcione adecuadamente, y se resuelvan los aspectos de seguridad, privacidad y validez legal de los documentos comerciales en formato electrónico se ha logrado a través de mecanismos sofisticados, como son las técnicas criptográficas y la firma electrónica o digital.

a.- Técnicas criptográficas

El sistema bancario que utiliza uno de los documentos electrónicos más conocidos en el ámbito de las transacciones comerciales, como lo es la tarjeta de crédito, o tarjeta inteligente, basa su manejo electrónico con técnicas criptográficas; mismas que se caracterizan por la utilización de una clave secreta para cifrar y descifrar depósitos bancarios y accesarlos para disponer de los mismos, según corresponda.

El sistema más utilizado consiste en una pareja de claves, una pública y otra privada, en la cual la clave pública, generalmente se encuentra inscrita en la tarjeta inteligente y se mantiene en secreto la

clave privada, la cual puede guardarse en un ordenador o computadora o en la memoria del usuario.

Las claves pueden consistir en letras, signos o números, las cuales deben ser manejadas con sumo cuidado por el usuario, ya que permiten la confidencialidad de la transacción.

b.- Firma electrónica o digital

El uso contínuo de las técnicas criptográficas han desarrollado lo que se denomina firma digital o electrónica, y que ha sido definida mediante la Ley 43 de 31 de julio de 2001 en Panamá, que señala:

> ***ARTICULO 2.*** *Definiciones . . .*
> *1...*
> *2...*
> *3...*
> *4...*
> *5. Firma electrónica. Todo sonido, símbolo o proceso electrónico vinculado a o lógicamente asociado con un mensaje, y otorgado o adoptado por una persona con la intención de firmar el mensaje que permite al receptor identificar a su autor.*
> *6...*
> *7...*
> *8. .*
> *9...*
> *10. .*
> *11..*
> *12 .*
> *13 ..*

Este procedimiento de firma digital o firma electrónica , consiste en colocar la firma en un resumen, conocido como *hash* en inglés, cifrándola con la clave privada del remitente. La firma digital o electrónica de un usuario no sería siempre la misma secuencia de bits, sino que depende del mensaje firmado.

Si por alguna razón se llegara a modificar el mensaje original, por pequeña que sea la modificación, dará lugar a un resumen cifrado diferente.[19]

Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma electrónica; si el mensaje hubiera sido alterado a su paso por la red, el resumen calculado por el destinatario no coincidiría con el original calculado por el remitente.

Los inconvenientes de las firmas digitales son la lentitud de los algoritmos y las claves establecidas, por lo cual se han creado autoridades de certificación oficial, que desde 1997 han creado un marco común para firma electrónica.

Panamá ha empezado a regular las entidades de certificación de comercio electrónico, y por ende, de documentos electrónicos, a través de la ley 43, la cual dispone en el artículo 2, numeral 4, lo siguiente:

> ***ARTICULO 2.***
> *1*
> *2...*
> *3...*
> *4 Entidad de certificación. Persona que emite certificados electrónicos en relación con las firmas electrónicas de las personas, ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos y realiza otras funciones relativas a las firmas electrónicas.*
> *5...*
> *6...*
> *7...*
> *8...*
> *9...*
> *10...*
> *11...*
> *12...*
> *13...*

Con respecto a la validez de las firmas electrónicas en los documentos electrónicos o mensajes de datos, el artículo 25 de la ley señala que:

> ***ARTICULO 25:*** *Atributos de la firma electrónica. El uso de una firma electrónica tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella 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 electrónica es inválida*

[19] **JUEZ MARTEL, Pedro.** Op Cit p 8

El texto de dicha norma hace referencia a las firmas electrónicas seguras, es decir, firmas electrónicas que son certificadas por una entidad reconocida por el Estado, pero que tienen como excepción los documentos a que hace referencia el artículo 7 de la Ley 43, el cual dispone que no se entenderá satisfecho este reconocimiento en los casos de:

1.- Contratos sobre bienes inmuebles y demás actos susceptibles de registro ubicados en Panamá.

2.- Los actos en materia de sucesiones que se otorguen bajo ley panameña o que sufran sus efectos en Panamá, y

3.- Los avisos y documentos dirigidos o emitidos por autoridades de Panamá, que no hayan sido autorizados por la entidad respectiva.

En este sentido, la ley panameña trata que el comercio electrónico a través de datos y documentos electrónicos, sea seguro para usar el sistema, y mantiene algunos temas de difícil regulación civil, comercial o procesal, conforme las técnicas normales de soporte de papel regular, para verificar su autenticidad, que es uno de las preocupaciones principales del Derecho Penal

CAPITULO SEGUNDO

MODALIDADES TIPICAS DE LA CONDUCTA DE FALSIFICACION EN DOCUMENTOS ELECTRONICOS

I.- TRASCENDENCIA DEL BIEN JURIDICO PROTEGIDO

Para analizar las diferentes modalidades de falsificación de documentos electrónicos, es necesario aclarar cual es el bien jurídico protegido en las conductas que consideramos ilícitas y que menoscaban la seguridad que tiene la sociedad en los documentos electrónicos.

La desmaterialización y falta de suscripción o constancia de autenticidad de los documentos electrónicos, provoca que la mayoría de los autores desconozcan que el bien jurídico protegido pueda ser la fe pública, como lo es en los documentos en general.[20]

Sin embargo, si vemos cuál es la finalidad de un documento, tenemos que estar claros que sea electrónico o no, el documento tiene como misión representar, evocar algo. En ese sentido SANCHIZ CRESPO nos declara que el documento es esencialmente representativo el mismo supera los obstáculos de espacio y tiempo, y por tanto debe

---

[20] Cfr. RIOL RIO, Juan Carlos. La prueba electrónica. Edit. Temis. Colombia. 2004. pp.

entenderse que los documentos electrónicos se deben considerar documentos en general.[21]

Jurídicamente, el documento electrónico tiene las mismas funciones que un documento público o privado en general, y en nuestro concepto, debe considerarse a la fe pública como el bien jurídico protegido, en la comisión de delitos de falsedad de documentos electrónicos, puesto que cualquier acción que permita cambiar o falsificar el documento informático, lo que viola es la fe que tenemos todos los asociados en los documentos que se generan, aunque sea por medios especializados.

I1.- ACCIONES TIPICAS DEL DELITO DE FALSEDAD

Uno de los análisis más importantes en el examen de los delitos de falsedad documental, es la determinación concreta de las diferentes manifestaciones de la conducta o actuar del sujeto activo, que permitan la configuración legal del tipo penal.

En la falsificación de documentos electrónicos, existe un gran debate entre destacados autores penales nacionales e internacionales, sobre si se debe considerar la creación de nuevas disposiciones penales

---

[21] Vease **SANCHIZ CRESPO, Carolina** La prueba por soportes informaticos Tirant Lo Blanc Valencia 1999 p 48 y 49

para calificar aquellas conductas lesivas a través de los medios informáticos, o si se pueden enmarcar entre los tipos penales existentes. Esta polémica surge a raíz del razonamiento que en la mayoría de los delitos informáticos no hay corporeidad o materialización del acto ilícito, sino resultados; lo que podría causar un problema jurídico al momento de analizar la acción en el tipo y por ende, la configuración de un tipo legal existente como es la falsificación, la estafa o la simulación, o por el contrario, se debe crear un tipo especial para los comisión de los delitos electrónicos o cibernéticos. [22]

Es evidente que uno de los aportes del siglo XX y su continuidad en el presente es la aparición de la llamada "revolución digital", donde el complejo sistema de cables, satélites, redes, computadoras, televisoras, y sistemas producidos pos impulsos eléctricos, constituyen la infraestructura del "ciberespacio", revolución, que encuentra su máxima expresión (hasta ahora) en el internet; gracias al fenómeno de convergencia del uso combinado de las computadoras y las redes de comunicación.

---

[22] Vease **ZARATE, Abdiel** "Delitos Informaticos" En La Prensa 22 de octubre de 2001 Seccion Revista Pag 1b

Los efectos de semejante transformación se hacen sentir en la economía, la política, la educación y el entretenimiento, con prácticas inimaginables como las compras ***on-line***, ***chats***, ***e-mail***, educación a distancia, foros de discusión, etc.

Esta revolución, ha dado un salto gigantesco en las instituciones, costumbres, y formas de relacionarse, lo que está impulsando a varios autores penales a recomendar la revisión y actualización de las conductas desvaloradas que se ejecutan con la destrucción de bases de datos personales, el hurto o el fraude informático, y que por la imposibilidad de hacer analogías en la aplicación del derecho penal, se permite la impunidad de tales actos.

Nuestra opinión es que los cambios se están registrando paulatinamente, - desafortunadamente no con la celeridad que se requiere- dándose calificaciones determinadas en el momento en que se puede conocer el fenómeno electrónico e informático; pero específicamente en el caso de falsificación de documentos electrónicos, existe la posibilidad de enmarcarlos en los tipos penales existentes en el Código Penal panameño, tomando en cuenta las diversas formas de

ejecución en que se puede cometer un delito contra la fe pública, especialmente en cuanto a la falsedad documental en general.

Existen diversas formas de conducta destinadas a lograr que un documento en general y un documento electrónico en especial, sean alterados o falsificados. Por ello, analizaremos las diferentes modalidades de conducta que pueden realizarse para materializar acciones de falsificación de documentos electrónicos.

a.- Formar o hacer un documento electrónico falso

En el ámbito propio de los delitos de falsedad de documento electrónico, es necesario poner de relieve las formas fundamentales de falsedad, como es la alteración o falsificación de un documento originariamente verdadero, a través de mecanismos materiales de alteración, llamada falsedad material, o por la alteración de fondo, a través de una falsa aseveración o narración, como es la falsedad ideológica o intelectual.

Según Casas Barquero, la forma de hacer una falsificación material de los documentos se puede dar por imitación o alteración de un documento, que implica la existencia de un documento previo que se

imita o se toma como modelo; o por la formación, creación, fabricación o construcción de un documento falso sin la existencia de un documento original que se pueda imitar o comparar.[23]

En la falsificación material de documentos electrónicos, las modalidades son variadas, a saber:

1.- Datos Engañosos: Es conocido en el idioma inglés como ***data didling***, y es uno de los sistemas más simples y comunes utilizados por las personas que se encargan de la entrada de datos en las cuentas o informaciones computarizadas, manipulándose datos que permite llevar a cabo transacciones falsas para la emisión de cheques o informes fraudulentos.

Este tipo de falsificación de documentos electrónicos implica no sólo la alteración o modificación parcial de los elementos genuinos de una cuenta existente, mediante añadiduras o eliminaciones en su forma o en su contenido, sino también de la generación de documentos falsos, inexistentes, como sería en ese caso un cheque o una tarjeta de crédito fraudulenta.

2.- Técnica Salami: Consiste en el redondeo de cuentas que pueden ser céntimos de cuentas corrientes, saldos de proveedores y

[23] Vease **CASAS BARQUERO** Op Cit Pag 168 - 178

talonarios de cheques, conocido como ***salami techniques*** y que permite a través de los medios electrónicos transferirse a otra cuenta con nombre ficticio, la sustracción de pequeñas cantidades de activos de diversas procedencias.

La técnica utilizada implica la falsificación de los datos reales de las cuentas corrientes o activos de las víctimas, que se mueven constantemente a través de los medios electrónicos por la emisión de cheques, la utilización de tarjetas electrónicas u otros medios que permitan del movimiento de capital en forma rápida, y la creación de documentos electrónicos falsos que impliquen la formación de una cuenta ficticia.

3.- ***Superzapping***: Es una forma de alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en una computadora o en los soportes magnéticos de un ordenador. El nombre proviene de una utilidad existente en las computadoras denominada ***superzap***, que permite acceder a cualquier parte de la computadora y modificarlo, su equivalente en una computadora personal sería lo denominado como ***Pctools*** o el ***Norton Disk Editor.***

4.- **Recogida de Residuos o Basura**: Esta terminología se utiliza en el sistema informático para determinar la forma de obtención de información residual impresa en papel o documentos magnéticos en memoria, después de la ejecución de un trabajo.

Se conoce en el idioma inglés como ***scavenging***, y puede ser utilizada ilícitamente, aprovechando información abandonada sin ninguna protección, debido al descuido de los usuarios y técnicos, de manera que se pueda tener acceso a computadoras u ordenadores, transformando un documento original, con adiciones o cambios, de manera que se manipula la verdad.

Además de los métodos fraudulentos de transformar, agregar, cancelar o cambiar un documento electrónico genuino, existe la posibilidad de hacer un documento falso si se señalan declaraciones falsas en un documento que se emitió por la persona o personas idóneas para hacerlo, pero contiene declaraciones falsas.

La falsedad ideológica sólo puede cometerse en el momento de la formación del documento electrónico y sólo se puede dar en los documentos narrativos y no en los dispositivos.[24]

---

[24] **RANIERI, Silvio.** Manual de Derecho Penal. De los delitos en particular. Parte Especial. Tomo IV. Edit. Temis. Bogotá. 1975. p. 460

En ese sentido, un documento electrónico afectado por una falsedad ideológica puede ser aquel en que se registran las declaraciones de un proceso legal, como son las cintas magnetofónicas, video, transcripciones a través de computadora en el disco duro, discos compactos o diskettes, adoptando así las modalidades propias de la falsedad documental histórica o ideológica, donde el contenido total o parcial es el que resulta falseado.

b.- Suprimir, ocultar o destruir

La conducta a la que ahora nos referimos se concreta con actos materiales con los cuales se destruye, suprime u oculta en todo o en parte un documento electrónico.

Se debe tratar de actos que privan la disponibilidad del documento electrónico, que hacen salir de la esfera jurídica del sujeto dicho documento.

La doctrina ha establecido este tipo de conducta como una forma de alterar la verdad, cuando vemos por ejemplo, la sustracción de documentos electrónicos referidos al registro público, status civil o nacionalidad de las personas, siendo estos dos últimos derechos

inalienables de todo ser humano según la Constitución Nacional, lo que puede dar lugar a un concurso ideal en la práctica.

El elemento material del delito en la sustracción, ocultación o destrucción de un documento electrónico es la eliminación de la función probatoria del documento, alterando sustancialmente la verdad de los hechos y dando lugar a que se dicten sentencias o resoluciones injustas que causan perjuicio a personas inocentes.

Si bien es cierto que las conductas descritas podrían dar lugar a otras figuras delictivas como las de daño o hurto, es importante prever que lo que se pretende es hacer aparecer lo falso en lugar de lo verdadero y lesionar los derechos de otra persona, afectando así el bien jurídico de la fe pública.

Las conductas específicas con que se puede configurar la acción descrita, puede ser no sólo por el hurto, destrucción o supresión de un documento electrónico tangible, como lo es un disco compacto, una cinta que contenga sonidos, imágenes o signos comprensibles, una tarjeta electrónica, o cualquier otro documento generado por sistemas electrónicos, sino también en todas las formas que se describen en los medios informáticos, a saber

1.- Puertas falsas o puertas con trampas: Definidas en el idioma inglés como ***trap doors***, es una práctica acostumbrada por los programadores de computadoras y de sistemas en el desarrollo de aplicaciones complejas, que introduce interrupciones en la lógica de los programas, para poder verificar si los resultados intermedios son correctos.

El sistema de puertas falsas puede ser utilizado con fines ilícitos por personas que desean eliminar en todo o en parte una información, ya que se puede accesar a través de estos sistemas a los programas, y con ello eliminar o destruir una información importante en las relaciones jurídicas de los interesados.

2.- Bombas lógicas: Conocidas como ***logic bombs***, es el procedimiento de sabotaje más comúnmente utilizado por los empleados descontentos de una empresa, quienes destruyen información conocida de manera definitiva.

Por este medio se logra destruir y suprimir información en documentos electrónicos, cuando se introduce un programa o rutina con una fecha determinada para destruir información

Todo lo anterior nos indica que en materia de documentos electrónicos, el Derecho Informático ha tenido que prever toda una variedad de modalidades de conductas deshonestas que, según su gravedad e incidencia en el ámbito penal puede ser objeto de tipificación en calidad de hechos punibles.

III.- FORMAS ACTIVA Y OMISIVA DE LA ACCION

La referencia y análisis de los hechos delictivos relacionados con la informática, todavía son hoy en día un concepto ambiguo, que no corresponde en sentido estricto a ninguna categoría jurídico-penal, al menos que las conductas se subsuman en los hechos punibles tipificados en el Código Penal.

En reuniones de expertos en la materia, se han utilizado expresiones o conceptos como: manipulación de datos, espionaje, destrucción o inutilización de datos o sistemas; términos que no han sido reconocidos legislativamente, pero que analizadas con otra óptica, se pueden concretar en modalidades delictivas ya existentes. como ocurre en la doctrina alemana donde se llega a definir que la informática y todo lo

relacionado con el procesamiento automatizado de datos es el instrumento o el objeto de la comisión de estos ilícitos. [25]

Los señalamientos previos hacen pertinente el análisis de las formas de comisión del tipo de falsificación de documentos en general, y de la falsificación de documentos electrónicos en particular, de manera que se pueda establecer si el tipo es susceptible tanto de comisión activa como de omisión o la llamada comisión por omisión, cuando se ejecutan diversas conductas desvaloradas en la manipulación y creación de documentos electrónicos, teniendo el agente la obligación jurídica de evitar el resultado.

a.- Comisión

Es evidente que los delitos de falsificación de documentos electrónicos pueden cometerse por comisión, es decir, donde se da la realización de un comportamiento, con la producción de una modificación del mundo exterior, es decir, un resultado material, como lo es la **alteración, formación, creación** o **fabricación** de un documento electrónico falso.

---

[25] Vease **MATA Y MARTIN, Ricardo M** Algunas consideraciones sobre Informatica y Derecho Penal El caso de la estafa informatica En Documentos Penales y Criminologicos Vol I Año 2001 Nicaragua 2001 pags 97-103

La denominada falsedad material tiene un resultado típico material, en cuanto la conducta actúa sobre un objeto corpóreo del mundo exterior, es decir, en este caso el documento electrónico, es que se manifiesta a través de un resultado materialmente tangible y apreciable por los sentidos.

La modalidad de falsedad material o falsificación por comisión, es aquella en la que se verifica el actuar ilícito en uno de los soportes magnéticos o electrónicos de información que agilizan el comercio electrónico, como lo es una cinta magnetofónica, discos magnéticos, cintas magnéticas para tarjetas, micropelículas, microfichas, micro formas, cintas para impresoras de inyección, cintas para marcas magnéticas, y formas que se asimilan a los documentos conocidos tales como: formas especiales de papel para impresión de rayos láser, impresión de papel sin papel carbón, formas no contínuas de papel y formas especiales para el uso manual o mecanizado de suministro de papel perforado. Toda acción por comisión, como es sabido, consiste en un hacer violatorio de una norma prohibitiva, es el ***facere quod non debere.***

Las acciones o conductas de comisión de falsificación de los documentos electrónicos son apreciables sensorialmente, de manera que se puede disponer o acceder al documento, leerlo u oírlo, conforme la idea de pensamiento que transmita, y percibir la ejecución por **comisión** del delito de falsificación de documento electrónico, porque se da un resultado. Este a su vez es la evidencia que demuestra la conducta o manipulación de voluntad positiva y el ente corpóreo sobre el que recayó la acción delictiva de falsificación.

b.- Omisión

Por otro lado, es posible además que la falsificación de documentos electrónicos se dé por la omisión de un dato en específico, que se equipara a la llamada falsificación ideológica, en donde si bien es cierto, existe una manifestación de voluntad de "faltar a la verdad"[26], no lleva a la producción causal de ningún cambio en el mundo externo perceptible a los sentidos.

---

[26] En este tema CASAS BARQUERO manifiesta haciendo un analisis de la jurisprudencia y el Código Penal Español que el criterio general no se muestra favorable en admitir la falsedad documental omisiva pero en Sentencias de junio de 1951 y 1952 se acepto la posibilidad de cometer una falsedad documental por omision debido a que cuando se realizo un acta de inspeccion no se recogio las regularidades registradas en el curso de dicha inspeccion y que eran objeto de la misma Op Cit Pags 196 y 197

La falsedad omisiva en documento electrónico se puede dar cuando no se hace lo que se debe hacer, esto es, no se anota una inscripción en donde esencialmente se debería anotar.

En un análisis más profundo de la forma omisiva para cometer el delito de falsificación de documento electrónico, valga el ejemplo del caso, cuando existe la obligación de expresar o consignar en un documento lo que en el documento falta o debía constar, es decir, se debe dar cuando hay un deber jurídico, un precepto imperativo de consignar una verdad en un documento electrónico, como lo es para un Notario, identificar a la persona que declara algo o quien debe transcribir una declaración, omite los puntos esenciales de la misma.

La omisión en los documentos en general, y en especial, en los documentos privados y electrónicos se da por la modalidad de **comisión por omisión**, que realmente es una forma especial de la omisión propia.

Las únicas formas en que se puede acreditar una falsedad documental por omisión, es en los casos en que existe un deber jurídico de hacer constar la verdad a través de un documento electrónico, de manera tal que su omisión produzca un efecto en el ámbito concreto del

delito de falsedad, y lo cual puede evidentemente recaer en otro tipo de conductas delictivas.

A pesar del análisis de las formas de conductas permitidas en el tipo, relacionadas con los documentos electrónicos, existe un vacío en lo relacionado con el aspecto "virtual" de algunas ideas que se emiten a través de las computadoras y que permiten recrear un hecho a través del monitor de una pantalla de computadora.

Las imágenes que se puedan emitir en un momento fugaz en un monitor y que permitan, por ejemplo, reconstruir la velocidad y ángulo en que se dio un accidente de tránsito, o cualquier hecho del que se quiera imaginar un resultado, tomando en cuenta los parámetros como peso, velocidad, altura, u otras características previsibles en un programa virtual, es todavía un área que no ha sido suficientemente estudiada en todo su contexto y que genera un sinnúmero de interrogantes, porque estas formas virtuales en un momento pueden servir de complementos probatorios y a su vez ser perfectamente manipuladas.

Ningún país, hasta el momento, ha podido señalar con propiedad los argumentos técnico-jurídicos que definen las formas o acciones para proteger los documentos electrónicos producidos por medios

informáticos, que manipulen la verdad y puedan causar un daño en algún bien jurídico existente, lo que impide la aplicación de la analogía para castigar comportamientos merecedores de pena con los medios del Derecho Penal tradicional.

Sin embargo, hay que mencionar que en la actualidad hay países como Estados Unidos de Norteamérica, donde se ha adoptado desde 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986 , y Francia, desde 1988, creó la Ley No. 88-19 sobre fraude informático, que señala en los artículos 462-5 y 462-6 la configuración de los delitos de falsificación de documentos informatizados y de uso de documentos informatizados falsos, a sabiendas de su falsedad.

IV.- CONCURSO DE DELITOS

Los delitos de falsedad documental, se encuentran tipificados en nuestro ordenamiento jurídico en el Título VIII del Libro Segundo del Código Penal, como protección al bien jurídico de la **fe pública**, que juristas como CASAS BARQUERO la describen como la confianza

colectiva o el sentimiento psicológico de una comunidad sobre ciertos instrumentos, objetos y actos que se dan en sociedad.[27]

Ese valor tan amplio que se le atribuye a los documentos en general –y a los documentos electrónicos en particular-, a través de tipos penales que permiten las transacciones económicas, sociales y jurídicas en sociedad; son considerados por los autores como tipos de naturaleza pluriofensiva [28], pues no sólo lesionan la fe pública, sino también el patrimonio, el honor, la libertad, etc.

En la práctica cabe anotar que a través de la comisión del delito de falsedad documental, se pretende cometer otras conductas que están tipificadas por el ordenamiento penal; como son la estafa, el delito de daños, delitos económicos, delitos contra el derecho de autor y otros.

Lo importante es determinar si la falsedad es un medio de ejecución o un delito instrumental o medio para lograr otros.

En nuestro ordenamiento no es posible hablar específicamente de "delitos informáticos", porque tal concepto ni siquiera ha sido delimitado en nuestro medio; sin embargo, países como Estados Unidos, Alemania,

---

[27] Cfr **CASAS BARQUERO.** Ob cit pp 61

[28] **RAFOLS LLACH, Juan** LALSEDAD DOCUMENTAL Y DEFRAUDACION FISCAL Cuadernos de Derecho Derecho Judicial La Nueva Delincuencia I Consejo General del Poder Judicial Mateu Cromo S A Madrid 1993 Pp 42-44

Suiza, España y Francia, ya cuentan con un ordenamiento relacionado con las conductas indeseables que se dan por el uso de computadoras y redes, donde se hace referencia a los delitos informáticos.[29]

El delito de falsedad documental en documento electrónico, es un "tipo" de delito informático, que se ejecuta con la finalidad de cometer otros ilícitos, por lo cual mencionaremos algunos de los delitos que se contemplan en la doctrina, el Derecho Comparado y la jurisprudencia.

a.- Estafa Informática

Una de las formas delictivas con que se puede causar un perjuicio patrimonial a las personas, es a través del engaño, que se ha tipificado como el delito de estafa.

El delito de estafa se caracteriza por contener los siguientes elementos: engaño, el error producido en el sujeto pasivo a causa de dicho engaño, la disposición patrimonial del sujeto pasivo fundado en el error, y el perjuicio producido por esta disposición patrimonial. [30]

---

[29] El termino de delitos informaticos es la traduccion de la terminologia anglosajona conocida como *computer crime* que es una forma simple y atractiva para hacer referencia a conductas y hechos que atacan bienes juridicos tradicionalmente protegidos por el Derecho Penal debido a los avances tecnicos y cientificos de la informatica o cualquier otro medio electronico o digital de transmision y comunicacion de datos sonidos o ideas Cfr **MATA Y MARTIN** Pp 21

[30] **GUERRA DE VILLALAZ, Aura** DERECHO PENAL PARTE ESPECIAL Editorial Mizrachi & Pujol S A Panama 2002 Pp 111-112

El delito de falsedad de documento electrónico se puede dar en concurso con la estafa, cuando se crea una falsa identidad a través de un documento electrónico (una cédula, un pasaporte) para poder cobrar por ejemplo una herencia.

Técnicamente hay un concurso de delitos, sin embargo, la práctica procesal es determinar que el delito de estafa absorbe al delito de falsedad documental, al considerar a este como el medio de ejecución de aquél.

b. El delito de daño

El caso de los delitos de daño informático es muy común, gracias a la gran cantidad de virus y bombas lógicas que existen en el medio y su concurso con el delito de falsedad en documento electrónico, se puede dar tal lesión patrimonial cuando se falsifica una orden que debe estar contenida en un medio electrónico, para que se ejecute y logre un daño en el software de un tercero.

A pesar que existe una gran cantidad de casos relacionados con el delito de daños en los soportes magnéticos de una computadora, los fallos de los tribunales no son consistentes en esta materia, tal como lo señala el

autor argentino PABLO PALAZZI, al analizar un fallo de la Sala VI de 30 de abril de 1993, de un Tribunal argentino, que se expresa así:

"... pues luego de reconocer que el programa de computación es una obra intelectual, años más tarde la Sala cambió de criterio y sostuvo en un caso posterior, confirmado por la Cámara de Casación que el *software* no se hallaba protegido por la ley 11.723".[31]

c. Delitos contra el derecho a la intimidad

En la emisión de documentos electrónicos falsos, existe la posibilidad que se traspasen los límites de información de una persona, y que además no sean fidedignos.

En un caso como este, a pesar de que existe la posibilidad de recurrir a la acción del *habeas data,* se da el delito de falsedad en documento electrónico, pues se emite o registra información o datos falsos de una persona, que además violan su derecho a la privacidad o la intimidad.

---

[31] PALAZZI, Pablo A. DELITOS INFORMATICOS Editora Ad-Hoc S.R.L. Argentina 2000 Pp 137

En este caso, se viola el bien jurídico protegido de la fe pública y el derecho fundamental de la libertad, los derechos de propiedad, identidad y privacidad.[32]

Este delito resulta con mayor viabilidad para las personas que por razón de su profesión, trabajo u oficio, tienen la custodia, registro o responsabilidad de manejar información confidencial y datos personalísimos de la exclusiva incumbencia de los interesados.

[32] Cfr **ARAUZ SANCHEZ, Heriberto.** LA ACCION DE HABLAS DATA Universal Books Panamá, 2002 Pp 29-31

CAPITULO TERCERO

ASPECTOS PROCESALES DEL DELITO DE FALSIFICACION DE DOCUMENTOS

I.- MEDIOS DE PRUEBA DEL DELITO DE FALSEDAD DE DOCUMENTO ELECTRONICO

Una de las mayores preocupaciones de los especialistas en materia procesal es la presentación, valoración y análisis de la prueba, como figura de tutela judicial en el debido proceso; que en el caso del delito de falsedad de documento electrónico, la eficacia del medio o la validez del documento, será el que permitirá esa tutela judicial.

A pesar que cada día los tribunales constitucionales de distintos países aceptan el ***numerus apertus*** sobre los medios de prueba, es evidente la necesidad de salvaguardar los derechos humanos consagrados por las Constituciones y los Convenios Internacionales, de manera que no se cause la indefensión del individuo cuando se acepta al documento electrónico como un medio de prueba.[33]

---

[33] Vease FABREGA, Jorge Op Cit pp 21 y 22

Esta anotación se hace necesaria, toda vez que los documentos electrónicos pueden ser usados en la transcripción de telecomunicaciones, que tienen especial protección constitucional.

La materialización de sonidos en forma de mensaje escrito, es una modalidad de ***chat*** o conversación a través del internet, que podría utilizarse en un proceso; pero si el acceso o interceptación de la comunicación es ilícito o ha sido aportado indebidamente a un proceso, no podrá utilizarse por el menoscabo que ello produce a principios fundamentales reconocidos por las legislaciones de los distintos países.[34]

Un ejemplo similar sobre la prohibición de utilización de documentos electrónicos en el proceso, se da en relación al correo electrónico y datos personales, cuando se viola el derecho a la intimidad.

Tomando en cuenta todas las protecciones legales, que impidan la utilización indebida de un documento electrónico en un proceso, se podrían aceptar los siguientes documentos:

---

[34] Cfr **MATA Y MARTIN.** Op Cit pp 130-132

a.- Copias de documentos electrónicos públicos y documentos electrónicos privados.

En lo que respecta a nuestro ordenamiento jurídico, la admisibilidad de los documentos electrónicos en la esfera procesal, como plena prueba o como indicio, se reconoce claramente en lo dispuesto por el artículo 832 del Código Judicial, y el artículo 11 de la Ley 43 de 2001, que a la letra dicen:

> **ARTICULO 832:** Son documentos los escritos, escrituras, certificaciones, copias, impresos, planos, dibujos, cintas, cuadros, fotografías, radiografías, discos, grabaciones magnetofónicas, boletos, contraseñas, cupones, etiquetas, sellos, telegramas, radiogramas y, en general, todo objeto mueble que tenga carácter representativo o declarativo y las inscripciones en lápidas, monumentos, edificios y similares.
>
> **ARTICULO 11:** Las solicitudes de que tratan los artículos anteriores se presentarán en papel simple o en formulario que proporcionará la Dirección de Empresas Financieras del Ministerio de Comercio e Industrias a los interesados, los cuales se habilitarán con los timbres fiscales que correspondan.
>
> Para comprobar la veracidad de la información, la Dirección de Empresas Financieras del Ministerio de Comercio e

> Industrias está facultada para realizar las investigaciones que considere pertinentes.

La aceptación de copias de documentos electrónicos en materia procesal se regula por lo establecido en los artículos 833 y 857 del Código Judicial. [35]

Tales disposiciones son del siguiente tenor:

> **ARTICULO 833:** Los documentos se aportarán al proceso en originales o en copias, de conformidad con lo dispuesto en este Código. Las copias podrán consistir en transcripción o reproducción mecánica, química o por cualquier otro medio científico. Las reproducciones deberán ser autenticadas por el funcionario público encargado de la custodia del original, a menos que sean compulsadas del original o en copia auténtica en inspección judicial y salvo que la ley disponga otra cosa.
>
> **ARTICULO 857:** Los documentos privados deben presentarse en sus originales para que tengan el valor que en este Capítulo se les da, pero tendrán el mismo valor las copias de tales documentos en los casos siguientes:
>
> **1.** Cuando la parte contra quien se presente la copia la reconozca expresa o tácitamente, como genuina;

---

[35] En opinion del Licenciado Heriberto Estribi las copias de los documentos electronicos publicos pueden ser aportados en el proceso debido a la frase "cualquier otro medio cientifico" que acepta el uso de las copias de documentos electronicos publicos con la unica condicion que las mismas se encuentren autenticadas por la autoridad en custodia del documentos electronico publico original **ESTRIBI, Heriberto.** E-COMMERCE ASEPCTOS LEGALES Y SEGURIDAD Litho Editorial Chen S A Panama p 115

2. Cuando la copia haya sido compulsada y certificada por el notario que protocolizó el documento a solicitud de quien lo firmó o por cualquier otro funcionario público cuando estuviere en su despacho;
3. Cuando se presente en copia fotostática o reproducida por cualquier otro medio técnico, siempre que sea autenticada por el funcionario encargado de la custodia del original;
4. Cuando el original no se encuentre en poder del interesado. En este caso será necesario, para que tenga valor probatorio, que la autenticidad haya sido certificada por el funcionario público correspondiente, o que haya sido reconocida expresa o tácitamente por la parte contraria o que se demuestre por cotejo; y
5. Cuando se trate de copias provenientes de archivos particulares que utilizan el sistema de microfilmación, debidamente autenticadas por un Notario Público.

Sin embargo, en materia informática es necesario acotar que surgen algunas discusiones con respecto a documentos originales o copias, debido a que por un lado se puede crear un documento a través de una computadora o pc y luego se copia en un dispositivo como lo es un diskette o un disco compacto, -para su archivo- lo que daría nacimiento a dos "originales" idénticos. el de la computadora y el del dispositivo

Es por ello que en los documentos electrónicos es fundamental la necesidad de métodos que le den valor y autenticidad a este medio probatorio, con la posibilidad de la determinación de su autoría, a través de una firma electrónica avanzada, u otros medios de prueba.

El problema en la generación de documentos electrónicos, se da cuando dichos documentos están relacionadas con la red mundial de computadoras, comúnmente llamada Internet, cuya autoría muchas veces queda en el anonimato, pero que los países están tratando de regular, de manera que los documentos electrónicos sean una herramienta útil en el comercio, investigación o en la vida en particular, con criterios de seguridad.

b.- Notarios Digitales

El delito de falsedad documental en documentos electrónicos tiene como base fundamental el bien jurídico protegido: la fe pública", concepto exclusivo que garantiza la confianza de la sociedad en ciertos instrumentos como son el dinero en moneda o papel, los documentos negociables, las tarjetas de crédito, los documentos públicos, los documentos privados debidamente reconocidos, etc., de

manera tal que se puedan dar las relaciones y transacciones entre las personas de una sociedad, de manera ordenada, debido a que está debidamente regulada su expedición.

La única manera conocida hasta el presente que se ha establecido legalmente para que se garantice la originalidad o no de un documento electrónico que puede ser relevante en la esfera jurídica, se da con la posibilidad que un ente público certifique la existencia de dicho documento.

En Venezuela, la Ley de Mensaje de Datos y Firmas Electrónicas, no confiere la autenticidad o fe pública a los documentos o certificados electrónicos, toda vez que dichos documentos no son otorgados conforme a la ley, mediante funcionarios públicos.[36] Sin embargo, en Colombia, la Corte Constitucional, declaró en fallo de 8 de junio de 2000, sobre el alcance probatorio de los mensajes de datos, que el servicio de certificación dan entidades o empresas de certificación privadas, "...puede proporcionar seguridad jurídica a las transacciones comerciales por vía informática, actuando la entidad de certificación como tercero de absoluta confianza.. "

[36] Op Cit pp 118

En Panamá, los "notarios digitales", han sido creados a través del artículo 41 de la Ley 43 de 2001, que señala a la Dirección del Comercio Electrónico o a la Contraloría General de la República, como las entidades o autoridades que en el ejercicio de sus funciones, certifiquen la emisión de un documento electrónico.

Algunos especialistas piensan que con la reglamentación de la Ley 43 de 2001 se pueda permitir que las entidades privadas en Panamá certifiquen los documentos electrónicos públicos, sin embargo, somos de la opinión que una concesión de esa naturaleza sólo se puede hacer a través de la modificación de la misma ley, ya que el Código Judicial, de manera general señala en el artículo 834, que sólo los funcionarios que ejercen un cargo por autoridad pública, en ejercicio de sus funciones, pueden certificar o emitir un documento público.

c.- Uso de otros medios de prueba en los documentos electrónicos

En el caso de los documentos electrónicos privados, existen varias modalidades admitidas por nuestro ordenamiento procesal, que permitirían establecer su autoría, y por lo tanto usar las copias o los documentos electrónicos privados en un proceso, como son

- Un documento electrónico sin firma, reconocido por la contraparte, o no tachado en el proceso, puede pasar a ser un indicio o un medio de prueba.
- La diligencia exhibitoria y la inspección judicial sobre los documentos electrónicos, permiten la identificación del autor del documento, y el uso de un documento electrónico en un proceso.
- Los informes que se puedan solicitar a las entidades u oficinas públicas, en el caso de documentos electrónicos, pueden en conjunto con otros medios de prueba ser valorados para determinar la autoría y validez de un documento electrónico.
- Los dictámenes de peritos sobre los documentos electrónicos, permiten establecer la integridad y originalidad de un documento, y puede perfectamente ser analizado en un proceso.
- Cualquier otro medio de prueba establecido por el artículo 780 del Código Judicial, permite determinar si los documentos electrónicos privados pueden ser considerados en un proceso, como son los testimonios, confesiones, etc.

II.- DETERMINACION ESPACIAL DE LA LEY PENAL APLICABLE

En la configuración del delito de falsedad de documento electrónico, es evidente las diferentes etapas que se dan para que se logre ejecutar un daño, destrucción, adulteración o falsificación de un documento; sin embargo, a pesar que la ejecución de esos "momentos" (ideación, tentativa, desistimiento o consumación) se da en un periodo de segundos por parte del sujeto activo, instigador, coautor o cómplices, lo importante en la protección de un bien jurídico como lo es la fe pública en un documento público o privado, emitido por un medio digital o electrónico, será el momento de consumación del ilícito.

Desde el punto de vista técnico, se dan sendos problemas de investigación del rastreo informático, que se caracteriza por la falta de visualización inmediata de todos los pasos lógicos ejecutados y la numerosa acumulación de procesos individuales que luego se añaden a un todo a lo largo del tiempo.[37]

---

[37] MATA Y MARTIN, Ricardo DELINCUENCIA INFORMATICA Y DERECHO PENAL Edisofer S.L. Madrid 2001 P.152-154

En esta secuencia de ideas, la determinación espacial de la ley penal aplicable en la expedición de un documento electrónico falso con relevancia jurídica es vital.

La información electrónica que se puede generar en un documento electrónico o digital emitido a través del Internet no tiene fronteras nacionales.

Quien lleva a cabo la manipulación informática puede encontrarse a miles de kilómetros de la terminal de la empresa o negocio que recibe un perjuicio patrimonial por la falsificación de un documento electrónico, tal es el hecho que podría darse cuando un sujeto utilice una tarjeta de crédito falsa en Tokio, sobre un cajero automático que tiene referencia al Banco HSBC de Panamá, dándose el perjuicio sobre una cuenta corriente existente de persona distinta al falsificador.

En esta materia, España no cuenta con ninguna norma positiva que señale el lugar en que se entiende cometido el delito, pero para la solución de este problema, la doctrina y la jurisprudencia española

aplican la teoría de la acción, la teoría del resultado y la teoría de la ubicuidad. [38]

En Suiza, país que regula ampliamente la actividad informática y que es uno de los países puntales en cuanto a la generación de normativas que permitan otorgarle la suficiente seguridad de los individuos para utilizar los medios informáticos y electrónicos a través del internet, debaten en la esfera penal y procesal los distintos problemas que se dan con la aplicación de alguna de las tres teorías antes enunciadas.

En los delitos de mera actividad o de resultado, de lesión, de peligro abstracto o peligro concreto, Suiza hace una delimitación más concreta de la aplicación de la ley penal en el espacio, y se inclina a la aplicación de la teoría de la ubicuidad, fijando el lugar de realización del delito tanto en el lugar de la acción como en el resultado.[39]

Situaciones como ésta permiten señalar que no es adecuada la utilización estricta del principio de territorialidad en la ejecución de delitos

---

[38] Cfr Op Cit pp 146

[39] Cfr **JUEZ MARTEL, Pedro.** El Comercio Electronico ¿Hacia una nueva Revolucion Economica y Juridica? http //comunidad derecho org/congreso/ponencia 7 html

de falsedad de documentos electrónicos porque permitiría la impunidad, y es por ello que es conveniente que países como el nuestro, que se dedica principalmente a la generación de servicios, haga un esfuerzo por regular con mayor interés los aspectos procesales y penales de conductas desvaloradas producidas a través de medios electrónicos.

La aplicación de los principios de territorialidad, de personalidad y de justicia universal, deben ser considerados en cada caso concreto, para impedir la anarquía o falta de homogeneidad respecto al derecho a aplicar.

III.- DETERMINACION EN EL TIEMPO DE LA LEY PENAL APLICABLE

Frente a la celeridad con que se dan nuevas conductas desvaloradas en el campo informático y la posibilidad de la creación de leyes penales que tipifiquen dichas conductas, podemos estar frente a la aplicación de los principios de ultractividad y retroactividad de la ley penal, que consagra nuestra Constitución y a los que se refieren los artículos 13 y 14 del Código Penal

El principio de legalidad y seguridad jurídica, basado en el término latino ***tempus regit actum***, puede ser un problema para el juzgador, cuando en la comisión del delito de falsificación en documento electrónico ".. se quieran penar conductas que no eran consideradas delitos al momento de realizarlas..."[40] debido a la posibilidad que la alteración de un documento electrónico se produzca por un programa para ejecutarse en otro momento –un mes o varios años después- con una nueva ley penal y procesal.

En este caso, concordamos con lo comentado por GUERRA DE VILLALAZ, cuando señala:

> "...En este supuesto y acorde con el precepto constitucional que prevé la retroactividad de la ley penal favorable al reo como excepción, este artículo dispone la aplicación de la ley más favorable al procesado. Esto significa que si la ley derogada la beneficia, debe aplicarse con efectos ultractivos y si por el contrario, es la nueva ley la que le favorece, entonces se le aplicaría con carácter retroactivo".[41]

Esta posibilidad debe ser considerada especialmente ante la tendencia nacional a la derogación, modificación o adición de las

---

[40] **RIQUERT, Marcelo Alfredo.** INFORMATICA Y DERECHO PENAL ARGENTINO Editora Ad-Hoc Buenos Aires Argentina 1999 pp 125

[41] **GUERRA DE VILLALAZ, Aura E.** CODIGO PENAL COMENTADO Editorial Mizrachi & Pujol S A Panama 2001 pp 16

leyes penales. Por ejemplo, ante el problema de un programa a ejecutarse en el tiempo, sería necesario tomar en cuenta el resultado, y no la manifestación de voluntad o el actuar positivo del sujeto activo, que aplicó un programa en un tiempo pasado (cuando no se había creado la ley penal que tipificaba y sancionaba su conducta), pero que el resultado se da cuando ya está promulgada la ley. En un supuesto como este, el juzgador estará ante la disyuntiva si debe tomar en cuenta que "el tiempo" es un artificio o una técnica para evadir el rastreo del autor, o por el contrario, se debe aplicar la ley más favorable al reo, y como al momento de la ejecución material del sujeto no existía la ley penal, no debe haber encausamiento.

Somos de la opinión que cada caso debe ser examinado conforme a Derecho, pero en un ejemplo como el anterior, se debe desistir de continuar con la causa, ya que no se puede admitir que se sancione a alguien que ejecutó un programa y tal hecho no estaba tipificado por la ley en ese momento.

CAPITULO CUARTO

CONSIDERACIONES DE POLÍTICA CRIMINAL EN EL DELITO DE FALSEDAD DE DOCUMENTOS ELECTRÓNICOS

I.- LA DIGITALIZACIÓN DE LOS DOCUMENTOS

La era electrónica, representada por la aparición de las computadoras y todo tipo de instrumentos electrónicos que son capaces de producir información, han dado paso a la era digital, que se caracteriza por la normalización de todas las redes informáticas constituidas desde finales de los años setenta, relacionándose de tal manera unas con otras, que el acceso a información –de cualquier naturaleza- llega con una rapidez insospechada y en cantidades ilimitadas.

A pesar que todavía hoy recibimos la mayor parte de información en libros, periódicos y revistas, concordamos en lo que advierte MORON LERMA, sobre este tema, al señalar que "...la evolución natural de esta era de la información, esto es, la interconexión de los ordenadores en redes y de éstas en autopistas de

la información está transformando el átomo en ***bit*** y, por tanto, lo analógico en digital"[42]

A pasos agigantados, los documentos electrónicos que nos están empezando a dar información de nuestro medio, ya son accesados por inmersión debido a la influencia de la masificación de la comunicación, y que por el avance acelerado de altas tecnologías están produciendo nuevas formas de realidad, en espacio y tiempo, cuya dimensión se le está denominando "ciberespacio".[43]

La avidez para adquirir más conocimientos, la evolución de la tecnología en cuanto permite obtener, procesar y transmitir información en tiempo real desde cualquier lugar del planeta – y más allá, como lo es a través de un satélite en el espacio-, el abaratamiento de las computadoras y todos los sistemas digitales que facilitan y globalizan la comunicación, ya al momento actual, estamos en capacidad de hablar no de un documento electrónico, sino de un

---

[42] **MORON LERMA, Esther.** INTERNET Y DERECHO PENAL HACKING Y OTRAS CONDUCTAS ILICITAS EN LA RED Editorial Aranzadi Pamplona España, 1999 pp 78

[43] La palabra *ciberespacio* proviene del termino ingles *cyberspace* utilizado por el escritor de ciencia ficcion William Gibson en su novela llamada "Neuromancer" de 1980, donde el autor imagina un futuro donde las grandes empresas internacionales han reemplazado a las naciones y todas las actividades como el comercio o el entretenimiento se da a traves de las redes informaticas con la construccion abstracta de datos que representan la realidad virtual Cfr **PALAZZI.** DELITOS INFORMATICOS Op Cit Pp 247 Este concepto se esta empezando a utilizar cada vez mas para describir las formas y tiempo de interconexion de las redes las distintas velocidades a que se puede accesar a la comunicacion por internet y las formas de interconexion

"documento digital", cuya transformación vertiginosa empieza a conducirnos a una memoria "molecular", debido a la posibilidad de almacenamiento de información en átomos de hidrógeno, que han llegado a más de 1,000 ***bits*** de información.[44]

a. Peligros de intercepción del documento electrónico.

Con la posibilidad de interconexión de todos los sistemas telemáticos, informáticos y electrónicos en el mercado, es viable la comunicación de los datos e informaciones contenidas en los sistemas.

La expansión ilimitada del ámbito operativo de las nuevas tecnologías, como por ejemplo: los celulares, laptops, agendas digitales, e-mail, calendarios y directorios corporativos, acceso a páginas web y monitoreo de sistemas remotos o VPN (Virtual Private Network) [45] hacen prácticamente imposible no afrontar el riesgo de

---

en donde el sujeto denominado *cibernauta* "navega" en cualquier direccion y sentido para accesar a la información Cfr **MORON LERMA,** pp 77 y ss

[44] EL PANAMA AMERICA Computaworld Tecnologia y Negocios Año 6, No 23 diciembre 2002 p 4

[45] La compañía Bellsouth Panama, anuncio en noviembre de 2002 el lanzamiento de telefonos de 'tercera generacion con tecnología CDMA garantizando la privacidad de las llamadas debido a que la informacion transmitida se encuentra codificada con una combinacion unica entre mas de 4 trillones de codigos los cuales pueden intereconectarse con la mas variada cantidad de dispositivos de datos de alta velocidad La Prensa 8 de noviembre de 2002 p 2A

que ser víctimas del fraude o la clonación de terminales, que permitan daños en los sistemas e información de datos.

En Panamá, La Superintendencia de Bancos ha declarado en entrevista realizada a su directora, que diariamente el sistema operativo de computadoras, que almacena información confidencial de los bancos del país, es atacado en más de una docena de veces.[46]

Personas comunes, que accesan al sistema de Internet por medio de su computadora personal, declaran que con la instalación de programas –algunos gratuitos y accesibles a través del sistema- han visto que "...en sólo tres meses he tenido 628 ataques sospechosos y 32 ataques críticos. Y menos de media docena de esos ataques fueron provocados por mi desconocimiento".[47]

Independiente de la conducta ilícita que se realiza, al modificar un documento, sustraer o apropiarse de información, o suplantar identidad, los costos económicos son incalculables, debido a que como medida de prevención se ha creado una gran cantidad de programas de protección, cuyos costos son elevados en el ámbito del ***hardware y software***, a ello cabe añadir el costo de reposición,

---

[46] LA PRENSA 2 de septiembre de 2002 pp 1 y

[47] Protegiendose contra ataques" en PC World Panama Año VIII Numero 90 agosto 2000 p 70

pérdida de productividad, inversiones en personal de mantenimiento, operación y reinstalación del programa y los datos.

La conducta usual de la víctima según algunos estudiosos del tema, es pactar con el sujeto activo, debido a que una denuncia en materia de ilícitos informáticos son difíciles de detectar, y el temor a que la trascendencia del hecho se traduzca en descrédito de la fiabilidad de la gestión de la empresa.[48]

Uno de los casos más alarmantes es el robo y sustitución de identidad que se ha hecho contra bancos y financieras de Estados Unidos de la empresa Teledata Communications Inc. (TCI), donde uno de sus empleados sustrajo claves y entregó contraseñas para descargar informes crediticios a voluntad. El ex-empleado logró falsificar varios documentos con datos e información falsa de los cuentahabientes, emitiendo tarjetas de crédito falsas o con saldos no justificados.[49]

---

[48] Cfr. **MORON LERMA**, Op. Cit. pp. 37 y 38.

[49] EL PANAMA AMERICA. 10 de diciembre 2002. p. 7.

b. Garantías de los documentos electrónicos con la nueva tecnología.

Así como las nuevas tecnologías generan la comisión de nuevas y novedosas formas de cometer abusos y falsificaciones sobre documentos contenidos en medios electrónicos, ellas igualmente ayudan a combatir y prevenir las conductas que pueden causar perjuicio, por el abuso del manejo de la información.

A continuación, y por considerarlo pertinente al punto que venimos tratando, mencionaremos algunos de los sistemas existentes, que pueden ayudar a garantizar la veracidad de un documento, o a prevenir los ataques:

1. Browser

El ***browser*** es un ***software*** comercial que se ha diseñado por los especialistas en programas de computadoras para monitorear las estaciones de trabajo de una compañía y sus comunicaciones a través de internet.

Con este programa se puede tener acceso de monitoreo hasta al correo electrónico, en el área laboral, el cual permite observar la manipulación de documentos y datos de la compañía por parte de sus empleados.

2. La criptografía

La palabra criptografía proviene de la raíz griega ***kriptos***, que significa oculto, y ***grafos*** , que hace referencia a lo escrito; de manera que es un sistema técnico que sirve para ocultar mensajes o información escrita.

En la década de los setenta, IBM en conjunto con la Universidad de Stanford en Estados Unidos desarrolló el método encriptado DES, que significa "estándar de encripción de datos" o *Data Encryption Standard* por sus siglas en inglés, y en la misma década se trabajó en el sistema RSA, desarrollado por el Instituto Tecnológico de Massachussets (MIT), que encripta asimétricamente los mensajes o datos y es el más utilizado en la actualidad en el intercambio comercial de datos en medios electrónicos.[50]

El sistema criptográfico, se ha ido desarrollando en el sistema informático, y en consecuencia, en la transmisión de datos, información y documentos electrónicos, desarrollando la firma

---

[50] Cfr. **ESTRIBI**, Op. Cit. Pp. 53-69

electrónica, como garante de seguridad, confidencialidad y privacidad en la comunicación.

Si bien existe la posibilidad de decodificar la forma cifrada en que se emiten los mensajes por sistemas telemáticos y electrónicos, de manera que se puede sustraer y falsificar información sensitiva, hasta ahora es uno de los métodos o sistemas técnicos más usados para lograr un buen grado de confidencialidad en el sistema.

II.- POLÍTICA CRIMINAL EN LOS DELITOS DE FALSEDAD DE DOCUMENTOS ELECTRÓNICOS

Es evidente que no existe en el ordenamiento penal de Panamá, ni en el de la mayoría de los países del mundo, regulaciones específicas que eleven a la categoría de delito, actividades relacionadas con la falsificación de documentos electrónicos (que han evolucionado a los llamados documentos informáticos y posteriormente a documentos digitales), que tienen la capacidad de comprometer a los asociados, crear relaciones económicas, civiles o privadas entre las partes y que por consiguiente, deben ser protegidos para que los usuarios tengan confianza en el sistema

Cuando tratamos de subsumir una conducta desvalorada, relacionada con la falsificación de documentos electrónicos, porque ocasiona un perjuicio moral, social o económico, y no se encuentran descritas todas las fórmulas posibles de actuación, es evidente que se hace necesaria una revisión de la regulación existente.

Panamá acaba de tener una experiencia negativa reciente, con motivo de la falsedad de documentos electrónicos sobre la cédula de identidad personal.

A la empresa estadounidense Unysis, que prestaba el servicio de expedición de cédulas al Tribunal Electoral, con relación al programa y el material con que se emitían los documentos de identidad personal de los ciudadanos panameños, le encontraron papelería y plásticos relacionados con ese servicio en depósitos ajenos a las empresas y parte de ellos en los Estados Unidos.

Este tipo de conducta, en lo que respecta a nuestro país, ha puesto en peligro hasta las elecciones presidenciales del año 2004, amén de los perjuicios económicos al Estado y a los particulares. Hasta ahora no se han cuantificado tales perjuicios, pero en la Policía Técnica Judicial, reposan desde hace varios meses sendas denuncias de nacionales panameños que se han enterado al requerir préstamos o

información comercial, que personas de otras nacionalidades han estado utilizando su identidad para trabajar o accesar beneficios financieros o económicos, con cédulas de identidad falsas.[51]

A raíz de estas denuncias, se están investigando otras falsificaciones o conductas peligrosas que se hayan podido dar, toda vez que la empresa también prestó servicios a la Dirección de Pasaportes del Ministerio de Gobierno y Justicia, en la expedición de pasaportes panameños.

Con estas realidades, es evidente que se hace necesario instaurar una política criminal en nuestro país, que abarque este tema, para evitar escándalos y perjuicios relacionados con la falsificación de documentos electrónicos.

a. Políticas Internacionales

Con el desarrollo tecnológico en materia de informática, los cuales traspasan fronteras geográficas de las naciones, los países desarrollados como Estados Unidos de Norteamérica, Gran Bretaña, Alemania, Austria y Francia, entre otros, han desarrollado desde la década de los ochenta normas legales específicas relacionadas con los delitos informáticos.

---

[51] LA PRENSA Noviembre 12 de 2002 pp 2

Es importante destacar la labor e iniciativas desarrolladas por la Organización de Cooperación y Desarrollo Económico (OCDE), que ha recomendado –desde 1983- una serie de consideraciones legales, para que se añadan en las legislaciones de los países y exista uniformidad entre las naciones, de forma tal que se puedan combatir conductas perjudiciales para los usuarios de datos, información o documentos generados por medios electrónicos.[52]

Se adiciona a esta labor, lo recomendado en el Octavo Congreso sobre Prevención del Delito y Justicia Penal organizado por Naciones Unidas en la Habana Cuba en 1990, consistente en una serie de directrices sobre la seguridad de las computadoras, de tal modo que se logre que la comunidad internacional controle las modalidades de delitos en esta materia.[53]

b. Consideraciones para la incriminación

La evidente transformación en nuestro mundo, con el desarrollo de la tecnología, ha demostrado que las formas de poder, de acceso al trabajo y a la información, está acarreando no sólo formas más rápidas

---

[52] Cfr. RIQUERT. Op. Cit. pp. 51-52

[53] Cfr. MORON LERMA. Op. Cit. Pp. 34

de desarrollo, sino también problemas sociales y políticos, que han revolucionado la estructura de la sociedad.

Estas consideraciones hacen evidente la necesidad de establecer nuevos planteamientos en el campo jurídico, que permitan la tutela y protección legal de la información, datos y documentos generados por la nueva tecnología.

La necesidad de ubicación sistemática de los delitos informáticos, nos llevan a plantearnos si debe tenerse como un delito de carácter pluriofensivo, o "propugnar por la aparición de un nuevo interés supraindividual, de carácter difuso, merecedor de la tutela penal, a saber, la seguridad en los sistemas informáticos".[54]

Las enormes pérdidas millonarias que se dan con la comisión de acciones desvaloradas en la información y los documentos, han estado propugnando por un exceso de reacción penal, que en cierto sentido pueden colisionar con derechos humanos constitucionales existentes.

La doctrina por su parte, ha estado argumentando que en principio, para lograr una tipificación de las conductas relacionadas

---

[54] MORON LERMA. Op Cit Pp 67

con los sistemas informáticos, se deben hacer las siguientes consideraciones:

1.- Los estudios criminológicos en países como Alemania, Francia y Estados Unidos, indican que la mayoría de los comportamientos de invasión, *hackeo* o ataques de computadoras a otros sistemas de datos no autorizados, terminan convirtiéndose en ilícitos más graves con ataques a la intimidad, al patrimonio, etc. [55]

En este sentido, es importante tomar en cuenta que si se desea incriminar conductas de peligro, como es el accesar a datos e información no autorizada a través de los sistemas de computadoras, hay que ser sumamente cuidadoso, ya que se pueden afectar los principios de intervención mínima del Derecho Penal y el de ***ultima ratio***, entendiendo que deben antes de una incriminación penal agotarse otros recursos o instrumentos jurídicos de carácter civil o administrativo, que pueden lograr los mismos fines.

---

[55] Cfr **ARAUZ SANCHEZ**, Op Cit p 54

2.- Se han dado recomendaciones a través de los técnicos de seguridad informática, criminólogos y penalistas, para que se apliquen medidas de seguridad preventivas, como respuesta al actuar desvalorado de algunas personas frente a la posibilidad de accesar, falsificar o cometer un fraude a través de los datos y documentos electrónicos digitales.[56]

Este planteamiento se puede fundamentar en el hecho que estamos ante una "sociedad de riesgos", debido al avance tecnológico creciente, y las penas y sanciones existentes por la comisión de conductas desvaloradas que causan pérdidas millonarias y hasta la quiebra de empresas, son intrascendentes, para motivar al "delincuente informático" en desistir de su actuar.

Es por ello que se recomiendan las auditorías y los programas de protección a las computadoras que tienen información sensitiva, de manera que se puedan proteger los datos existentes.

3,- Es imprescindible la colaboración y asistencia técnica entre los países, para regular uniformemente el acceso a las computadoras y a la información, ya que tal como se ha mencionado anteriormente, la

[56] Cfr. MORON LERMA Op Cit Pp 72

dimensión de acceso descentralizado de la información, y la posibilidad infinita de intromisión a información de otras naciones con regulación o no de los sistemas informáticos, permite las actitudes con fines ilícitos de las personas que sin autorización accesan a documentos con validez jurídica.

CAPITULO QUINTO

ANÁLISIS DE ENTREVISTAS REALIZADAS

I.- INTRODUCCIÓN

Como parte de este trabajo, sobre los delitos de falsedad documental en documentos electrónicos, consideramos necesario hacer una investigación de campo, a fin de complementar la información bibliográfica con otras técnicas que, capten cómo operan en el mundo fáctico.

Realizamos entrevistas sobre diversos temas relacionados con la utilización inadecuada y falsificación de documentos electrónicos, telemáticos y digitales, a personas relacionadas con empresas o instituciones del Estado, que tienen entre sus funciones guardar información sensitiva, o generar documentos electrónicos que pueden utilizarse como pruebas, pues son idóneos para entrar en el tráfico jurídico.

Logramos hacer entrevistas en dos bancos privados de la localidad y al personal de la Superintendencia de Bancos, adscrita al Ministerio de Economía y Finanzas y el Registro Público, que se rige por lo que establezca el Ministerio de Gobierno y Justicia

Las entrevistas realizadas tuvieron como propósito determinar el conocimiento de las personas relacionadas con el manejo o custodia de documentos electrónicos en los siguientes aspectos:

- Conocimiento de la normativa penal, en materia de documentos electrónicos.
- Conocimiento de la reglamentación de carácter administrativo sobre protección de documentos electrónicos.
- Causas de la comisión del delito de falsificación de documentos electrónicos
- Sujetos más propensos a cometer el delito de falsificación de documentos electrónicos.
- Si se recomienda que se debe mejorar la legislación o reglamentación vigente para la protección de los documentos electrónicos, de posibles fraudes o falsificaciones.

Cada una de estas variables, guarda relación con los temas desarrollados en esta investigación.

La muestra invitada fue de 15 personas, y la muestra participante fue de 12. Dos personas del sector privado y 10 del sector público

Todos los invitados son profesionales de distintas ramas, a saber: licenciatura en tecnología, licenciatura en sistemas, auditores, licenciados en contabilidad y abogados.

Todos los invitados tienen más de 30 años, de los cuales 8 son mujeres y 4 hombres.

Las limitaciones o dificultades para realizar las entrevistas y realizar la totalidad de la cifra invitada, se debió a que en las entidades privadas se trata de guardar una mayor confidencialidad sobre la materia de documentos electrónicos, y las personas que deseábamos entrevistar estaban impedidas por cuestiones de seguridad, según la gerencia.

En el sector público tuvimos una amplia disposición del personal a entrevistar, que creemos se debió a que las jefas de las entidades con las cuales conversamos previamente y se les solicitó permiso previo para la entrevista son abogadas, ello nos permitió la disponibilidad de información y del personal entrevistado.

II.- ANALISIS DE LAS ENTREVISTAS REALIZADAS

Se hizo un análisis por parte de los funcionarios y empleados del conocimiento sobre temas mencionados en los capítulos anteriores.

1.- Legislación penal sobre documentos electrónicos

Se cuestionó al entrevistado si conocía o tenía poco conocimiento sobre legislación penal relacionada con la falsificación de documentos electrónicos, de los cuales el 33.33% declaró que sabía que no existía normativa penal específica sobre falsificación de documentos, pero que en esta materia se regulaba por el Código Penal, de ahí, un 25% señaló que sabía muy poco de la legislación penal relacionada con falsificación de documentos, y un 41.67% declaró que no conocía ninguna norma penal relacionada con falsificación de documentos electrónicos. (Ver Fig. No. 1)

2.- Legislación administrativa sobre documentos electrónicos

En la entrevista sobre el conocimiento de los encuestados, relacionada con la legislación administrativa existente, que regulara la emisión de documentos electrónicos, el 41.67% expresó que sí

conocía otras normativas de carácter administrativo, como es la Ley No. 43 de 2001, por la cual se define y regulan los documentos y firmas electrónicas, las entidades de certificación en el comercio electrónico y el intercambio de documentos electrónica.

De todos los entrevistados, sólo uno reconoció que además de la Ley 43, existía un reglamento interno en la institución, que regulaba el tema de falsificación de documentos electrónicos, de manera indirecta, al establecer formalidades de manejo y de carácter ético al personal que manejaba material sensitivo.

El 58.33 de los entrevistados reconoció que desconocía alguna normativa de carácter civil, administrativo o reglamentario sobre documentos electrónicos (Ver Fig. No. 2)

3.- Causas de falsificación de documentos electrónicos

Cuando se hizo la entrevista a las personas, se les dijo que fuesen amplios en la respuesta a esta pregunta, toda vez que la profesión y los cargos no son homogéneos y se puede tener conocimiento de distintas formas de falsificación de documentos electrónicos

El 41.67% señaló que una de las causas de falsificación de documentos electrónicos era el descuido o negligencia, no sólo de las entidades, sino de los mismos usuarios al manejar en los códigos y claves además de la falta de programas de protección adecuados a la información o al ***software.***

De la muestra, el 25% señaló que otra de las causas era el acceso a internet, que permitía la intrusión de terceros a los e-mails y cuentas de los cuentahabientes de los Bancos. En ese sentido, el grupo que señaló que el internet era una causa, explicó que no importaba cuantos programas de protección pusiera, siempre sería violado el programa por alguien; además señalaron que existía mucha ignorancia en el medio y muchas veces se tenían las computadoras en un modo que permitían el acceso de intrusos.

Un 16.63% de los encuestados señaló que una de las causas de falsificación de documentos se debía a los mismos funcionarios o trabajadores de las instituciones y empresas, que tienen acceso a los programas y computadoras del sistema.

Se hizo referencia a la falta de ética y responsabilidad de los funcionarios, señalando por parte de dos entrevistados que por experiencia, los casos de falsificación o fraude cometidos en el

sistema, se debían a fuga de información confidencial de los mismos empleados.

Por otro lado, para nuestra sorpresa, un 25% contestó que desconocía cuáles eran las causas de falsificación de documentos, de lo cual nos permitimos suponer que una respuesta como ésta, de un personal directamente relacionado con el archivo o generación de información que se traduce en documentos electrónicos, se debe a ese aspecto de seguridad y confiabilidad que las empresas o instituciones de esta naturaleza deben mantener ante los usuarios. (Ver Fig. No. 3)

4.- Sujetos que pueden ser causantes de falsificación de documentos electrónicos.

Todos los entrevistados nos señalaron en orden de prioridad con respecto al sujeto que puede ser causante del delito de falsificación de documentos electrónicos, incluyendo los que en la respuesta anterior no contestaron cuáles eran las causas de falsificación de documentos electrónicos.

En un análisis de estas respuestas, pareciera que existe contradicción en los encuestados sobre la causa y la persona que puede ser el causante de una falsificación de documentos electrónicos,

sin embargo, el hecho que un 25% de los entrevistados manifestó desconocer las causas, pero luego todos aceptan conocer quién es más proclive en la comisión del ilícito, nos refuerza la opinión en manifestar que casi el 50% de los posibles causantes de falsificación de documentos electrónicos son personas que laboran o han laborado con la empresa.

En esta etapa de la entrevista, se cuantificó que el 50% de los entrevistados reconocían al funcionario o empleado de la entidad garante de los documentos electrónicos, como el principal causante que ocurra la falsificación de documentos.

De la muestra, 41.67% señaló a los usuarios y cuentahabientes como los posibles agentes en la comisión de los delitos de falsificación de documentos electrónicos.

El 8.33% reconoció que un tercero, sin relación alguna a la empresa puede ser el causante de la falsificación de documentos electrónicos. (Ver Fig. No. 4)

5.- Debe mejorarse la legislación penal existente. ¿Por qué?

En esta etapa de la entrevista, sólo el 16.67% de los encuestados consideró que no era necesario modificar la legislación

penal existente, toda vez que muchas de las conductas que se querían sancionar, por estar relacionadas con la emisión de documentos electrónicos, se subsumen a conductas ya tipificadas en el Código Penal existente.

El 83.33% de los entrevistados consideró que se hace necesaria una mejor legislación penal sobre falsedad de documentos electrónicos.

Las razones que se estimaron para mejorar la legislación , fueron las siguientes:

- La falsificación de documentos electrónicos no sólo viola normas contra la fe pública, sino que con su realización se cometen delitos, penalizados con penas más graves.
- Es necesario modificar las sanciones para agravarlas, debido al gran perjuicio que ocasionan, muchas veces millonario.
- Panamá es un país con economía terciaria, de servicios, los cuales se brindan con las últimas tecnologías del mundo, y si las operaciones bancarias representan el 13% del PIB, traducidas en documentos electrónicos, deben ser mejor protegidas todas las transacciones que ellos generen, o lo existente quedaría obsoleto

- La globalización de las transacciones bancarias o de toda naturaleza implica que la legislación nacional se adecue a la existente en otros países, con referencia a la falsificación o fraude de documentos electrónicos.

  (Ver Fig. No. 5)

CONCLUSIONES

Finalizado el trabajo de investigación sobre la falsificación de documento electrónico, podemos hacer las siguientes conclusiones:

El documento electrónico es un elemento material que en algún momento puede ser intangible, pero siempre puede ser reproducido, copiado o accesado, el cual contiene un pensamiento, imagen, sonido o idea, con un significado lógico a nuestros sentidos.

Entre las formas que puede contener un documento electrónico están las cintas magnetofónicas, cintas cinematográficas, diskettes, discos compactos de escritura o sonido, tarjetas con banda magnética, chips, microchips, y el disco duro de una computadora, entre los más conocidos y utilizados.

Debido a que Panamá es un país dedicado principalmente a la actividad de servicios, se ha estado usando en forma contínua y creciente las nuevas formas de documentos electrónicos y digitales, lo cual ha permitido que se sancionara la Ley 43 de 31 de julio de 2001, que regula lo referente al comercio y documentos electrónicos, firmas electrónicas y entidades de certificación en el comercio electrónico y el intercambio de documentos electrónicos.

La Ley 43 de 31 de julio de 2001 no desvirtúa los principios establecidos en el Código Judicial en materia de documentos en general, y añade de manera exclusiva entidades reconocidas por el Estado como son la Contraloría General de la República y el Ministerio de Comercio e Industrias, a través de la Dirección de Empresas del Comercio Electrónico para ejercer como "Notarios Digitales".

Las formas de falsificar un documento electrónico se mantienen en lo establecido hasta ahora por nuestro Código Penal, como es el formar, hacer, suprimir, ocultar o destruir un documento, pero con el uso de nuevas tecnologías, como son: datos engañosos, técnica salami, *superzapping*, recogida de residuos o basura en el internet, puertas falsas o puertas con trampas y bombas lógicas, los cuales se instauran por el sujeto activo en los programas de las computadoras

Debido a que lo que interesa al Derecho Penal es todo lo que es capaz de entrar al tráfico jurídico, el documento electrónico que se debe tutelar es aquel que puede valorarse y presentarse en el debido proceso, como garante de la información que contiene.

Es posible que se tutele en el ámbito penal las copias de documentos electrónicos públicos y documentos electrónicos

privados, si son autenticadas por la autoridad en custodia del documento electrónico original.

La conducta usual de las víctimas en la comisión del delito de falsificación de documentos electrónicos, es transar con el sujeto activo, por un beneficio económico, por la complejidad de la investigación al rastrear los datos, y el temor a que la trascendencia del hecho se traduzca en descrédito o falta de fiabilidad de la víctima.

La manifestación del delito de falsificación de documento electrónico también refleja la ejecución de una diversidad de conductas típicas y modalidades delictivas, como son la comisión de delitos contra la administración pública, el patrimonio, la seguridad colectiva, la libertad y la economía nacional, por lo cual se considera como un delito "pluriofensivo".

Se considera que el delito de falsificación de documento electrónico es un "medio" para la ejecución de otros delitos.

Los problemas de investigación y rastreo informático por la gran cantidad de pasos lógicos que se ejecutan en fracción de segundos, en la emisión de los documentos electrónicos falsos o la manipulación informática a miles de kilómetros de la terminal de la

empresa o negocio, abren varias interrogantes en el ámbito penal, para determinar la ley penal aplicable en el tiempo y en el espacio.

El problema de ultractividad o retroactividad penal , así como el rastreo geográfico del lugar donde se produjo una falsificación de documento electrónico, debe ser analizado en forma particular y conforme a Derecho, a fin de dar respuestas adecuadas a la problemática penal de la ejecución del delito de falsedad en documento electrónico.

En virtud de los esfuerzos y avances en otras latitudes por reglamentar, y establecer procedimientos uniformes en materia de delitos informáticos, y la interconexión de las redes de información, se propugna que Panamá se adhiera a esos esfuerzos y reforme la legislación vigente en materia comercial, administrativa y penal sobre todas las conductas que pueden ser lesivas a los derechos de las personas en la emisión de documentos electrónicos falsos.

RECOMENDACIONES

1. Recomendamos que se reglamente la Ley 43 de 31 de julio de 2001, que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos; a fin que se dé un verdadero reconocimiento jurídico a los documentos electrónicos y digitales, con validez y fuerza obligatoria para las partes.
2. Debe crearse la Dirección de Comercio Electrónico en la Dirección Nacional de Comercio del Ministerio de Comercio e Industrias, para que se garantice un nivel básico y de seguridad en los documentos y firmas electrónicas.
3. Es necesario que se implemente la firma digital o firma electrónica en todos los documentos electrónicos que contienen datos o información de importancia, a fin que su emisión y transacción se dé en forma ordenada.
4. Recomendamos se hagan esfuerzos en materia legislativa para que se integre la legislación comercial, administrativa y penal nacional a la codificación internacional que ya han hecho

países como Estados Unidos, Alemania y España en el llamado "delito informático".

5. Debe haber una toma de conciencia en política criminal sobre los ataques a los sistemas informáticos, de manera que se puedan proteger las fuentes de servicio y emisión de documentos electrónicos y digitales en nuestro país.

BIBLIOGRAFIA

OBRAS GENERALES

ARAUZ SANCHEZ, Heriberto. LA ACCION DE HABEAS DATA. Universal Books. Panamá, 2002.

BREWER, Allan-Randolph. CONSIDERACIONES ACERCA DE LA DISTINCION ENTRE DOCUMENTO PUBLICO O AUTENTICO, DOCUMENTO PRIVADO RECONOCIDO Y AUTENTICADO Y DOCUMENTO REGISTRADO. Ediciones Fabreton, Caracas, 1995.

CASAS BARQUERO, Enrique. EL DELITO DE FALSEDAD EN DOCUMENTO PRIVADO. Bosch, casa editorial, Barcelona, 1984.

ESTRIBI, Heriberto. E-COMMERCE, ASEPCTOS LEGALES Y SEGURIDAD. Litho Editorial Chen, S.A. Panamá

FABREGA, Jorge. 1.MEDIOS DE PRUEBA 2. LA PRUEBA EN MATERIA MERCANTIL. Segunda Edición. Editora Jurídica Panameña, Panamá. 1998.

GUERRA DE VILLALAZ, Aura E. CODIGO PENAL COMENTADO. Editorial Mizrachi & Pujol, S.A., Panamá, 2001.

GUERRA DE VILLALAZ, Aura. DERECHO PENAL PARTE ESPECIAL. Editorial Mizrachi & Pujol, , S.A., Panamá, 2002.

MATA Y MARTIN, Ricardo. DELINCUENCIA INFORMATICA Y DERECHO PENAL. Edisofer, F.L. Madrid, 2001 .

MORON LERMA, Esther. INTERNET Y DERECHO PENAL: HACKING Y OTRAS CONDUCTAS ILICITAS EN LA RED. Editorial Aranzadi, Pamplona, 1999

MUÑOZ CONDE. Francisco. DERECHO PENAL. PARTE ESPECIAL. 7a. ed., Tirant Lo Blanch, Valencia, 1988.

PALAZZI, Pablo A. DELITOS INFORMATICOS. Editora Ad-Hoc S.R.L., Buenos Aires, 2000.

PALAZZI, Pablo A. LA TRANSMISION INTERNACIONAL DE DATOS PERSONALES Y LA PROTECCION DE LA PRIVACIDAD. Argentina, América Latina, Estados Unidos y la Unión Europea. Editora Ad-Hoc S.R.L., Buenos Aires, 2002.

RIOFRIO, Juan Carlos. LA PRUEBA ELECTRONICA. Editorial Temis, Bogotá, 2004

RANIERI, Silvio. Manual de Derecho Penal. De los delitos en particular. Parte Especial. Tomo IV,. Edit. Temis. Bogotá, 1975.

RIQUERT, Marcelo Alfredo. INFORMATICA Y DERECHO PENAL ARGENTINO. Editora Ad-Hoc. Buenos Aires, 1999.

SANCHIZ CRESPO, Carolina. LA PRUEBA POR SOPORTES INFORMATIOS. Tirant lo Blanch. Valencia. 1999.

TELLEZ VALDES, Julio. DERECHO INFORMATICO. Universidad Nacional Autónoma de México, México, 1987.

VILLALOBOS, Edgardo. INTRODUCCIÓN A LA INFORMATICA. INFORMATICA JURÍDICA Y DERECHO INFORMATICO. Alfa Omega Impresores. Panamá 1997.

MONOGRAFIAS

GUERRA DE VILLALAZ, Aura E. DELITOS CONTRA LA FE PUBLICA. (Tíulo VIII del Código Penal), Taller Senda, Panamá, 1989.

MATA Y MARTIN, Ricardo. ALGUNAS CONSIDERACIONES SOBRE INFORMATICA Y EL DERECHO PENAL. EL CASO DE LA ESTAFA INFORMATICA Colección Austral Madrid, 2001.

REVISTAS

CASTRO, Jorge. LA SOCIEDAD DEL CONOCIMIENTO. INTERNET Y EDUCACION. Revista Derecho y Economía Digital 2000, Buenos Aires, 2000.

JOVANE, Lissy. PROBLEMAS JURIDICOS DEL COMERCIO ELECTRONICO. En Revista Lex. Colegio Nacional de Abogados. Editorial Mizrachi & Pujol, S.A., Marzo 2001

MATA Y MARTIN, Ricardo M. Algunas consideraciones sobre Informática y Derecho Penal. El caso de la estafa informática. En Documentos Penales y Criminológicos, Vol. 1, Año 2001, Nicaragua 2001

RAFOLS LLACH, Juan. FALSEDAD DOCUMENTAL Y DEFRAUDACION FISCAL. En Cuadernos de Derecho, Derecho Judicial. La Nueva Delincuenca I. Consejo General del Poder Judicial. Mateu Cromo, S.A., Madrid, 1993.

RIBAS, Xavier. LA FIRMA DIGITAL. Revista informática, enero. Madrid, 1997

STEVE, Bass. Protegiéndose contra ataques". Alta Velocidad, guía de supervivencia. En PC World. Panamá. Año VIII Número 90, agosto 2000.

TEXTOS LEGALES

CODIGOS

ARGENTINA, Códigos. CODIGO PENAL DE LA NACIÓN ARGENTINA, Editorial LaRocca. 1994

PANAMA, Códigos. CODIGO PENAL. Editorial Mizrachi & Pujol, S.A., Panamá, 1993

PANAMA, Códigos. CODIGO JUDICIAL. Editorial Mizrachi & Pujol, S.A., Panamá, 2001.

LEYES

PANAMA, Leyes. Ley No. 43 de 31 de julio de 2001.

PÁGINA WEB

JUEZ MARTEL, Pedro. EL COMERCIO ELECTRÓNICO: ¿HACIA UNA NUEVA REVOLUCIÓN ECONÓMICA Y JURÍDICA? . Ponencia en el VIII Congreso Iberoamericano de Derecho e Informática realizado en Lima Perú, Marzo, 2001. http://comunidad.derecho.org/congreso/ponencia 7.html

PERIODICOS

ROBERTS, Paul. «Robo de Identidad cuestiona Seguridad ».En El Panamá América. 10 de diciembre de 2002. Computerworld. Pp. 7
ZARATE, Abdiel. "Delitos Informáticos" en **La Prensa**, 22 de octubre de 2001, Sección Revista Pag. 1b.

ANEXOS

UNIVERSIDAD DE PANAMA
FACULTAD DE DERECHO Y CIENCIAS POLITICAS
MAESTRIA EN CIENCIAS PENALES

ENTREVISTA

OBJETIVOS:

- Determinar el conocimiento que tiene la ciudadanía sobre la normativa penal existente en materia de documentos electrónicos
- Determinar el conocimiento que se posee en torno a la clase de documentos electrónicos sobre los cuales puede haber responsabilidad penal.
- Establecer qué documentos electrónicos están y/o deben estar protegidos por normativas de carácter penal.
- Detectar la fase o forma en que se realizan la mayor cantidad de fraudes y/o falsificaciones en los documentos electrónicos
- Hacer recomendaciones para minimizar las conductas desviadas en lo relacionado con documentos electrónicos.

DATOS DEL ENTREVISTADO:

SEXO _____

EDAD. _____

EDUCACION: _____

PROFESION U OFICIO: _____

SECTOR DONDE TRABAJA: PUBLICO: _____ PRIVADO: _____

PREGUNTAS:

1.- ¿Conoce la legislación penal relacionada con la falsificación de documentos electrónicos?

Sí _____ No _____

2.- ¿Conoce alguna otra norma de carácter civil, administrativo o de reglamentación privada que permita controlar la falsificación de documentos electrónicos?

Sí _____ No _____

Descríbala si la respuesta es si:

_____

_____

_____

3.- ¿En la entidad donde trabaja existe algún tipo de reglamentación especial relacionada con la falsificación de documentos?

Sí _____ No _____

4.- ¿Conoce los tipos de documentos electrónicos sobre los que se puede cometer una falsificación?

Sí _____ No _____

5.- Señale qué tipos de documentos pueden ser falsificados?

_____

_____

_____

6.- Según sus conocimientos o experiencias, quién comete generalmente algún tipo de falsificación (señalar de 1 a 3 en orden de prioridad)

a) A través de los trabajadores de la empresa _____.

b) A través de los mismos usuarios _____.

c) A través de un tercero-particular, no relacionado con la empresa _____

7.- Anote los objetos o documentos sobre los que generalmente se comete algún tipo de falsificación

a) A través del software o programa de la empresa

_____

b) A través del manejo de los programas de redes informáticas en internet, que dan acceso a las cuentas privadas

_____

c) A través de tarjetas bancarias con banda electrónica

_____

d) A través de otros documentos producidos electrónicamente

_____

8.- Mencione un supuesto en el que se puede cometer falsificación de documentos electrónicos (un hecho)

_____

_____

_____

_____

9.- Señale por lo menos dos causas que permiten la falsificación de documentos electrónicos:

a) _____

b) _____

10.- ¿Considera que Panamá debe mejorar su legislación penal relacionada con falsificación de documentos electrónicos?

Sí _____ No _____

¿Por qué?

LEY No. 43
De 31 de julio de 2001

Que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos

LA ASAMBLEA LEGISLATIVA

DECRETA:

Título I

Comercio Electrónico y Documentos Electrónicos en General

Capítulo I

Ámbito de Aplicación

Artículo 1. Regulación La presente Ley regula los documentos y firmas electrónicas y la prestación de servicios de certificación de estas firmas, y el proceso voluntario de acreditación de prestadores de servicios de certificación, para su uso en actos o contratos celebrados por medio de documentos y firmas electrónicas, a través de medios electrónicos de comunicación

Artículo 2. Definiciones Para los efectos de la presente Ley, los siguientes términos se definen así.

1 *Certificado.* Manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas electrónicas o la integridad de un mensaje.

2 *Destinatario* Persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a ese mensaje.

3 *Documento electrónico.* Toda representación electrónica que da testimonio de un hecho, una imagen o una idea

4 *Entidad de certificación* Persona que emite certificados electrónicos en relación con las firmas electrónicas de las personas, ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos y realiza otras funciones relativas a las firmas electrónicas

5 *Firma electrónica* Todo sonido símbolo o proceso electrónico vinculado a o lógicamente asociado con un mensaje, y otorgado o adoptado por una persona con la intención de firmar el mensaje que permite al receptor identificar a su autor

6 *Iniciador* Toda persona que, a tenor del mensaje, haya actuado por sí mismo o en cuyo nombre se haya actuado, para enviar o generar ese mensaje antes de ser archivado si

éste es el caso, pero que no haya actuado a título de intermediario con respecto a ese mensaje

7 *Intermediario* Toda persona que, actuando por cuenta de otra, envíe, reciba o archive un mensaje o preste algún otro servicio con respecto a él

8 *Mensaje de datos* Información generada, enviada, recibida o archivada 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.

9 *Repositorio* Sistema de información utilizado para guardar y recuperar certificados u otro tipo de información relevante para la expedición de éstos

10 *Revocar un certificado* Finalizar definitivamente el periodo de validez de un certificado, desde una fecha específica en adelante.

11 *Sistema de información* Todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

12 *Suscriptor* Persona que contrata con una entidad de certificación la expedición de un certificado, para que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma electrónica

13 *Suspender un certificado.* Interrumpir temporalmente el periodo operacional de un certificado, desde una fecha en adelante.

Artículo 3. Interpretación. Las actividades reguladas por esta Ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional, equivalencia del soporte electrónico al soporte de papel y equivalencia funcional del comercio tradicional con el comercio electrónico. Toda interpretación de los preceptos de esta Ley deberá guardar armonía con los principios señalados.

Artículo 4. Modificación mediante acuerdo Salvo que se disponga otra cosa, en las relaciones entre las partes que generan, envían, reciben, archivan o procesan de alguna u otra forma mensajes de datos, las disposiciones del Capítulo III, Título I, podrán ser modificadas mediante acuerdo Lo dispuesto en este artículo no se aplicará a las disposiciones contenidas en el Capítulo II del Título I de la presente Ley

Artículo 5. Reconocimiento jurídico de los mensajes de datos Se reconocen efectos jurídicos, validez y fuerza obligatoria a todo tipo de información, que este en forma de mensaje de datos o que figure simplemente en el mensaje de datos en forma de remisión

Capítulo II

Aplicacion de los Requisitos Juridicos a los Mensajes de Datos

Artículo 6. Escrito Cuando la ley requiera que la información conste por escrito, los actos y contratos, otorgados o celebrados, por medio de documento electrónico, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito en soporte de papel Dichos actos y contratos se reputaran como escritos, en los casos en que la ley exija que éstos consten por escrito, siempre que se cumplan las condiciones siguientes

1 Que la información que éste contiene sea accesible para su posterior consulta

2 Que el mensaje de datos sea conservado con el formato original en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida.

3. Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, la fecha y la hora en que fue enviado o recibido.

Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito

Lo dispuesto en el presente artículo no será aplicable a.

a. Los actos para los cuales la ley exige una solemnidad que no sea verificable mediante documento electróruco

b. Los actos jurídicos para los que la ley requiera la concurrencia personal de alguna de las partes

c. Los actos jurídicos relativos al Derecho de Familia

Artículo 7. Firma Cuando la ley exija la presencia de una firma o establezca ciertas consecuencias en ausencia de ella, en relación con un documento electrónico o mensaje de datos, se entenderá satisfecho dicho requerimiento si éste ha sido firmado electrónicamente.

La firma electrónica, cualquiera que sea su naturaleza, será equivalente a la firma manuscrita para todos los efectos legales En cuanto a su admisibilidad en juicio y al defecto probatorio de los documentos y firmas electrónicas se aplicará lo dispuesto en la presente Ley Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que no exista una firma

Si una disposición legal requiere que una firma relacionada a un documento electrónico o mensaje de datos o una transacción sea notarizada, reconocida, refrendada o hecha bajo la gravedad del juramento, dicho requisito será satisfecho si la firma electrónica de la persona autorizada para efectuar dichos actos, junto con toda la información requerida bajo la norma legal aplicable, sea vinculada con la firma o mensaje

Lo dispuesto en el presente artículo no será aplicable a

1 Los contratos sobre bienes inmuebles y demas actos susceptibles de registro ubicados en Panamá

2 Los actos en materia de sucesiones que se otorguen bajo ley panameña o que sufran sus efectos en Panamá

3 Los avisos y documentos dirigidos o emitidos por autoridades de Panamá, que no hayan sido autorizados por la entidad respectiva

Artículo 8. Original Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si

1 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

2 De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar

Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no conste 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 documentos, firmas electrónicas y mensajes de datos Los documentos y firmas electrónicas y mensajes de datos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Capítulo III, del Título VII del Libro Segundo de Procedimiento Civil del Código Judicial, de conformidad con lo que dispone la ley

Artículo 11. Criterio para valorar probatoriamente los documentos electrónicos, firmas electrónicas y mensajes de datos Para la valoracion de la fuerza probatoria de los documentos electrónicos, las firmas electrónicas y de los mensajes de datos a que se refiere esta Ley, se tendran en cuenta las reglas de la sana critica y demas criterios reconocidos legalmente para la apreciacion de las pruebas

Por consiguiente, al valorar la fuerza probatoria de un documento electrónico, firma electrónica o mensaje de datos se habrá de tener presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad de la forma en la se haya conservado la integridad de la información y la forma en la que se identifiquen a su iniciador y a cualquiér otro factor pertinente

Artículo 12. Conservación de los mensajes de datos Cuando la ley requiera que ciertos documentos, registros o información sean conservados, ese requisito quedara satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las siguientes condiciones

1 Que la información que contenga sea accesible para su posterior consulta,

2. Que el mensaje de datos sea conservado en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida; y

3. Que se conserve, de haber alguno, todo dato que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido

Si un cambio en la configuración en el sistema de información requerido para consultar un mensaje de datos crea un riesgo material de que el consumidor no pueda acceder a él, el proveedor suministrará al consumidor una declaración de las nuevas configuraciones requeridas, así como la oportunidad de dar por terminado el contrato.

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 y demás documentos electrónicos.

Los libros y documentos del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta Esta obligación estará sujeta a la prescripción de toda acción que pudiera derivarse de ella, según lo establecido en el artículo 93 del Código de Comercio.

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 a través de terceros, siempre que se cumplan las condiciones enunciadas en el artículo anterior, además de que estos datos no contengan información sensible a los intereses del usuario

Capítulo III

Comunicación de los Mensajes de Datos y Documentos Electrónicos

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 Se reconoce validez y fuerza obligatoria a un contrato que para su formacion utilice 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, se reconocen efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración que conste en forma de mensaje de datos o documento electrónico

Artículo 16. Atribución de los mensajes de datos Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por.

1 El propio iniciador;

2 Alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o

3 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, y por lo tanto puede actuar en consecuencia, cuando:

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, con el fin de 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.

Parágrafo. Lo dispuesto en el presente artículo no se aplicará.

a A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia; o

b A partir del momento en que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o haber aplicado algún método convenido, que el mensaje de datos no provenía de éste

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 meusaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algun 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:

1 Toda comunicación del destinatario, automatizada o no; o

2. 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 recibido el acuse de recibo

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, pero aquél no indicó expresamente que los efectos del mensaje de datos están condicionados a la recepción del acuse de recibo y, si no se ha recibido acuse en el plazo fijado o convenido, o no se ha fijado o convenido ningún plazo, en un plazo no mayor de cuarenta y ocho horas a partir del momento del envío o del vencimiento del plazo fijado o convenido, el iniciador:

a Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un nuevo plazo para su recepción, el cual será de cuarenta y ocho horas, contado a partir del momento del envío del nuevo mensaje de datos, y

b De no recibirse acuse de recibo dentro del término señalado conforme al literal anterior, podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener

Artículo 21. Presunción de recepción de un mensaje de datos Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que este 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 recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así

Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo

Artículo 22. 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 el control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

Artículo 23. Tiempo de la recepción de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

1. Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar 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,
3. 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 un lugar distinto de donde se tenga por recibido el mensaje conforme al artículo siguiente.

Artículo 24. 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

1. Si el iniciador o el 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 operacion subyacente, su establecimiento principal,
2. Si el iniciador o el destinatario no tiene establecimiento, se tendrá en cuenta su lugar de residencia habitual

Título II

Firmas y Certificados Electrónicos

Capítulo I

Firmas Electrónicas

Artículo 25. Atributos de la firma electrónica El uso de una firma electrónica 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 electrónica es inválida

Artículo 26. Firma electrónica segura. Es una firma electrónica que puede ser verificada de conformidad con un sistema o procedimiento de seguridad, de acuerdo con estándares reconocidos internacionalmente.

Artículo 27. Mensaje de datos firmado electrónicamente Se entenderá que un mensaje de datos ha sido firmado, si el símbolo o la metodología adoptada por la parte, cumple con un procedimiento de autenticación o seguridad

Capítulo II

Certificados

Artículo 28. Contenido de los certificados. Un certificado emitido por una entidad de certificación, además de estar firmado electrónicamente 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 Nombre, dirección y lugar donde realiza actividades la entidad de certificación

4 Metodología para verificar la firma electrónica del suscriptor impuesta en el mensaje de datos

5 Numero de serie del certificado

6 Fecha de emisión y expiración del certificado

Artículo 29 Expiracion de un certificado Un certificado emitido por una entidad de certificacion expira en la fecha indicada en él

Artículo 30. Aceptación de un certificado Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificacion, a solicitud de éste o de una persona en nombre de éste, lo ha publicado en un repositorio o lo ha enviado a una o mas personas

Artículo 31. Garantía derivada de la aceptación de un certificado El suscriptor, al momento de aceptar un certificado, garantiza a todas las personas de buena fe exentas de culpa, que se soportan en la misma información en él contenida, que

1 La firma electrónica autenticada mediante éste, está bajo su control exclusivo,

2 Ninguna persona ha tenido acceso al procedimiento de generación de la firma electrónica,

3. La información contenida en el certificado es verdadera y corresponde a la suministrada por éste a la entidad de certificación.

Artículo 32. Suspensión y revocación de certificados El suscriptor de una firma certificada podrá solicitar a la entidad de certificación que expidió un certificado, la suspensión o renovación de éste. La revocación o suspensión del certificado se hace efectiva a partir del momento en que se registra por parte de la entidad de certificación Este registro debe hacerse en forma inmediata, una vez recibida la solicitud de suspensión o revocación.

Artículo 33. Causales para la revocación de certificados. El suscriptor de una firma electrónica certificada está obligado a solicitar la revocación del certificado en los siguientes casos·

1. Por pérdida de la información que da validez al certificado

2. Si la privacidad del certificado 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 la pérdida o perjuicio en los cuales incurran terceros de buena fe exentos de culpa, que confiaron en el contenido del certificado

Una entidad de certificación revocará un certificado emitido por las siguientes razones

a Petición del suscriptor o un tercero en su nombre y representación

b Muerte del suscriptor

c. Disolución del suscriptor, en el caso de las personas jurídicas

d. Confirmación de que alguna información o hecho, contenido en el certificado, es falso

e La privacidad de su sistema de seguridad ha sido comprometida de manera material, que afecte la confiabilidad del certificado

f Cese de actividades de la entidad de certificacion

g Orden judicial o de autoridad administrativa competente

Artículo 34. Notificación de la suspensión o revocación de un certificado Una vez registrada la suspensión o revocación de un certificado, la entidad de certificación debe publicar, en forma inmediata, un aviso de suspensión o renovación en todos los repositorios en los cuales la entidad de certificación publicó el certificado También deberá notificar de este hecho a las personas que soliciten información acerca de una firma electrónica verificable, por remisión al certificado suspendido o revocado.

Si los repositorios en los cuales se publicó el certificado no existen al momento de la publicacion del aviso o son desconocidos, la entidad de certificación deberá publicar dicho aviso en un repositorio que designe la Dirección de Comercio Electrónico del Ministerio de Comercio e Industrias.

Artículo 35. Registro de certificados Toda entidad de certificación deberá llevar un registro de los certificados emitidos, que se encuentre a disposición del público, el cual debe indicar las fechas de emisión, expiración y los registros de suspensión, revocación o reactivación de ellos.

Artículo 36. Término de conservación de los registros Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término de quince años, contado a partir de la fecha de revocación o expiración del correspondiente.

Capítulo III

Suscriptores de Firmas Electrónicas

Artículo 37. Deberes de los suscriptores. Son deberes de los suscriptores:

1. Recibir los certificados por parte de la entidad de certificación, utilizando un sistema de seguridad exigido por la entidad de certificación con la que haya contratado sus servicios, o en un esquema de interoperabilidad para aceptar certificados reconocidos por diferentes entidades de certificación.
2. Suministrar información completa, precisa y verídica a la entidad de certificación con la que haya contratado sus servicios.
3 Aceptar los certificados emitidos por la entidad de certificación, demostrando aprobación de sus contenidos mediante el envío de éstos a una o mas personas o solicitando la publicación de éstos en repositorios
4 Mantener el control de la información que da privacidad al certificado y reservarla del conocimiento de terceras personas.
5 Efectuar oportunamente las correspondientes solicitudes de suspensión o revocación

Un suscriptor cesa en la obligación de cumplir con los anteriores deberes, a partir de la certificación de un aviso de revocación del correspondiente certificado por parte de la entidad de certificación

Artículo 38. Solicitud de información Los suscriptores podrán solicitar a la entidad de certificación información sobre todo asunto relacionado con los certificados y las firmas electrónicas

Artículo 39. Responsabilidad de los suscriptores Los suscriptores serán responsables por la falsedad o error en la información suministrada a la entidad de certificación y que es objeto material del contenido del certificado También serán responsables en los casos en los cuales no den oportunamente el aviso de revocación o suspensión de certificados, en los casos indicados anteriormente.

Título III

Autoridad de Registro y Entidades de Certificación

Capítulo I

Autoridad de Registro Voluntario

Artículo 40. La Autoridad. Se crea dentro del Ministerio de Comercio e Industrias, la Dirección de Comercio Electrónico, adscrita a la Dirección Nacional de Comercio, como Autoridad de Registro Voluntario de Prestadores de Servicios de Certificación. La Dirección de Comercio Electrónico establecerá un sistema de acreditación mediante registro voluntario.

Por medio de la presente Ley, la Autoridad queda facultada para acreditar y supervisar a las entidades de certificación, de acuerdo con criterios establecidos en normas internacionales, a fin de garantizar un nivel básico de seguridad y calidad de sus servicios, que son de vital importancia para la confiabilidad de las firmas electrónicas. La expedición de certificados u otros servicios relacionados no estará sujeta a autorización previa.

Para realizar el registro voluntario, se deberá pagar una tasa por este servicio a la Autoridad, cuyo monto y procedimiento de pago será determinado por reglamento. Hasta que no haya sido dictado el reglamento, se establece que la tasa de registro será de mil balboas (B/ 1,000 00)

Entre las funciones de la Autoridad se encuentran las siguientes

1 Registrar a las entidades de certificación que así lo soliciten, conforme a la reglamentación expedida por el Ministerio de Comercio e Industrias

2 Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de toda entidad de certificación, y por el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad

3 Dictar los reglamentos sobre la materia.

4 Revocar o suspender el registro de la entidad de certificación

5. Requerir a las entidades de certificación que suministren información relacionada con los certificados, las firmas electrónicas emitidas y los documentos en soporte informático que custodien o administren, pero únicamente cuando se refieran a los procesos que afecten la seguridad e integridad de datos Esta función no permite el acceso al contenido de los mensajes, a las firmas o a los procesos utilizados, excepto mediante orden judicial

6 Imponer sanciones a las entidades de certificacion por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio.

7 Ordenar la revocación o suspensión de certificados, cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.

8. Designar los repositorios en los eventos previstos en la ley

Las entidades de certificación que no lleven a cabo la acreditación voluntaria, quedarán sujetas a las facultades de inspección de la Autoridad de Registro, para los efectos de velar por el cumplimiento de las obligaciones correspondientes que establece esta Ley o sus reglamentos, así como al cumplimiento de las disposiciones legales sobre la materia.

Una vez presentada toda la documentación establecida para obtener la acreditación, la Autoridad de Registro dispondrá del término de noventa días para emitir criterio. De no efectuar ningún pronunciamiento al respecto, se entenderá que ha emitido criterio favorable y deberá procederse con el registro. Otorgada la acreditación, la entidad de certificación será inscrita en un registro que será de carácter público, que a tal efecto llevará la Autoridad y al cual se podrá tener acceso por medios electrónicos. La entidad de certificación tendrá la obligación de informar a la Autoridad de Registro cualquier modificación de las condiciones que permitieron su acreditación.

Artículo 41. La Contraloría General de la República como entidad certificadora. Para toda la documentación, firmas electrónicas, servicios de certificación, claves de descuentos y otros actos que afecten o puedan afectar fondos o bienes públicos, la entidad certificadora es la Contraloría General de la República

Artículo 42. Infracciones y sanciones Se consideran infracciones las siguientes

1. Incumplimiento de cualquiera de las disposiciones de esta Ley

2 Negligencia en la prestacion del servicio

3 Comisión de delito en la prestación del servicio

La Autoridad de Registro, 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 que incumplan o violen las normas a las cuales debe sujetarse su actividad

a Amonestación

b Multa de cien balboas (B/.100 00) hasta cien mil balboas (B/ 100,000 00).

c Suspensión de inmediato de todas o algunas de las actividades de la entidad infractora

d Prohibición a la entidad de certificación infractora de prestar directa o indirectamente los servicios de la entidad de certificación por el término de hasta cinco años

e Revocación definitiva de la acreditación y prohibición para operar en Panamá como entidad de certificación, cuando la aplicación de las sanciones anteriormente enumeradas, no haya sido efectiva y se pretenda evitar perjuicios reales o potenciales a terceros.

Artículo 43. Recursos Las resoluciones de la Autoridad de Registro 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 Registro y/o de Apelación ante el Ministro de Comercio e Industrias. La Autoridad de Registro tendrá un plazo de dos meses para decidir 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 Comercio e Industrias dispondrá de dos meses para resolver el Recurso de Apelación. Si en tal plazo no ha sido resuelto el Recurso, la decisión se considerará favorable al recurrente.

Capítulo II

Entidades de Certificación

Artículo 44. Naturaleza, características y requerimientos de las entidades de certificación. Podrá ser acreditada como entidad de certificación, toda persona nacional o extranjera, la cual podrá acreditarse de forma voluntaria en la Autoridad de Registro, cumpliendo con los requerimientos establecidos por la ley o sus reglamentos, con base en las siguientes condiciones:

1. Contar con la capacidad económica y financiera suficientes para prestar los servicios autorizados como entidad de certificación

2 Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad

3 Los representantes legales, administradores y personal operativo no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, o que hayan sido suspendidas en el ejercicio de su profesión por faltas graves contra la ética o hayan sido excluidas de aquélla

Artículo 47. Manifestación de práctica de la entidad de certificación Cada entidad de certificación acreditada publicará, en un repositorio de la Autoridad de Registro o en el que ésta designe, una manifestación de práctica de entidad de certificación que contenga la siguiente información.

1 Nombre, dirección y número telefónico de la entidad de certificación

2 Sistema electrónico de la entidad de certificación

3 Resultado de la evaluación obtenida por la entidad de certificación en la última auditoria realizada por la Autoridad del Registro

4 Si la acreditación para operar como entidad de certificación ha sido revocada o suspendida, o si con motivo de la auditoría se ha impuesto alguna sanción. Este registro deberá incluir igualmente la fecha de la revocación o suspensión y los motivos de ésta.

5 Límites para operar la entidad de certificación

6. Cualquier evento que sustancialmente afecte la capacidad de la entidad de certificación para operar.

7. Lista de normas y procedimientos de certificación.

8 Denominación del sistema de seguridad y protección utilizado.

9. Método para la identificación de dicho sistema.

10. Descripción del plan de contingencia que garantice los servicios.

11 Cualquier información que se requiera mediante reglamento.

Artículo 48. Remuneración por la prestación de servicios La remuneración por los servicios de las entidades de certificación será establecida libremente por éstas

Artículo 49. Deberes de las entidades de certificación. Las entidades de certificación tendrán, entre otros, los siguientes deberes:

1 Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

2 Demostrar la fiabilidad necesaria de sus servicios.

3. 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.

4 Emplear personal calificado 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

5 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

certificación no serán responsables de los daños o perjuicios que tengan en su origen el uso indebido o fraudulento de un certificado de firma electrónica por parte del suscriptor.

Los prestadores de servicios deberán disponer de los recursos económicos suficientes para operar, de conformidad con lo dispuesto en esta Ley, 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

Para los efectos de este artículo, los prestadores de servicios de certificación deberán acreditar la contratación y mantenimiento de una garantía que cubra su eventual responsabilidad civil contractual y extracontractual El tipo, monto y procedimiento para consignar esta garantía será fijada mediante reglamento

Artículo 52. Cesación de actividades por parte de las entidades de certificación Las entidades de certificación podrán cesar en el ejercicio de actividades, siempre que hayan notificado a la Autoridad de Registro con cuatro meses de anticipación.

Una vez haya sido notificada la cesación de actividades, la entidad de certificación que cesará de operar, deberá enviar a cada suscriptor un aviso, con no menos de noventa días de anticipación a la fecha de la cesación efectiva de actividades, en el cual solicitará autorización para revocar o publicar en otro repositorio de otra entidad de certificación, los certificados que aún se encuentran pendientes de expiración.

Pasados sesenta días sin obtenerse respuesta por parte del suscriptor, la entidad de certificación podrá revocar los certificados no expirados u ordenar su publicación, dentro de los quince días siguientes, en un repositorio de otra entidad de certificación, en ambos casos, dando aviso de ello al suscriptor.

Si la entidad de certificación no ha efectuado la publicación en los términos del párrafo anterior, la Autoridad ordenará la publicación de los certificados no expirados en los repositorios de la entidad de certificación por ella designada

En el evento de no ser posible la publicación de estos certificados en los repositorios de cualquier entidad de certificación, la Autoridad efectuará la publicación de los certificados no expirados en un repositorio de su propiedad.

Capítulo III

Repositorios

Artículo 53. Reconocimiento y actividades de los repositorios La Autoridad de Registro autorizará únicamente la operación de los repositorios que mantengan las entidades de certificación acreditadas

Los repositorios autorizados para operar deberan

1 Mantener una base de datos de certificados de conformidad con los reglamentos

respectivos.

2 Garantizar que la información que mantienen se conserve íntegra, exacta y razonablemente confiable, de forma que pueda ser recuperada para su ulterior consulta

3. Mantener un registro de las publicaciones de los certificados revocados o suspendidos

Capítulo IV

Disposiciones Varias

Artículo 54. Certificaciones recíprocas Los certificados emitidos por entidades de certificación extranjeras podrán ser reconocidos en los mismos términos y condiciones exigidos en ella para la emisión de certificados por parte de las entidades de certificación nacionales, cuando:

1. Tales certificados sean reconocidos por una entidad de certificación acreditada en Panamá 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
2. Tales certificados sean reconocidos en virtud de acuerdos con otros países, ya sean bilaterales o multilaterales, o efectuados en el marco de organizaciones internacionales de las que Panamá sea parte.
3. Tales certificados sean aceptados en virtud de su validez, de acuerdo con estándares internacionalmente reconocidos y éstos sean emitidos por entidades de certificación, debidamente avalados en su país de origen, por autoridades homólogas a la Autoridad de Registro panameña.

Artículo 55. 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 estos términos están incorporados por remisión a ese mensaje de datos. Entre las partes, y conforme a la ley, estos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

Título IV

Reglamentación y Vigencia

Capítulo I

Disposiciones Varias

Artículo 56. Las entidades de certificación que hayan iniciado la prestación de sus servicios con anterioridad a la entrada en vigencia de la presente Ley, deberán adecuar sus actividades a

lo dispuesto en ella dentro de los seis meses contados a partir de la promulgación del reglamento respectivo

Artículo 57 El Órgano Ejecutivo deberá reglamentar la presente Ley dentro de los seis meses siguientes a su entrada en vigencia, en lo que se refiere al funcionamiento de la Autoridad de Registro y demás aspectos contenidos dentro de la presente Ley El Órgano Ejecutivo realizará consultas con el sector privado para la promulgación de leyes y reglamentos sobre esta materia, así como para hacer recomendaciones y actualizaciones periódicas, con el fin de contemplar innovaciones por avances tecnológicos

Capítulo II

Vigencia

Artículo 58. Vigencia y derogatoria. **La presente Ley entrará a regir desde su promulgación y deroga las normas que le sean contrarias**

COMUNÍQUESE Y CÚMPLASE.

Aprobada en tercer debate, en el Palacio Justo Arosemena, ciudad de Panamá, a los 18 días del mes de junio del año dos mil uno

El Presidente,

Laurentino Cortizo Cohen

El Secretario General Encargado,

Jorge Ricardo Fábrega

ORGANO EJECUTIVO NACIONAL.- PRESIDENCIA DE LA REPUBLICA.-PANAMA, REPUBLICA DE PANAMA, 31 DE julio DE 2001

MIREYA MOSCOSO
Presidenta de la República

JOAQUIN E. JACOME D.
Ministro de Comercio e Industrias

Sentencia C-662/00

LIBERTAD INFORMATICA-Intercambio electrónico de informaciones/**MEDIOS DE COMUNICACION**-Modernización/**ACCESO A LA INFORMACION**-Escrita y mensaje de datos

DERECHO A LA INFORMACION-Transacciones comerciales telemáticas

Los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley.

PRESTACION DE SERVICIOS PUBLICOS-Entidades de certificación

CERTIFICACION TECNICA-Transacciones comerciales por vía informática y mensaje de datos

El servicio de certificación a cargo de las entidades certificadoras propende por proporcionar seguridad jurídica a las transacciones comerciales por vía informática, actuando la entidad de certificación como tercero de absoluta confianza, para lo cual la ley le atribuye importantes prerrogativas de certificación técnica. La certificación técnica busca dar certeza a las partes que utilizan medios tecnológicos para el intercambio de información, en cuanto a la identidad y origen de los mensajes intercambiados. No busca dar mayor jerarquía ni validez a los mensajes de datos de los que pretende un documento tradicional.

AUTENTICIDAD DE LA INFORMACION-Función de entidades de certificación

Las entidades de certificación certifican técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, a saber la confidencialidad, la autenticidad, la integridad y la no

repudiación de la información, lo que, en últimas permite inequívocamente tenerlo como auténtico.

FUNCION NOTARIAL-Regulación por el legislador

FUNCIONES PUBLICAS POR PARTICULARES-Servicio de certificación

RESERVA DE LEY ESTATUTARIA EN MATERIA DE JUSTICIA-Sentido restrictivo

No es necesario un análisis detallado acerca de la naturaleza jurídica de las leyes estatutarias y de las materias a ellas asignadas por el artículo 152 constitucional, pues ya la Corte se ha ocupado con suficiencia del tema y ha establecido que únicamente aquellas disposiciones que de una forma y otra se ocupen de afectar la estructura de la administración de justicia, o de sentar principios sustanciales o generales sobre la materia, deben observar los requerimientos especiales para este tipo de leyes. Las demás y en particular los códigos, deben seguir el trámite ordinario previsto en la Carta Política, pues se tratan de leyes ordinarias dictadas por el Congreso de la República en virtud de lo dispuesto en el numeral 2 del artículo 150 Superior. La reserva de Ley estatutaria no significa que toda regulación que se relacione con los temas previstos en el artículo 152 de la Carta Constitucional deba someterse a dicho trámite especial.

ADMINISTRACION DE JUSTICIA-No todos los aspectos deben ser regulados por ley estatutaria/**CODIGO**-Expedición

La Carta autoriza al Congreso a expedir, por la vía ordinaria, Códigos en todos los ramos de la legislación, por lo cual, mal puede sostenerse que toda regulación de los temas que han sido objeto de ley estatutaria, haga forzoso el procedimiento restrictivo y más exigente previsto por el Constituyente para su formación. El propósito de las Leyes Estatutarias no es el de regular en forma exhaustiva la materia que constituye su objeto.

UNIDAD NORMATIVA-Aplicación/**VALOR PROBATORIO DE MENSAJES ELECTRONICOS**

Referencia: expediente D-2693

Acción pública de inconstitucionalidad contra la Ley 527 de 1999 y, particularmente sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45, "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".

Actora: Olga Lucia Toro Perez

Temas:

El reconocimiento jurídico de la validez plena y del valor probatorio de los mensajes de datos

El Comercio Electrónico

La firma digital

Las entidades de certificación y la emisión de certificados sobre la autenticidad de los mensajes de datos y las firmas digitales

La actividad de las entidades de certificación y la función notarial

Magistrado Ponente:

Dr. FABIO MORóN DíAZ

Santafé de Bogotá, D.C., junio ocho (8) del año dos mil (2000).

La Sala Plena de la Corte Constitucional, en cumplimiento de sus atribuciones constitucionales y de los requisitos y trámites establecidos en el Decreto 2067 de 1991, ha proferido la siguiente

SENTENCIA

En el proceso instaurado por OLGA LUCIA TORO PEREZ, en ejercicio de la acción pública de inconstitucionalidad, en contra de la Ley 527 de 1999 y, especialmente de los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la 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".

I. ANTECEDENTES

La ciudadana **OLGA LUCIA TORO PEREZ,** en ejercicio de la acción pública de inconstitucionalidad consagrada en la Constitución Política de 1991, pide a la Corte declarar inexequibles los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999.

El Magistrado Sustanciador mediante auto de noviembre diecinueve (19) del pasado año, admitió la demanda al haberse satisfecho los requisitos establecidos en el Decreto 2067 de 1991.

Dispuso, asimismo, el traslado al Señor Procurador General de la Nación, para efectos de obtener el concepto de su competencia, al tiempo que ordenó comunicar la iniciación del proceso al Señor Presidente de la República y a los señores Ministros de Desarrollo Económico, Comercio Exterior, Comunicaciones y Transporte, así como al Superintendente de Industria y Comercio.

Cumplidos los trámites constitucionales y legales propios de los procesos de inconstitucionalidad, la Corte Constitucional procede a decidir acerca de la demanda de la referencia.

II. EL TEXTO DE LA LEY ACUSADA

En el texto de la Ley 527 de 1999 se destaca en negrillas los artículos acusados parcialmente:

"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 1º. 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 2º. Definiciones. Para los efectos de la presente ley se entenderá por:

*a) **Mensaje de datos**. La información generada, enviada, recibida, almacenada 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 3º. 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 4º. Modificación mediante acuerdo. Salvo que se disponga otra cosa, en las relaciones entré 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 5º. 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 6º. 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 7º. 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 8º. 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 9º. 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 dato.

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 3º 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. Esta 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.
9. 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.

...

III.LA DEMANDA

La demandante dice cuestionar el texto íntegro de la Ley 527 de 1999 y, en especial, sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999, por estimar que violan el artículo 131 de la Carta Política, así como los artículos 152 y 153.

La transgresión del artículo 131 Constitucional en su criterio, se produce, en cuanto las normas acusadas crean unas entidades de certificación las que, de conformidad con la misma Ley 527 de 1999, están facultadas para emitir certificados en relación con las firmas

digitales de las personas y para ofrecer los servicios de registro y estampado cronológico, la de certificación de la transmisión y recepción de mensajes de datos, así como cualquier otra de autenticación de firmas relativas a las comunicaciones basadas en firmas digitales, a emitir certificados en relación con la veracidad de firmas digitales de personas naturales o jurídicas y, en fin, a realizar actos que son propios de la función fedal, la que, según el entendimiento que da a la norma constitucional antes citada, es del resorte exclusivo de los Notarios, únicos depositarios de la fé pública.

En su criterio, "*lo que no permite la Constitución Política es que la autenticidad del documento privado sea función que pueda ejercer cualquier persona, por cuanto esta es una función propia del servicio público notarial y solo le puede corresponder al Notario, el cual siempre tiene que ser una persona natural, que llegue a serlo en propiedad o por concurso.*"

"*.. si la ley le asigna la función fedante a personas diferentes de los Notarios, infringiría en forma directa lo establecido en el artículo 131 de la Carta y esto es, precisamente lo que ha hecho la ley acusada, en especial en los artículos antes citados 2, 10, 11, 12, 13, 14, 15, 26, 27, 28, 29, 30 32, 34, 35, 36, 37, 38, 39, 40 41, 42, 43 y 45 de la Ley 527 en comento.*

De otra parte, argumenta que se incurrió en violación de los artículos 152 y 153 de la Carta Política, en cuanto sin respetar la reserva de Ley Estatutaria ni el trámite especial, en especial, los artículos 9, 10, 11, 12, 13, 14, 15 y 28 de la Ley 527 de 1999 modificaron y adicionaron el Código de Procedimiento Civil, que en su entendimiento es equivalente a la administración de justicia, al conferir a los mensajes de datos la fuerza probatoria de que tratan las disposiciones del Capítulo VIII del Título XIII, Sección Tercera del Libro Segundo del Código de Procedimiento Civil (i); ordenar que en toda actuación jurídica se dé eficacia, validez y fuerza obligatoria y probatoria a todo tipo de información emitida en forma de mensaje de datos (ii); y, finalmente, al disponer que los jueces deben aplicar a los mensajes de datos las reglas de la sana crítica al apreciarlos como prueba (iii)".

I. INTERVENCIONES CIUDADANAS Y DE AUTORIDADES PUBLICAS

En defensa de la constitucionalidad de la Ley 527 de 1999 durante el término legal intervinieron, de manera conjunta, los ciudadanos Carolina

Deyanira Urrego Moreno, Edgar Iván León Robayo, Jair Fernando Imbachí Cerón; los ciudadanos Carolina Pardo Cuéllar y Santiago Jaramillo Caro; el doctor Ramón Francisco Cárdenas, en representación de la Superintendencia de Industria y Comercio; los doctores María Clara Gutiérrez Gómez en representación del Ministerio de Comercio Exterior y José Camilo Guzmán Santos, como apoderado del Ministerio de Justicia; el doctor Carlos Blas Buraglia Gómez, en su condición de Presidente Ejecutivo (e) de la Cámara de Comercio de Bogotá; el doctor Carlos César Rolón Bermúdez, en representación del Ministerio de Comunicaciones; los ciudadanos Eleonora Cuéllar Pineda y Sergio Pablo Michelsen Jaramillo, en representación de la Fundación Foro Alta Tecnología; y, el doctor Carlos Eduardo Serna Barbosa en representación del Ministerio de Desarrollo Económico.

Puesto que en su gran mayoría, los argumentos en que los intervinientes apoyan su defensa son coincidentes, su resumen se hará en forma unificada, en aras de la brevedad y para evitar repeticiones innecesarias. Son ellos, en síntesis, los que siguen:

- El examen de constitucionalidad de la Ley debe tener en cuenta la trascendencia que el comercio electrónico tiene en la globalización de las relaciones económicas, el impacto de su evolución, las consecuencias que genera en el desarrollo de los actos y negocios jurídicos celebrados, no solamente por los particulares, sino también por el mismo Estado, así como la importancia de regular y reglamentar jurídicamente su utilización

- La Ley 527 de 1999 sigue los lineamientos del proyecto tipo de Ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional - CNUDMI.

- En el caso Colombiano fué el producto de un proceso en el que participaron los sectores público y privado que tuvieron asiento en la Comisión Redactora de la que formaron también parte los Ministros de Justicia y del Derecho, Transporte, Desarrollo Económico y Comercio Exterior.

- El Comercio Electrónico encierra dentro de su filosofía los postulados de la buena fe comercial y de la libertad contractual entre los negociantes, principios éstos que rigen todas y cada una de las transacciones realizadas mediante su utilización.

La regulación del Comercio Electrónico busca permitir el acceso de todas las personas a esta forma tecnológica de realizar transacciones de índole comercial y contractual.

- Ni el comercio electrónico ni la actividad de las entidades de certificación son un servicio público, pues las partes no se encuentran en la obligación ni en la necesidad de solicitar los servicios de una entidad de certificación para la celebración de un negocio jurídico. Por el tipo de relaciones que regula, se trata de un asunto de la órbita del Derecho Privado que, por supuesto, precisa de un control estatal, que estará a cargo de la Superintendencia de Industria y Comercio, que vigila a las entidades de certificación desde el punto de vista técnico y operativo.
- La Ley cuestionada apunta a proveer tanto a los mensajes de datos como al comercio electrónico de la integridad, confiabilidad y la seguridad que en este tipo de intercambios electrónicos son cruciales, comoquiera que se trata de operaciones y de transacciones en que las partes interactúan electrónicamente, a través de redes telemáticas, sin haber contacto directo o físico.
- Las firmas digitales, el certificado electrónico, y el servicio de certificación que prestan las entidades de certificación son herramientas de índole eminentemente técnica que apuntan a dotar de seguridad los mensajes de datos y el comercio electrónico.
- Los cargos de la demanda resultan infundados porque las entidades de certificación no prestan un servicio público y menos dan fé pública. Las entidades de certificación no son notarías electrónicas, pues no sustituyen ni prestan los mismos servicios, según se deduce de la sola lectura del artículo 30 de la Ley 527 de 1999 que relaciona las actividades que las primeras pueden realizar.
- La actividad de certificación es un servicio de índole eminentemente técnico que tiene que ver con la confianza y la credibilidad, y que propende por la seguridad en los mensajes de datos empleados para realizar un cierto acto o negocio y en el comercio electrónico, la cual básicamente comprende: la inobjetabilidad de origen; la integridad de contenido, la integridad de secuencia, la inobjetabilidad de recepción, la confidencialidad, la unicidad de fin y la temporalidad. Ello se logra a través de una entidad reconocida por un grupo de usuarios, quien certifica sobre el iniciador en quien se originó la información, que su contenido no ha sufrido alteraciones ni modificaciones y que fue recibida por su destinatario

- Ni la Constitución ni las leyes han establecido que las funciones públicas o los servicios públicos sólo puedan ser prestados por entidades o servidores públicos. Todo lo contrario: de acuerdo con los artículos 2°., 210 y 365 de la Carta Política, el Estado, para el debido cumplimiento de sus fines, tiene la facultad de asignar, delegar o conferir transitoriamente ciertas y precisas responsabilidades públicas a los particulares.
- De ahí que, si las funciones de las entidades certificadoras de que trata la Ley 527/99 fueran eventualmente calificadas como relacionadas con la fe pública, ello en momento alguno significa que el legislador dentro de su competencia no pueda atribuírselas a dichas entidades en su condición de entes privados, tal como lo ha hecho la ley con los notarios respecto de las funciones a ellos asignadas.
- Si en gracia de discusión, la actividad de las entidades de certificación se catalogase como servicio público, se trataría de uno diferente del que prestan las Notarías, y en todo caso su constitucionalidad estaría amparada por el artículo 365 de la Carta Política.

Por lo tanto, si ahora, debido a los desarrollos tecnológicos, el legislador consideró necesario para garantizar la protección del derecho fundamental de los particulares a obtener información veraz, consagrado en el artículo 20 de la Carta, otorgar facultades relacionadas con la guarda de la fe pública a entidades certificadoras, desde una perspectiva diferente a la de los notarios, no quiere decir que el legislador esté contraviniendo el artículo 131 de la Carta Política.

- Si bien puede ser cierto que la referida ley efectivamente modificó algunas disposiciones contenidas en códigos, dichas modificaciones en momento alguno pueden siquiera llegar a considerarse que afectan la estructura general de la administración de justicia o los principios sustanciales y procesales sobre la materia, por lo cual, mal podría sostenerse que han debido ser objeto de una ley estatutaria, cuando su materia es propia de la ley ordinaria, la que, como tal, cuenta con la facultad suficiente para modificar normas anteriores de igual o inferior jerarquía, incluyendo naturalmente las contenidas en los códigos.
- La Ley 527 de 1999 no modifica ni deroga una ley estatutaria y su tema no forma parte de la reserva atribuida a estas leyes, razón por la cual su trámite y aprobación no debía sujetarse a la mayoría absoluta de los miembros del Congreso, siendo procedente que su contenido fuera regulado a través de una ley ordinaria.

Por lo tanto, es igualmente infundado el cargo de violación de los artículos 152 y 153 aunque la Ley 527 de 1999 haya modificado el Código de Procedimiento Civil, de ello no se sigue que su contenido sea el propio de la Ley Estatutaria sobre la Administración de Justicia.

En abundante jurisprudencia, esta Corte ha sostenido que no toda reforma procedimental puede entenderse como un cambio a la estructura misma de la Administración de Justicia. Sólo un cambio en su estructura o en sus principios sustanciales y procesales, deben ser regulados a través de legislación estatutaria. Por el contrario, las modificaciones procesales que no toquen estos principios, son del resorte de la ley ordinaria.

V.CONCEPTO DEL PROCURADOR GENERAL DE LA NACION

El señor Procurador General de la Nación, rindió en tiempo el concepto de su competencia, en el cual solicita declarar constitucional la Ley acusada.

Acerca de la presunta vulneración del artículo 131 constitucional por parte de los artículos 28, 29, 30 y 32 de la ley 527 de 1999, el Jefe del Ministerio Público considera que esta alegación se funda en una particular interpretación según la cual el artículo 131 de la Constitución Política, habría encargado de manera exclusiva a los notarios el servicio público de otorgar la fe pública.

El señor Procurador General señala que no comparte esa interpretación pues, en su parecer, el artículo 131 de la Carta no consagra ni explícita ni implícitamente la pretendida exclusividad, ya que se limita a señalar que compete a la ley la reglamentación del servicio público que prestan los notarios y registradores, además de la definición del régimen laboral de sus empleados y lo relativo a los aportes como tributación especial de las notarías, con destino a la administración de justicia.

Observa que el resto del contenido del artículo 131 Constitucional se refiere a la constitucionalización de la carrera notarial y la facultad gubernamental de crear los Círculos de notariado y registro y de determinar el número de notarios y oficinas de registro, sin que, en parte alguna de dicho artículo se prevea que la función de otorgar la fe pública sea de competencia exclusiva de los notarios.

Es probable que la confusión de la demandante provenga de identificar la prestación del servicio público de notariado con la actividad de dar fe de determinados actos o contratos o de certificar la autenticidad de las firmas con la que tales actos se suscriben, pero aun siendo esto cierto, no

podría deducirse que el Constituyente haya establecido que la actividad fedante sea privativa de los notarios. Es más, no existe referencia alguna, ni siquiera indirecta, en el artículo 131, a qué personas son las competentes para otorgar la fe pública.

Acerca de la presunta violación de los artículos 151 y 152 de la Carta Política, ese Despacho considera infundado el argumento de inconstitucionalidad según el cual la Ley 527 de 1999, debió haberse sometido a los trámites propios de una ley estatutaria, habida cuenta de que algunas de sus normas están relacionadas con la administración de justicia, al preverse en ellas asuntos relacionados con el procedimiento civil.

Recuerda que esta Corte ha sentado el criterio de acuerdo con el cual la exigencia constitucional de la reserva de la ley estatutaria, en el caso de las normas legales que se refieran a la administración de justicia, procede cuando la norma legal trate asuntos concernientes a derechos fundamentales de las personas o a la estructura misma de dicha administración, que no son precisamente los tratados por las normas aquí cuestionadas.

Corrobora que, de acuerdo a la jurisprudencia constitucional, no es exigible esa modalidad de legislación, por la sola circunstancia de que una determinada ley haga referencia a algunos de los temas respecto de los cuales el Constituyente previó el trámite especial contenido en el artículo 152 de la Carta.

VI. CONSIDERACIONES Y FUNDAMENTOS

1. La Competencia.

En virtud de lo dispuesto por el artículo 241-4 de la Carta Política, la Corte Constitucional es competente para decidir definitivamente sobre la demanda de inconstitucionalidad que dio lugar al presente proceso, dado que versa sobre presuntos vicios atribuidos a una Ley de la República.

2. El contexto de la Ley 527 de 1999

2.1.La revolución en los medios de comunicación de las dos últimas décadas a causa de los progresos tecnológicos en el campo de los computadores, las telecomunicaciones y la informática

Es bien sabido que los progresos e innovaciones tecnológicas logrados principalmente durante las dos últimas décadas del siglo XX, en el campo de la tecnología de los ordenadores, telecomunicaciones y de los programas informáticos, revolucionaron las comunicaciones gracias al surgimiento de redes de comunicaciones informáticas, las cuales han

puesto a disposición de la humanidad, nuevos medios de intercambio y de comunicación de información como el correo electrónico, y de realización de operaciones comerciales a través del comercio electrónico.

El Vicepresidente Ejecutivo (e) de la Cámara de Comercio de Bogotá, se refirió a los avances tecnológicos que ambientaron la regulación sobre mensajes de datos y comercio electrónico así como a su incalculable valor agregado en la expansión del comercio, en los siguientes términos:

"...

La posibilidad de transmitir digitalmente la información de manera descentralizada, el desarrollo de Internet a finales de los años sesenta y el perfeccionamiento de sus servicios desde la aparición de la Red de Redes en los años ochenta, se constituyeron en los pilares básicos para el despegue del comercio electrónico.

En la actualidad el desarrollo del comercio electrónico a nivel mundial es un hecho innegable e irreversible. No sólo es así, sino que según se prevé, seguirá en crecimiento en los próximos años generando grandes ingresos a través de la red, el cual innegablemente causa un impacto sobre las actividades económicas, sociales y jurídicas en donde estas tienen lugar.

A pesar de no haber madurado aún, el comercio electrónico crece a gran velocidad e incorpora nuevos logros dentro del ciclo de producción. A nivel general, todo parece indicar que este nuevo medio de intercambio de información, al eliminar barreras y permitir un contacto en tiempo real entre consumidores y vendedores, producirá mayor eficiencia en el ciclo de producción aparejado a un sin número de beneficios como la reducción de costos, eliminación de intermediarios en la cadena de comercialización, etc. Trayendo importantes e invaluables beneficios a los empresarios que estén dotados de estas herramientas.

En Colombia, las ventas por Internet son una realidad. Los centros comerciales virtuales y las transferencias electrónicas, entre otros, ya pueden encontrarse en la red. En 1995 existían en nuestro país 50.000 usuarios de Internet, hoy, según estudios especializados, llegar a los 600.000 y en el año 2.000 sobrepasarán el millón de suscriptores. Así las cosas Colombia se perfila como uno de los países de mayor crecimiento en América Latina en utilización de recursos informáticos y tecnológicos para tener acceso a Internet y podría utilizar estos

recursos para competir activa y efectivamente en el comercio internacional.

..."

2.2.La necesidad de actualizar los regímenes jurídicos, para otorgar fundamento jurídico al intercambio electrónico de datos

Desde luego, este cambio tecnológico ha planteado retos de actualización a los regímenes jurídicos nacionales e internacionales, de modo que puedan eficazmente responder a las exigencias planteadas por la creciente globalización de los asuntos pues, es indudable que los avances tecnológicos en materia de intercambio electrónico de datos ha propiciado el desarrollo de esta tendencia en todos los órdenes, lo cual, desde luego, implica hacer las adecuaciones en los regímenes que sean necesarias para que estén acordes con las transformaciones que han tenido lugar en la organización social, económica y empresarial, a nivel mundial, regional, local, nacional, social y aún personal.

La exposición de motivoGaceta del Congreso No. 44, viernes 24 de abril de 1998, pp. 26 ss. del proyecto presentado al Congreso de la República por los Ministros de Justicia y del Derecho, de Desarrollo, de Comercio Exterior y de Transporte, que culminó en la expedición de la Ley 527 de 1999, ilustró las exigencias que el cambio tecnológico planteaba en términos de la actualización de la legislación nacional para ponerla a tono con las nuevas realidades de comunicación e interacción imperantes y para darle fundamento jurídico a las transacciones comerciales efectuadas por medios electrónicos y fuerza probatoria a los mensajes de datos, en los siguientes términos :

"...

El desarrollo tecnológico que se viene logrando en los países industrializados, permite agilizar y hacer mucho más operante la prestación de los servicios y el intercambio de bienes tangibles o intangibles, lo cual hace importante que nuestro país incorpore dentro de su estructura legal, normas que faciliten las condiciones para acceder a canales eficientes de derecho mercantil internacional, en virtud a los obstáculos que para éste encarna una deficiente y obsoleta regulación al respecto

"

2.3.La Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil Internacional -CNUDMComisión de las Naciones Unidas para el

desarrollo del Derecho Mercantil Internacional; en inglés UNCITRAL.

Como quedó expuesto, las regulaciones jurídicas tanto nacionales como internacionales resultaron insuficientes e inadecuadas frente a los modernos tipos de negociación y de comunicación.

Ante esa realidad, la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil promovió la gestación de un proyecto de ley tipo en materia de comercio electrónico, inspirada en la convicción de que al dotársele de fundamentación y respaldo jurídicos, se estimularía el uso de los mensajes de datos y del correo electrónico para el comercio, al hacerlos confiables y seguros, lo cual, de contera, redundaría en la expansión del comercio internacional, dadas las enormes ventajas comparativas que gracias a su rapidez, estos medios ofrecen en las relaciones de índole comercial entre comerciantes y usuarios de bienes y servicios.

La Asamblea General de la ONU, mediante Resolución 51/162 de 1996 aprobó la Ley Modelo sobre Comercio Electrónico elaborada por la CNUDMI y recomendó su incorporación a los ordenamientos internos como un instrumento útil para agilizar las relaciones jurídicas entre particulares.

El régimen legal modelo formulado por la Comisión de Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional -CNUDMI- busca ofrecer:

"...

al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitieran eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permitiera un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de comercio electrónico.".

"...

La ley modelo tiene la finalidad de servir de referencia a los países en la evaluación y modernización de ciertos aspectos de sus leyes y prácticas en las comunicaciones con medios computarizados y otras técnicas modernas y en la promulgación de la legislación pertinente cuando no exista legislación de este tipoExposición de motivos, Supra.

"

Según se hizo constar en la propia exposición de motivos, el proyecto colombiano se basó en la Ley modelo de la Comisión de las Naciones

Unidas para el desarrollo del Derecho Mercantil Internacional - CNUDMI- sobre Comercio Electrónico.

2.4.Los antecedentes de la Ley 527 de 1999

La Ley 527 de 1999 es, pues, el resultado de una ardua labor de estudio de temas de derecho mercantil internacional en el seno de una Comisión Redactora de la que formaron parte tanto el sector privado como el público bajo cuyo liderazgo se gestó -a iniciativa del Ministerio de Justicia y con la participación de los Ministerios de Comercio Exterior, Transporte y Desarrollo.

Como ya quedó expuesto, obedeció a la necesidad de que existiese en la legislación colombiana un régimen jurídico consonante con las nuevas realidades en que se desarrollan las comunicaciones y el comercio, de modo que las herramientas jurídicas y técnicas dieran un fundamento sólido y seguro a las relaciones y transacciones que se llevan a cabo por vía electrónica y telemática, al hacer confiable, seguro y válido el intercambio electrónico de informaciones.

Así, pues, gracias a la Ley 527 de 1999 Colombia se pone a tono con las modernas tendencias del derecho internacional privado, una de cuyas principales manifestaciones ha sido la adopción de legislaciones que llenen los vacíos normativos que dificultan el uso de los medios de comunicación modernos, pues, ciertamente la falta de un régimen específico que avale y regule el intercambio electrónico de informacionellamado por sus siglas en inglés "EDI" y otros medios conexos de comunicación de datos, origina incertidumbre y dudas sobre la validez jurídica de la información cuyo soporte es informático, a diferencia del soporte documental que es el tradicional.

De ahí que la Ley facilite el uso del EDI y de medios conexos de comunicación de datos y concede igual trato a los usuarios de documentación con soporte de papel y a los usuarios de información con soporte informático.

3.Estructura de la Ley 527 de 1999

La Ley 527 de 1999 contiene 47 artículos, distribuidos en cuatro Partes, a saber: Mensajes de datos y comercio electrónico (i); Transporte de mercancías (ii); firmas digitales, certificados y entidades de certificación (iii) reglamentación y vigencia.

Del texto de la Ley y para los efectos de este fallo, resulta pertinente destacar cuatro temas: - Mensajes electrónicos de datos y Comercio electrónico; - Las firmas digitales; - Las entidades de certificación y, -

La admisibilidad y fuerza probatoria de los mensajes de datos. Dado su carácter eminentemente técnico, con apartes de la exposición de motivos, se ilustra cada uno de estos temas:

3. 1. Mensajes electrónicos de datos

El mensaje electrónico de datos, se considera la piedra angular de las transacciones comerciales telemáticas.

Por ello la ley lo describe en la siguiente forma:

"**Mensaje de datos**: *la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax*". (Artículo 2º literal b).

La noción de "mensaje" comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación modernas, bajo la configuración de los progresos técnicos que tengan contenido jurídico.

Cuando en la definición de mensaje de datos, se menciona los "medios similares", se busca establecer el hecho de que la norma no está exclusivamente destinada a conducir las prácticas modernas de comunicación, sino que pretenden ser útil para involucrar todos los adelantos tecnológicos que se generen en un futuro.

El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.

Dentro de las características esenciales del mensaje de datos encontramos que es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse; es un documento legible que puede ser presentado ante las Entidades públicas y los Tribunales; admite su almacenamiento e inalterabilidad en el tiempo; facilita la revisión y posterior auditoría para los fines contables, impositivos y reglamentarios; afirma derechos y obligaciones jurídicas entre los intervinientes y es accesible para su ulterior consulta, es decir, que la información en forma de datos computarizados es susceptible de leerse e interpretarse.

Por otra parte, en el proyecto de ley se hace hincapié como condición de singular trascendencia, en la integridad de la información para su originalidad y establece reglas que deberán tenerse en cuenta al apreciar esa integridad, en otras palabras que los mensajes no sean alterados y

esta condición la satisfacen los sistemas de protección de la información, como la Criptografía y las firmas digitales, al igual que la actividad de las Entidades de Certificación, encargadas de proteger la información en diversas etapas de la transacción, dentro del marco de la autonomía de la voluntad.

Así mismo, cuando el contenido de un mensaje de datos sea completo y esté alterado, pero exista algún anexo inserto, éste no afectará su condición de "original". Esas condiciones se considerarían escritos complementarios o serían asimiladas al sobre utilizado para enviar ese documento "original".

- Equivalentes funcionales

El proyecto de ley, al igual de la Ley Modelo, sigue el criterio de los "equivalentes funcionales" que se fundamenta en un análisis de los propósitos y funciones de la exigencia tradicional del documento sobre papel, para determinar cómo podrían cumplirse esos propósitos y funciones con técnicas electrónicas.

Se adoptó el criterio flexible de "equivalente funcional", que tuviera en cuenta los requisitos de forma fiabilidad, inalterabilidad y rastreabilidad, que son aplicables a la documentación consignada sobre papel, ya que los mensajes de datos por su naturaleza, no equivalen en estricto sentido a un documento consignado en papel.

En conclusión, los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley.

3.2.Firmas digitales

En el capítulo I de la parte III, respecto de la aplicación específica de los requisitos jurídicos de los mensajes de datos, se encuentra la firma, y para efectos de su aplicación se entiende por firma digital.

".... un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido vinculado a la clave criptográfica privada del iniciado, permite determinar que este valor numérico se ha obtenido exclusivamente con la clave criptográfica privada del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación" (Artículo 2° Literal h).

A través de la firma digital se pretende garantizar que un mensaje de datos determinado proceda de una persona determinada; que ese mensaje no hubiera sido modificado desde su creación y transmisión y que el receptor no pudiera modificar el mensaje recibido.
Una de las formas para dar seguridad a la validez en la creación y verificación de una firma digital es la Criptografía, la cual es una rama de las matemáticas aplicadas que se ocupa de transformar, mediante un procedimiento sencillo, mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.
Mediante el uso de un equipo físico especial, los operadores crean un par de códigos matemáticos, a saber: una clave secreta o privada, conocida únicamente por su autor, y una clave pública, conocida como del público. La firma digital es el resultado de la combinación de un código matemático creado por el iniciador para garantizar la singularidad de un mensaje en particular, que separa el mensaje de la firma digital y la integridad del mismo con la identidad de su autor.
La firma digital debe cumplir idénticas funciones que una firma en las comunicaciones consignadas en papel. En tal virtud, se toman en consideración las siguientes funciones de esta:

- Identificar a una persona como el autor;

- Dar certeza de la participación exclusiva de esa persona en el acto de firmar;
- Asociar a esa persona con el contenido del documento.

Concluyendo, es evidente que la transposición mecánica de una firma autógrafa realizada sobre papel y replicada por el ordenador a un documento informático no es suficiente para garantizar los resultados tradicionalmente asegurados por la firma autógrafa, por lo que se crea la necesidad de que existan establecimientos que certifiquen la validez de esas firmas.
Por lo tanto, quien realiza la verificación debe tener acceso a la clave pública y adquirir la seguridad que el mensaje de datos que viene encriptado corresponde a la clave principal del firmante; son las llamadas entidades de certificación que trataremos más adelante.

3.3.Entidades de certificación.

Uno de los aspectos importantes de este proyecto, es la posibilidad de que un ente público o privado con poderes de certificar, proporcione la seguridad jurídica a las relaciones comerciales por vía informática Estos entes son las entidades de certificación, que una vez autorizadas, están

facultados para: emitir certificados en relación con claves criptográficas de todas 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.

La entidad de certificación, expide actos denominados Certificados, los cuales son manifestaciones hechas como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las claves criptográficas y la integridad de un mensaje de datos.

La naturaleza de la función de las entidades de certificación se considera como la prestación de un servicio público, para lo cual vale la pena detenerse un momento.

El artículo 365 de la Constitución Política hace referencia al tema de los servicios públicos, los cuales pueden ser prestados tanto por las entidades públicas como las privadas o conjuntamente. Esta norma permite que este servicio lo presten los particulares, si reúnen los requisitos exigidos por la ley y cuenta con la aprobación de la Superintendencia, organismo rector para todos los efectos.

El proyecto de ley señala que podrán ser entidades de certificación, las Cámaras de Comercio y en general las personas jurídicas, tanto públicas como privadas, autorizadas por la Superintendencia respectiva, que cumplan con los requerimientos y condiciones establecidos por el Gobierno Nacional, con fundamento en el artículo 31 del proyecto.

Una vez las entidades de certificación sean autorizadas, podrán realizar actividades tales como, emitir certificados en relación con las firmas digitales; ofrecer o facilitar los servicios de creación de firmas digitales certificadas; servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos; servicios de archivo y conservación de mensajes de datos, entre otras.

A la par con las actividades definidas anteriormente, estas entidades tendrán deberes que cumplir frente a los involucrados dentro del proceso mercantil, deberes atinentes a cada una de las actividades que pretendan ejercer.

En consecuencia, las entidades de certificación, son las encargadas entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto grado de confiabilidad, lo que las hace importantes y

merecedoras de un control ejercido por un ente público, control que redunda en beneficio de la seguridad jurídica del comercio electrónico.
La comisión redactora del proyecto de ley, consideró que la Superintendencia de Industria y Comercio debe ser la entidad encargada del control y vigilancia de las entidades de certificación, por cuanto su competencia es afín con estas labores.
La función que actualmente ejercen las Superintendencias y que les fue delegada, le corresponde constitucionalmente al Presidente de la República como Suprema Autoridad Administrativa, cuando señala que una de sus funciones es la de ejercer la inspección y vigilancia de la prestación de los servicios públicos.
En razón a que la naturaleza de las funciones de las entidades de certificación se consideran como la prestación de un servicio público, la inspección y vigilancia de los servicios públicos que tienen que ver con la certificación, actividades que ejercerán las entidades de certificación, debe radicarse en cabeza de una Superintendencia como la de Industria y Comercio.

3. 4. Alcance probatorio de los mensajes de datos

El proyecto de ley establece que los mensajes de datos se deben considerar como medios de prueba, equiparando los mensajes de datos a los otros medios de prueba originalmente escritos en papel. Veamos
"Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el capítulo VIII de título XIII del Código de Procedimiento Civil.
En toda actuación administrativa o judicial, vinculada con el ámbito de aplicación de la presente ley, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho de que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original" (artículo 10).
Al hacer referencia a la definición de documentos del Código de Procedimiento Civil, le otorga al mensaje de datos la calidad de prueba, permitiendo coordinar el sistema telemático con el sistema manual o documentario, encontrándose en igualdad de condiciones en un litigio o discusión jurídica, teniendo en cuenta para su valoración algunos criterios como: confiabilidad, integridad de la información e identificación del autor.

Criterio para valorar probatoriamente un mensaje de datos. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad de 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 11).

4.Los cargos globales

Son dos los reparos que generan el cuestionamiento de constitucionalidad que plantea la demandante a saber: que las entidades certificadoras, estarían dando fe pública en Colombia, cuando esta función está reservada constitucionalmente de manera exclusiva a los notarios, según es su entendimiento del artículo 131 de la Carta Política (i) y que se habrían desconocido los artículos 152 y 153 Superiores al haberse modificado el Código de Procedimiento Civil por la vía de una ley ordinaria cuando, según su afirmación, ha debido hacerse por Ley Estatutaria.

Así las cosas, le corresponde en esta oportunidad a esta Corporación determinar si constitucionalmente la fé pública es una función privativa de los Notarios. Y si las modificaciones a los medios de prueba previstos en el Código de Procedimiento Civil son materia reservada a la Ley Estatutaria. A ello, seguidamente se procederá.

La supuesta invasión de la función notarial y la libertad del Legislador para regular el servicio notarial

No considera la Corte que para el esclarecimiento de los cargos lo relevante sea definir la naturaleza de la actividad que realizan las entidades de certificación, pues aunque su carácter eminentemente técnico no se discute, comoquiera que se desprende inequívocamente del componente tecnológico que es característico de los datos electrónicos, es lo cierto que participa de un importante componente de la tradicional función fedante, pues al igual que ella, involucra la protección a la confianza que la comunidad deposita en el empleo de los medios electrónicos de comunicación así como en su valor probatorio, que es lo realmente relevante para el derecho, pues, ciertamente es el marco jurídico el que crea el elemento de confianza.

Y, a su turno, la confianza es la variable crítica para incentivar el desarrollo progresivo de las vías electrónicas de comunicación conocidas como correo electrónico y comercio electrónico, pues es el elemento que

permite acreditarlos como un medio seguro, confiable y, de consiguiente, apto para facilitar las relaciones entre los coasociados.

E, indudablemente, es esta zona de frontera la que produce la inquietud que lleva a la ciudadana demandante a cuestionar su constitucionalidad.

En efecto, ya quedó expuesto, el servicio de certificación a cargo de las entidades certificadoras propende por proporcionar seguridad jurídica a las transacciones comerciales por vía informática, actuando la entidad de certificación como tercero de absoluta confianza, para lo cual la ley le atribuye importantes prerrogativas de certificación técnica, entendiendo por tal, la que versa, no sobre el contenido mismo del mensaje de datos, sino sobre las características técnicas en las que este fue emitido y sobre la comprobación de la identidad, tanto de la persona que lo ha generado, como la de quien lo ha recibido.

Es, pues claro que la certificación técnica busca dar certeza a las partes que utilizan medios tecnológicos para el intercambio de información, en cuanto a la identidad y origen de los mensajes intercambiados. No busca dar mayor jerarquía ni validez a los mensajes de datos de los que pretende un documento tradicional.

A diferencia de los documentos en papel, los mensajes de datos deben ser certificados técnicamente para que satisfagan los equivalentes funcionales de un documento tradicional o en papel y, es allí en donde las entidades de certificación juegan un papel importante.

Las entidades de certificación certifican técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, a saber la confidencialidad, la autenticidad, la integridad y la no repudiación de la información, lo que, en últimas permite inequívocamente tenerlo como auténtico.

La confidencialidad connota aquellos requisitos técnicos mínimos necesarios para garantizar la privacidad de la información.

La autenticidad es la certificación técnica que identifica a la persona iniciadora o receptora de un mensaje de datos.

La integridad es el cumplimiento de los procedimientos técnicos necesarios que garanticen que la información enviada por el iniciador de un mensaje es la misma del que lo recibió.

Y, la no repudiación es el procedimiento técnico que garantiza que el iniciador de un mensaje no puede desconocer el envío de determinada información.

En abundante jurisprudencia, esta Corte ya ha tenido oportunidad de precisar que el legislador goza de una amplia libertad para regular el servicio notarial, lo cual es de por sí un argumento suficiente para desechar los cargos de la demandante quien, en sentir de esta Corte, ciertamente confunde la competencia que el legislador tiene para reglamentar el servicio público que prestan los notarios y registradores, al tenor de lo preceptuado por el artículo 131 Constitucional, con la asignación a estos de la función fedante como una atribución constitucional privativa y excluyente, por lo cual, encuentra que asiste razón tanto al Ministerio Público como a los intervinientes, al señalar que este cargo parte de un supuesto equivocado.

De otra parte, resulta también pertinente señalar que conforme a lo preceptuado por los artículos 2º., 210 y 365 de la Carta Política, el legislador está constitucionalmente habilitado para conferir transitoriamente el ejercicio de funciones públicas a los particulares, lo cual, permite concluir que, también por este aspecto, la Ley acusada, en cuanto faculta a las personas jurídicas privadas a prestar el servicio de certificación, tiene pleno sustento constitucional.

Así las cosas, aún cuando las funciones de las entidades certificadoras de que trata la Ley 527 de 1999 se asociaran con la fe pública, no por ello serían inconstitucionales, pues, como ya se dijo, el legislador bien puede atribuírselas a dichas entidades en su condición de entes privados, sin que ello comporte violación del artículo 131 de la Carta.

Entrar a calificar como función pública o servicio público las atribuciones que la Ley 527 de 1999 otorgó a las entidades certificadoras, no es en modo alguno asunto relevante para este examen comoquiera que su sustento constitucional es ajeno a esa categorización.

Como lo tiene establecido esta CortSentencia C-741 de 1998, M.P. Dr. Alejandro Martínez Caballero en su jurisprudencia:

"...

En efecto, independientemente del debate doctrinal y jurisprudencial sobre la naturaleza jurídica de los notarios en el ordenamiento legal colombiano, es claro que constitucionalmente estas personas ejercen una función pública Además, no es cierto que la Constitución ordene, como equivocadamente lo indica el actor, que este servicio debe ser prestado por particulares, por cuanto la ley puede radicar la función fedante en determinadas instituciones estatales y conferir por ende a los notarios la calidad de servidores públicos Nada en la Carta se opone a

esa posible regulación, puesto que la Constitución en manera alguna ordena que los notarios deban ser particulares y que este servicio deba ser prestado obligatoriamente mediante una forma de descentralización por colaboración, puesto que es también posible que la ley regule de manera diversa el servicio notarial y establezca que los notarios y sus subalternos adquieren la calidad de servidores públicos. La Constitución confiere entonces una amplia libertad al Legislador para regular de diversas maneras el servicio notarial, puesto que el texto superior se limita a señalar que compete a la ley la reglamentación del servicio que prestan los notarios y registradores, así como la definición del régimen laboral para sus empleados (CP art. 131). Por consiguiente, bien puede la ley atribuir la prestación de esa función a particulares, siempre y cuando establezca los correspondientes controles disciplinarios y administrativos para garantizar el cumplimiento idóneo de la función; sin embargo, también puede el Legislador optar por otro régimen y atribuir la prestación de ese servicio a funcionarios públicos vinculados formalmente a determinadas entidades estatales.

..."

5. Los acusados artículos 9°. a 15 y 28 y la supuesta violación de los artículos 151 y 152 de la Constitución Política

Argumenta la interviniente que la Ley 527 de 1999 y, particularmente los artículos 9 al 15, así como el 28, modifican y adicionan el Código de Procedimiento Civil en cuanto a los medios de prueba y a su valor probatorio, lo que en su sentir, ha debido hacerse mediante el trámite y las mayorías propias de una Ley Estatutaria, en cuanto implica una reforma a la Ley Estatutaria de la Administración de Justicia.

Así, pues, en el entendimiento de la demandante, todo aspecto sustantivo o procesal relacionado con la Administración de Justicia estaría reservado al ámbito de la Ley Estatutaria, según su lectura del artículo 152 de la Carta Política.

A juicio de la Corte este cargo también se basa en una premisa equivocada, comoquiera que la accionante parte de un erróneo entendimiento acerca del ámbito material que constituye la reserva de la Ley Estatutaria sobre la Administración de Justicia.

No es necesario un análisis detallado acerca de la naturaleza jurídica de las leyes estatutarias y de las materias a ellas asignadas por el artículo 152 constitucional, pues ya la Corte se ha ocupado con suficiencia del tema y ha establecido en múltiple y reiterada jurisprudencia que

únicamente aquellas disposiciones que de una forma y otra se ocupen de afectar la estructura de la administración de justicia, o de sentar principios sustanciales o generales sobre la materia, deben observar los requerimientos especiales para este tipo de leyes.

Las demás y en particular los códigos, deben seguir el trámite ordinario previsto en la Carta Política, pues se tratan de leyes ordinarias dictadas por el Congreso de la República en virtud de lo dispuesto en el numeral 2 del artículo 150 Superior.

En otros términos, la reserva de Ley estatutaria no significa que toda regulación que se relacione con los temas previstos en el artículo 152 de la Carta Constitucional deba someterse a dicho trámite especial.

Tal conclusión conduciría al absurdo extremo de que toda norma relacionada con cualquier aspecto de la administración de justicia, tendría que aprobarse bajo los estrictos requisitos de las leyes estatutarias, lo cual entrabaría gravemente la función legislativa y haría inane la función de expedir códigos en todos los ramos de la legislación y la de reformar las leyes preexistentes que el Constituyente también atribuye al Congreso, y que este desarrolla por medio de la ley ordinaria.

De ahí que esta Corte, en su jurisprudencia, haya sostenido que la interpretación de los asuntos sometidos a reserva de ley estatutaria debe ser restrictiva a fin de garantizar, entre otras cosas, la integridad de la competencia del legislador ordinario.

Es suficiente, para los efectos de este fallo, recordar las precisiones que, acerca del contenido propio de la Ley Estatutaria de la Administración de Justicia, la Corporación consignó en la sentenciM.P. Dr. Vladimiro Naranjo Mesa. C-037 de febrero 5 de 1996 al referirse al campo propio de la Ley ordinaria.

Dijo entonces la Corporación:

"... Para la Corte, una ley estatutaria encargada de regular la administración de justicia, como lo dispone el literal b) del artículo 152 superior, ***debe ocuparse esencialmente sobre la estructura general de la administración de justicia y sobre los principios sustanciales y procesales que deben guiar a los jueces en su función de dirimir los diferentes conflictos o asuntos que se someten a su conocimiento***

De conformidad con lo anterior, esta Corporación entiende que el legislador goza, en principio, de la autonomía suficiente para definir cuáles aspectos del derecho deben hacer parte de este tipo de leyes. Sin embargo, debe señalarse que ***esa habilitación no incluye la facultad de***

consagrar asuntos o materias propias de los códigos de procedimiento, responsabilidad esta que se debe asumir con base en lo dispuesto en el numeral 2o del artículo 150 superior, es decir, a través de las leyes ordinarias. *Con todo, debe reconocerse que no es asunto sencillo establecer una diferenciación clara y contundente respecto de las materias que deben ocuparse uno y otro tipo de leyes. Así, pues, resulta claro que, al igual que ocurre para el caso de las leyes estatutarias que regulan los derechos fundamentales (literal A del artículo 152),* ***no todo aspecto que de una forma u otra se relacione con la administración de justicia debe necesariamente hacer parte de una ley estatutaria. De ser ello así, entonces resultaría nugatoria la atribución del numeral 2o del artículo 150 y, en consecuencia, cualquier código que en la actualidad regule el ordenamiento jurídico, o cualquier modificación que en la materia se realice, deberá someterse al trámite previsto en el artículo 153 de la Carta.***

...

Y, más adelante se lee:

"...

Las consideraciones precedentes sirven, además, de fundamento para advertir la inconveniencia de permitir al legislador regular aspectos propios de ley procesal en una ley estatutaria, pues es sabido que el trámite de este tipo de normatividad reviste características especiales *- aprobación en una sola legislatura, votación mayoritaria de los miembros del Congreso, revisión previa de la Corte Constitucional-,* ***las cuales naturalmente no se compatibilizan con la facultad que le asiste al legislador para expedir o modificar códigos a través de mecanismos eficaces –es decir, mediante el trámite ordinario-, en los eventos en que las necesidades del país así lo ameriten. Permitir lo contrario sería tanto como admitir la petrificación de las normas procesales y la consecuente imposibilidad de contar con una administración de justicia seria, responsable, eficaz y diligente.*** *(Subrayas fuera de texto)*

... "

no todo aspecto que de una forma u otra se relacione con la administración de justicia debe necesariamente hacer parte de una ley estatutaria. De ser ello así, entonces resultaría nugatoria la atribución del numeral 2o del artículo 150 y, en consecuencia, cualquier código que en la actualidad regule el ordenamiento jurídico, o cualquier

modificación que en la materia se realice, deberá someterse al trámite previsto en el artículo 153 de la Carta.

...

Recuérdese que la misma Carta autoriza al Congreso a expedir, por la vía ordinaria, Códigos en todos los ramos de la legislación, por lo cual, mal puede sostenerse que toda regulación de los temas que han sido objeto de ley estatutaria, haga forzoso el procedimiento restrictivo y más exigente previsto por el Constituyente para su formación. Se reitera: el propósito de las Leyes Estatutarias no es el de regular en forma exhaustiva la materia que constituye su objeto.

6. La unidad Normativa

De otra parte, la Corte encuentra que el artículo 4°. del Decreto 266 del 2000, expedido por el Presidente de la República en ejercicio de las facultades extraordinarias conferidas por el numeral 5°. del artículo 1°. de la Ley 573 del 7 de febrero del 2000, conforma unidad normativa con el artículo 10 de la acusada Ley 527 de 1999, dada su identidad de contenido.

Ciertamente, el artículo 4°. de la Ley 573 del 7 de febrero del 2000 dispone:

Artículo 4°. Medios tecnológicos. Modificase el artículo 26 del decreto 2150 de 1995, el cual quedará así:

"Artículo 26. Medios tecnológicos Se autoriza a la Administración Pública el empleo de cualquier medio tecnológico o documento electrónico, que permita la realización de los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa, así como el establecimiento de condiciones y requisitos de seguridad que cada caso sean procedentes, sin perjuicio de las competencias que en la materia tengan algunas entidades especializadas.

Toda persona podrá en su relación con la administración hacer uso de cualquier medio técnico o electrónico, para presentar peticiones, quejas o reclamaciones ante las autoridades. Las entidades harán públicos los medios de que dispongan para permitir esta utilización.

Los mensajes electrónicos de datos serán admisibles como medios de prueba y su fuerza probatoria será la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección III Libro Segundo del Código de procedimiento Civil, siempre que sea posible verificar la identidad del remitente, así como la fecha de recibo del documento.

Por su parte el artículo 10 de la Ley 527 de 1999, preceptúa:

*"**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."

Por consiguiente y en vista de que se presenta el fenómeno jurídico de unidad de materia entre el artículo 10 de la Ley 527 de 1999 acusado y el artículo 4 del Decreto 266 del 2000 dictado con base en las facultades extraordinarias establecidas en la Ley 573 del 2000, pues regulan un mismo aspecto, esto es, el valor probatorio de los mensajes electrónicos, la Corte estima que la declaratoria de constitucionalidad comprenderá también al artículo 4°. del Decreto 266 del 2000 por las razones atrás referidas.

Es pues, del caso, extender el pronunciamiento de exequibilidad, en cuanto hace al cargo examinado, también a la norma últimamente mencionada. Así se decidirá.

VII.D E C I S I Ó N

En mérito de lo expuesto, la Corte Constitucional, en nombre del pueblo y por mandato de la Constitución,

R E S U E L V E:

Primero.-En cuanto a los cargos examinados, **DECLÁRANSE EXEQUIBLES** los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999.

Segundo.- Declarar **EXEQUIBLE** el artículo 4°. del Decreto 266 del 2000 dictado en ejercicio de las facultades extraordinarias establecidas en la Ley 573 del 2000, conforme a la parte motiva de esta providencia.

Cópiese, notifíquese, comuníquese a quien corresponda, publíquese, insértese en la Gaceta de la Corte Constitucional, archívese el expediente y cúmplase.

ALEJANDRO MARTINEZ CABALLERO
Presidente
ANTONIO BARRERA CARBONELL

Magistrado
ALFREDO BELTRAN SIERRA
Magistrado
EDUARDO CIFUENTES MUÑOZ
Magistrado
CARLOS GAVIRIA DIAZ
Magistrado
JOSE GREGORIO HERNANDEZ GALINDO
Magistrado
FABIO MORON DIAZ
Magistrado
VLADIMIRO NARANJO MESA
Magistrado
ALVARO TAFUR GALVIS
Magistrado

FIGURAS

Fig.1 Gráfica representativa del conocimiento sobre la normativa penal existente en materia de documentos electrónicos

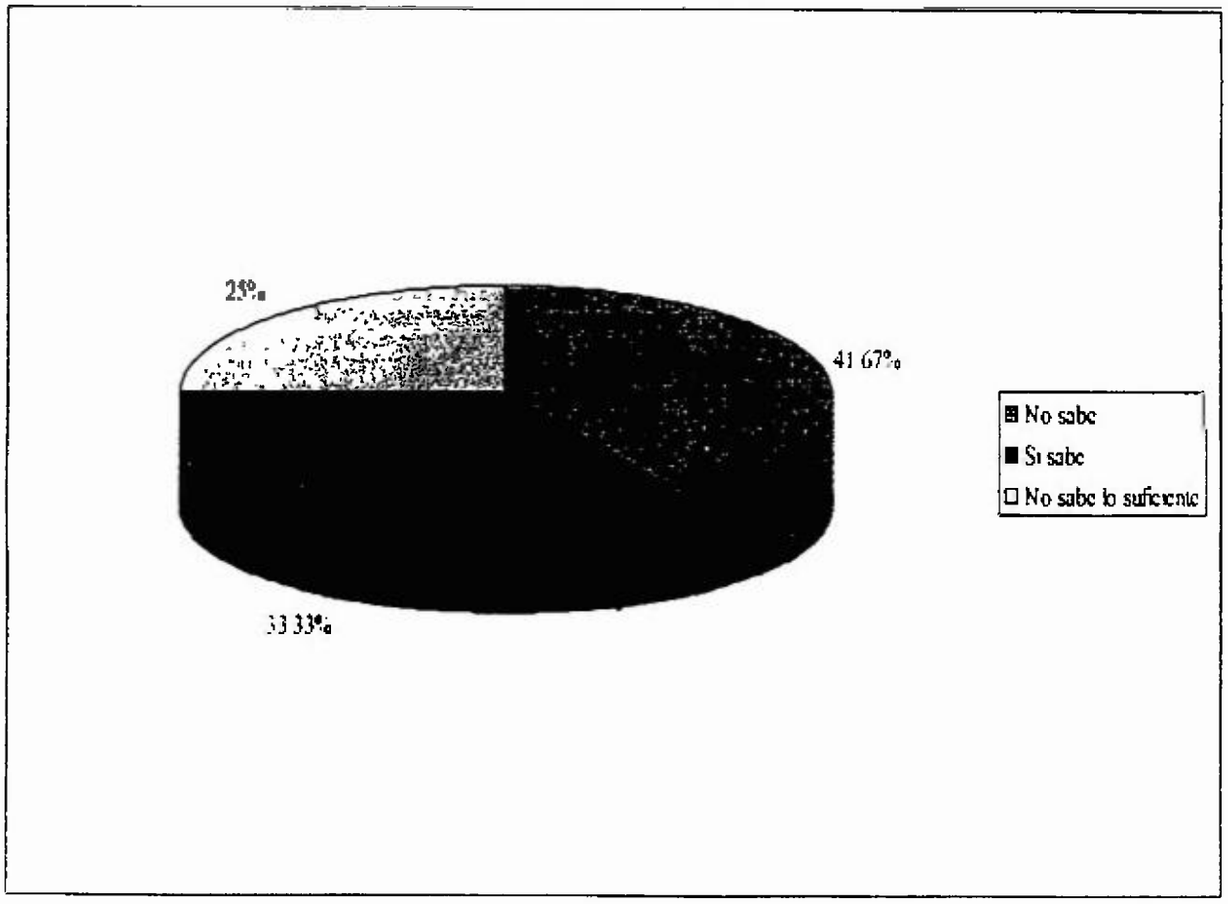


Fig 2 Gráfica representativa del conocimiento de la normativa administrativa relacionada con protección de documentos electrónicos

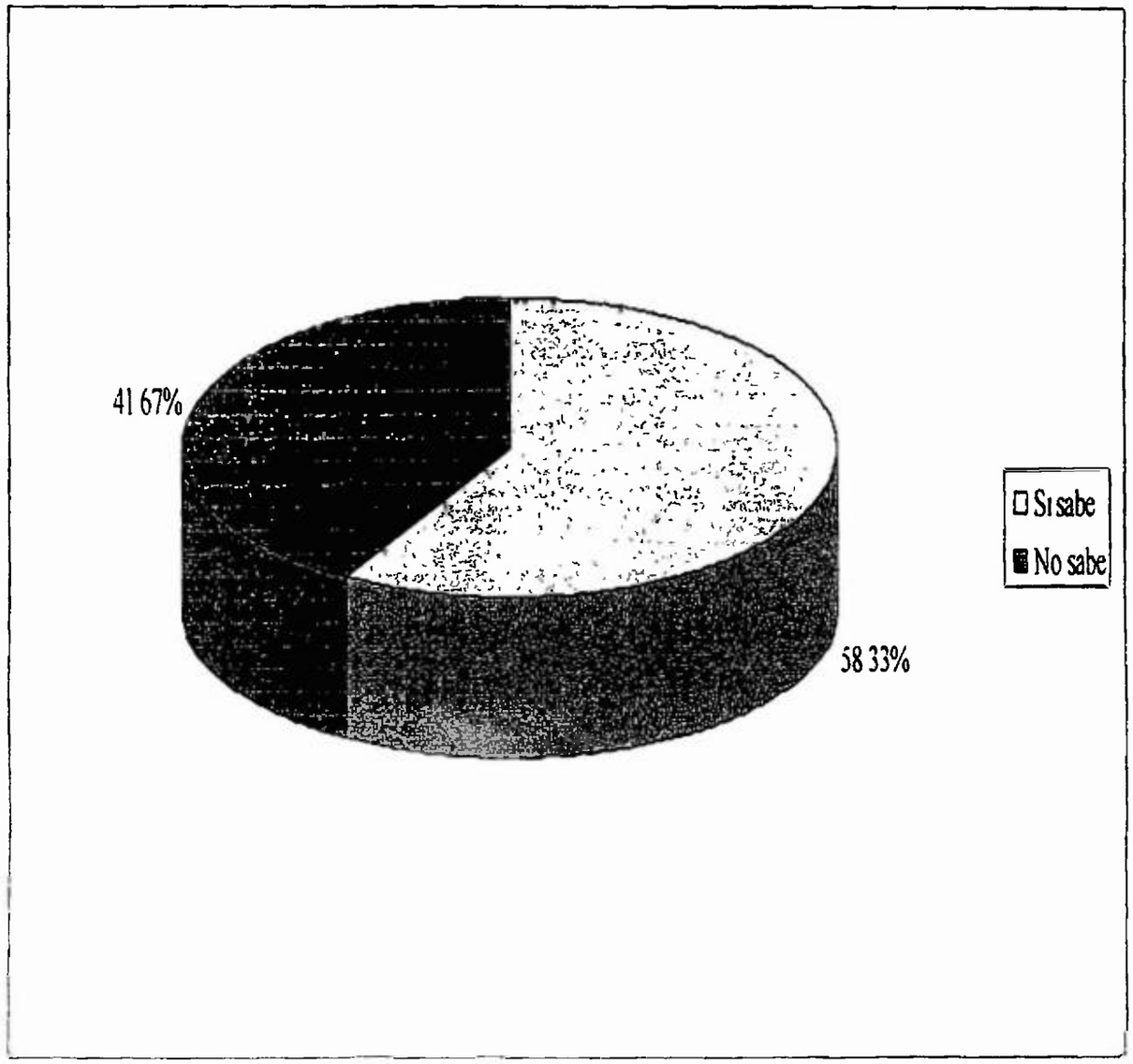


Fig 3 Causas de falsificación de documentos electrónicos

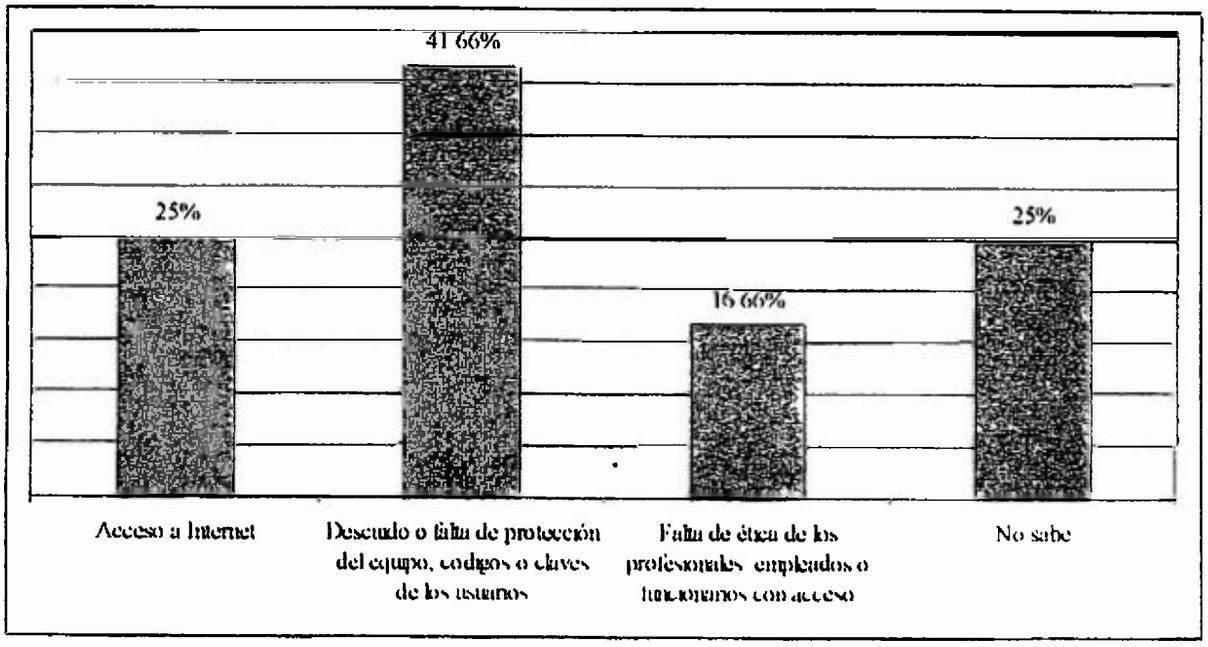
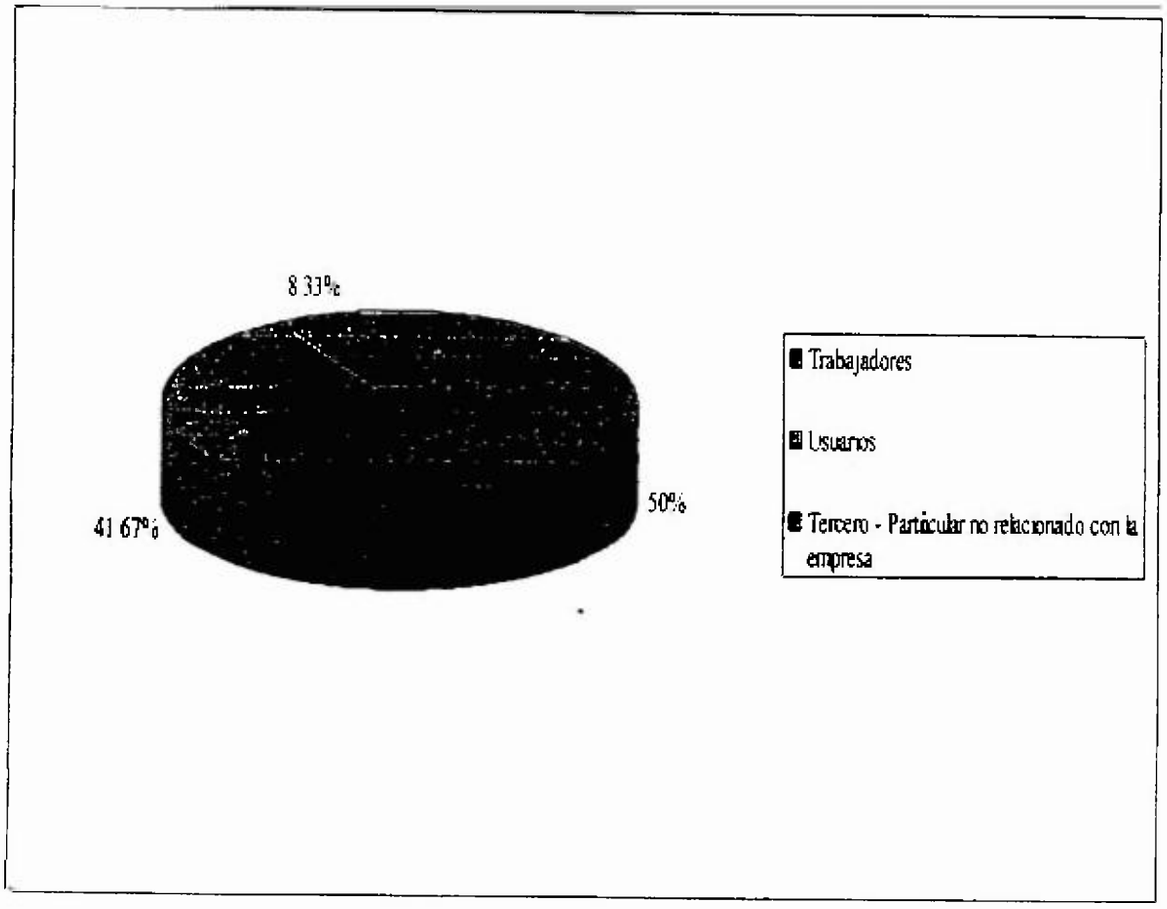


Fig 4 Gráfica representativa por experiencia, del sujeto que ejecuta algún tipo de documentos electrónicos



Delitos informáticos: llegan los forenses

Por BBC News Online

Los médicos forenses suelen decir que el cadáver habla. Cuando llegan a la escena del crimen, estos investigadores saben que el cuerpo de la víctima puede ser su mejor testigo.

¿Pero qué pasa cuando el lugar del crimen es una oficina y el arma del delito es una computadora? Ahí llegan los forenses informáticos.

Muy solicitados en los últimos tiempos en los estados Unidos y gran parte de Europa, estos expertos informáticos ayudan a médicos legistas a extraer toda la información posible de los discos duros sobre todo la que ha sido borrada.

Como señala el experto del grupo Control de Riesgos Peter Yapp, en los casos de fraude corporativo o fraudes contra los inversionistas, los investigadores pueden determinar a partir de un trabajo exhaustivo en los recovecos de las computadoras cuánto sabían los directores de todo lo que estaba pasando.

Además de los trapos sucios de las corporaciones, los forenses de las computadoras hacen de todo un poco.

No siempre es tan fácil escapar

LA PRUEBA DEL DELITO

Los investigadores saben que la tecla de delete no alcanza para hacer desaparecer los archivos incriminatorios. Y consideran que una vez que un documento ha sido salvado, es casi virtualmente imposible borrarlo para siempre.

La computadora está conectada a una red interna, como en la mayoría de las oficinas, limpiar la prueba del delito es aún más difícil.

"Es posible que uno pueda controlar su propia computadora

...un lugar no tan inaccesible como muchos piensan.

y al borrar algo haya muchas posibilidades de que ese archivo desaparezca", explica el investigador de fraudes financieros Simon Dawson.

"Pero si tu terminal está conectada a una red existe una gran cantidad de lugares a donde la información puede dirigirse. Podría estar en cualquier lugar alrededor del mundo".

Deshacerse de un cadáver suele ser una tarea complicada para los asesinos, borrar un archivo para siempre no parece ser mucho más fácil.

Fuente: www.bbcmundo.com

EDITORA PANAMÁ AMÉRICA, S.A.
Avenida Ricardo J. Alfaro, al lado de [illegible]
Apdo. B-4, zona 9-A Panamá, República de Panamá
[illegible]
COMPUTERWORLD
es publicado por IDG
CON LICENCIA DE
Impreso en Panamá por: Editora Panamá América S.A. Distribuido por: El Panamá América

Robo de identidad cuestiona la seguridad

Por Paul Roberts
News Service de Boston
STON, MASSACHUETTS

Se afirma que durante ese tiempo Cummings utilizó su acceso a las cuentas de clientes de TCI para copiar las claves y los códigos de abono que utilizan muchas empresas suscritas, que incluyen bancos y financieras como Ford Motor Credit Corp

Luego Cummings y otros usaron esa información para hacerse pasar como empleados legítimos de las instituciones financieras y para descargar el historial crediticio de miles de consumidores, a lo largo de dos años, según una denuncia revelada por James Comey, procurador federal del distrito sur de Nueva York. Cummings luego vendió esos informes, según la fiscalía federal.

Aún más alarmante es que después de robar claves parece que Cummings pudo continuar usando la información obtenida en su empleo en TCI mucho después de haber renunciado a la empresa en marzo de 2000, y hasta entregó a uno de sus cómplices una laptop con el software de TCI y con contraseñas para descargar informes crediticios a voluntad.

En un comunicado TCI reconoció que había empleado a Cummings, pero declinó hacer comentarios sobre la demanda pendiente contra su ex-empleado.

Un vocero de la fiscalía federal dijo que TCI estaba cooperando con la investigación pero declinó responder preguntas sobre cuándo la compañía advirtió el fraude o si Cummings utilizaron bienes de TCI para el robo de identidad.

Detrás de la aparentemente deficiente seguridad de TCI hay un problema aún más serio sobre las normas de seguridad establecidas por las tres organizaciones de informes crediticios más importantes Experian, Equifax y TransUnion, dicen los expertos en seguridad.

Las tres compañías fueron objetivos de Cummings y sus cómplices. Todas estas empresas permiten a los clientes que usan el software de TCI descargar informes crediticios de los consumidores de sus masivas bases de datos con una contraseña válida y un código de abonado que es exclusivo para cada cliente o sucursal.

No obstante, dado que ambos datos son aparentemente accesibles a los empleados de la mesa de ayuda de TCI, las tres agencias quedaron vulnerables a un ataque "interno" desde TCI o de uno de los clientes de esa empresa, dicen los expertos.

"Lo que esto muestra realmente es la vulnerabilidad general del sistema", dijo Chris Kelly, analista de Forrester Research Inc.

"Durante los últimos años, la atención a la privacidad del consumidor se ha concentrado en Internet. Pero pareciera que esta vez los datos fueron obtenidos con un recurso de baja tecnología, sencillamente (Cummings) tenía acceso a los códigos".

A pesar de la delicada información que contienen sus bases de datos, las tres mayores agencias estadounidenses de informes crediticios no parecen haber instalado una protección firme al acceso de estos datos desde el exterior, dijeron los expertos.

"Es bien sabido en la industria de la seguridad que las claves o contraseñas son la forma de protección más débil", dijo Randy Vanderhoof, director ejecutivo de Smart Card Alliance, una organización que promueve el uso de la tecnología de tarjetas inteligentes.

"Una vez que se emite una contraseña no hay ninguna manera de determinar si esa clave ha pasado a otros individuos".

Las denuncias presentadas contra Cummings y sus cómplices muestran que ellos aprovecharon a fondo esta debilidad.

Después de mudarse de Nueva York a Georgia, se cree que Cummings viajó durante algún tiempo entre los dos estados para reunirse con Linus Baptiste, un cómplice que ahora está cooperando con las autoridades, para descargar informes crediticios. Después, Cummings suministró a Baptiste una laptop con el software, aunque continuó en posesión de las contraseñas de los clientes y códigos de abonado.

Cuando las actividades de Baptiste llamaron la atención de las organizaciones de crédito, que cambiaron las contraseñas, Cummings dio por teléfono los códigos necesarios de una de las tres agencias, lo que le permitió seguir descargando informes crediticios.

Se supone que Cummings y Baptiste han llamado a las tres mayores agencias crediticias de Nueva York, haciéndose pasar como los empleados de empresas verdaderas de Ohio, Texas, Florida, Michigan y otros estados

Vanderhoof dijo que si se usara tecnología como las tarjetas inteligentes -elaboradas tarjetas de seguridad, generalmente con chips y que pueden almacenar una variedad de datos, desde claves a información biométrica- ese proceder hubiera sido imposible.

Ese sistema hubiera requerido que el dueño de la tarjeta estuviese físicamente presente, conjuntamente con un lector de tarjetas, para utilizar el software TCI software y descargar informes, y de este modo hubiera evitado la fácil diseminación de contraseñas que permitió poner en riesgo tantas cuentas de los consumidores, según Vanderhoof

También se hubiera utilizado un único punto de acceso que podría haber sido desactivado fácilmente cuando se detectó el fraude por primera vez, dijo Vanderhoof.

Al final fue la codicia, más que los controles internos, los que expusieron la maniobra delictuosa. Según un vocero de la fiscalía federal, el fraude fue descubierto por primera vez cuando una filial de Ford Motor Credit Corp. tomó contacto con el Buró Federal de Investigaciones cuando Experian le facturó más de 15,000 informes no autorizados.

Una vez que supieron sobre las descargas ilegales, Experian y las otras agencias pudieron identificar la fuente del fraude sólo después de investigar sus bases de datos en busca de solicitudes masivas de informes, y correlacionarlos con los códigos de usuario hurtados

Una investigación sobre los registros telefónicos vinculó las descargas dolosas a los números de teléfono de Baptiste y de otros cómplices, según las denuncias hechas públicas la semana pasada

No hubo respuesta por parte de Experian ni de Equifax a las llamadas telefónicas en busca de sus comentarios, y no está claro si se tomarán medidas para resolver las deficiencias expuestas por Cummings, Baptiste y sus secuaces

Vanderhoof afirmó que la magnitud del robo de identidad puede obligar al gobierno federal a observar más de cerca al sector de los informes crediticios, al igual que las muy publicitadas fugas de información personal de los hospitales y compañías de seguros provocó en 1996 la sanción de una ley al respecto, la llamada Health Insurance Portability and Accountability Act (HIPAA)

"Como resultado de esta ley el sector de la atención sanitaria ha debido invertir en una nueva infraestructura tecnológica para proteger la información de los pacientes. Parece que ocurrirá algo similar en los mercados financieros y en el sector de informes crediticios si no se suprime este tipo de fraude", dijo Vanderhoof

Pero por ahora, Kelly de Forrester Research dijo que el hurto de tantos informes crediticios de las principales agencias de informes del país obliga aún más a los consumidores a verificar si no se ha violado su información financiera.

Kelly recomendó que todos los consumidores pidan un ejemplar actualizado de su informe crediticio.

En algunos estados, los ciudadanos pueden solicitar gratuitamente el propio informe crediticio una vez por año calendario, dijo Kelly.

Al recibirlo, el consumidor debe verificar que no se hayan registrado actividades extrañas, como la emisión de nuevas tarjetas de crédito, o saldos no justificados, dijo Kelly

"Lo importante es detectar la actividad antes de que se salga de control", dijo Kelly

Peligroso nuevo gusano Winevar

Por Paul Roberts
IDG News Service de Boston

BOSTON, MASSACHUSETTS

Está circulando un nuevo gusano de correo electrónico que podría dañar seriamente los equipos infectados, con la posibilidad de borrar todos los archivos de la computadora, mientras se burla del usuario, dicen advertencias emitidas de varios productores de software antivirus.

El nuevo gusano se llama Winevar y fue detectado primeramente en Corea del Sur. Posiblemente, su lanzamiento debía coincidir con la convención de investigadores antivirus del Asia (AVAR), que se realizó en Seúl, Corea del Sur, hace dos semanas, según un comunicado de advertencia distribuido por la empresa de seguridad F-Secure Corp., con sede en Helsinki.

Los mensajes de correo electrónico portadores del gusano pueden mostrar el asunto "Re: AVAR (Association of Anti-Virus Asia Researchers)", según F-Secure.

El gusano es también conocido por otros nombres, por ejemplo: W32/Winevar.un, W32/Korvar, W32/Winevar@mm, I-Worm.Winevar, y el "Gusano Coreano" ("Korean Worm").

Según los informes, el gusano parece ser una variante del reciente gusano Bridex o "Braid".

Al igual que éste, Winevar aprovecha la conocida vulnerabilidad IFRAME del "browser" para la Web Internet Explorer y de los clientes de correo electrónico como Outlook y Outlook Express, todos de Microsoft Corp. Esa vulnerabilidad permite que los adjuntos a mensajes de correo electrónico en formato HTML sean abiertos sin la intervención del usuario.

Al igual que Bridex, Winevar inserta una variante del virus Funlove en los equipos infectados, e intenta cerrar los procesos usados por el software antivirus. Según un comunicado de advertencia de Kaspersky Labs Ltd., con sede en Moscú, hay signos de que el gusano podría también estar programado

para realizar un ataque de denegación de servicio contra el sitio Web del productor de software antivirus Symantec Corp.

Winevar se propaga buscando entre los archivos del correo electrónico y extrayendo las direcciones. El gusano utiliza luego el protocolo SMTP (Simple Mail Transport Protocol) para enviar copias de sí mismo a esas direcciones, utilizando series de números al azar para disimular el nombre del adjunto portador del gusano, lo que complica más la identificación de los mensajes de correo electrónico infectados.

Mientras Bridex sencillamente recogía información de los sistemas infectados, Winevar puede causar verdadero daño.

Cuando se reinician los equipos infectados el gusano muestra un mensaje titulado "Make n fool of oneself" ("Comportarse como tonto") con el mensaje "What a foolish thing you have done!" ("¡Qué cosa estúpida acabas de hacer!") Al hacer clic sobre el botón Aceptar se borran todos los archivos del disco duro que no estén abiertos en ese momento, según los comunicados de prevención.

Ya se han conocido infecciones causadas por Winevar, según Kaspersky Labs.

Las empresas de antivirus más importantes han presentado definiciones actualizadas del nuevo gusano e instrucciones para eliminarlo de las máquinas infectadas. Los usuarios que sospechen padecer la infección no deben reiniciar su máquina antes de eliminar los archivos del gusano

Además, Microsoft ha emitido un parche para la vulnerabilidad IFRAME que usa Winevar (http://www.microsoft.com/windows/ie/downloads/critical/q323759ie/default.asp), así como una vulnerabilidad de ActuveX utilizada por Winevar (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-075.asp) ◗

¿QUÉ DICEN?

UNISYS

❖ Culpó al Tribunal Electoral por no remitirles un manual de procedimientos que garantizara la seguridad y el manejo de los plásticos base para la elaboración de las cédulas digitalizadas

❖ De los 30 mil plásticos defectuosos, solo 5 mil fueron retirados de sus bodegas y capturados por la Fiscalía Auxiliar. Los restantes 29 mil 500 quedaron "debidamente almacenados" en las bodegas contratadas por Unisys en Panamá.

Jorge Villalobos, representante de Unisys World Trade, Inc.

❖ Aseguran que "ninguna cédula fue falsificada" con el material extraviado.

❖ La razón por la que no regresaron los plásticos con números de serie duplicados se debió a que Silcox (la empresa fabricante) había entrado en bancarrota.

❖ Silcox cerró y dejó en sus bóvedas plásticos terminados y en proceso de producción, sin notificarles. El material fue descubierto por Unisys y se encuentra en una de sus bodegas de seguridad en Estados Unidos a disposición de las autoridades panameñas.

TRIBUNAL ELECTORAL

...rdo Valdés Jery, magistrado ...iente del T...

❖ Declaró "urgencia nacional" debido a la crisis surgida por el extravío de los plásticos para confeccionar las cédulas digitalizadas. Anunció que tendrá que reemplazar 700 mil cédulas digitalizadas.

❖ Acusó a los empleados de Unisys World Trade Inc. de pretender "hacer un negociado con los 30 mil plásticos que ... institución les devolvió ... eran destruidos. El ... octubre, el TE devolvió a ... presa Unisys un to... de ... icos defectuosos para cédulas, ya que tenían n... duplicada. En vez de ser destruidos, los p... ...cieron en los depósitos de Unisys sin ... provocó la pérdida de miles de unidades.

Citó a los representantes de Unisys para que defi... ...vés de un acuerdo o vía judicial– si arreglará los ...os y perjuicios ocasionados al Tribunal Electoral.

❖ Decidió resolver administrativamente el contrato ... illones de dólares con la empresa Unisys por no r... ...r la carta de crédito bancaria. Corresponderá a la em... sa afianzadora, la Aseguradora Mundial, sustituir al ...ratista y deberá presentar una empresa idónea para que ...ea material de cedulación al Tribunal Electoral.

EL PRESUPUESTO

Valdés confía en que "no se va a gastar ni un dólar más" de lo presupuestado para contratar a la empresa (que aún no se conoce) que suministrará los insumos y la tecnología para confeccionar la nueva cédula.

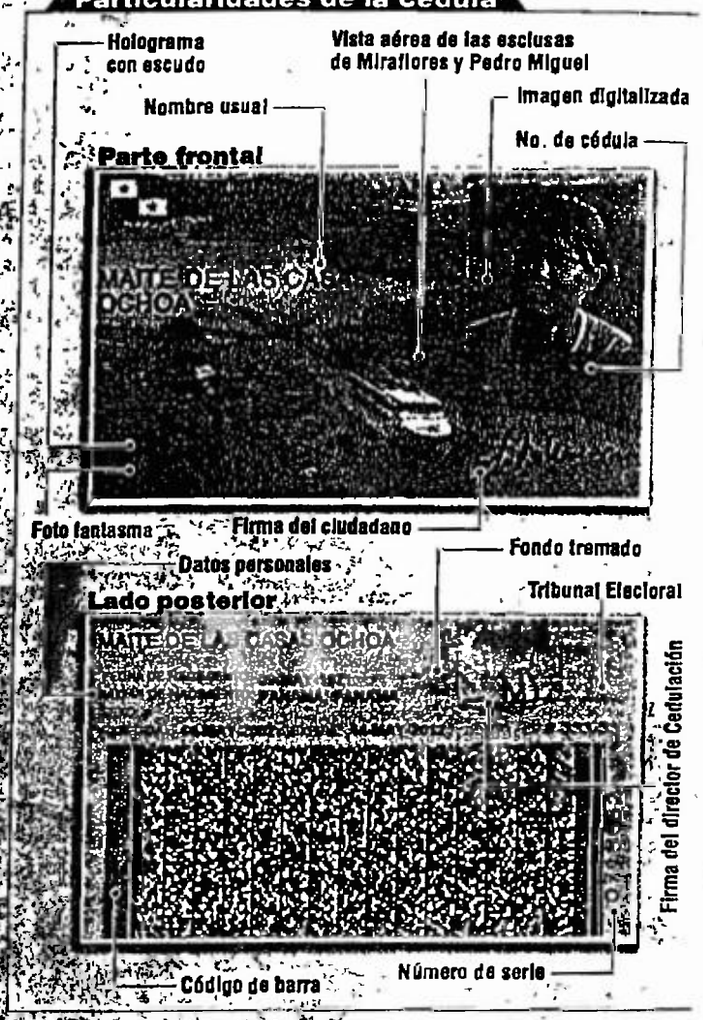
Para hacerle frente al costo que supone el proceso de recedulación, el TE recuperó algunos fondos para sufragarlo.

La institución dispone de los 2 millones 328 mil dólares fijados en el contrato con Unisys Centroamérica, S.A. para el suministro de 2 millones de plásticos necesarios para el programa de cedulación.

Estos fondos quedaron libres después de que el contralor general de la República Alvin Weden decidiera no refrendar la carta de crédito que estaba por ser abierta con el Banco Nacional a favor de Unisys Centroamérica, S.A. y resolver administrativamente el contrato con esa compañía.

Adicionalmente, el Tribunal Electoral tiene previsto ...orrar parte del presupuesto ... 0.5 millones destinado ... los comicios del 2004, ... caso de ...cesario.

Particularidades de la cédula



Es una tarjeta modelo Sillcocks D-VII-40 utilizado en EU para el "green card". Se forma en un substrato único de 40% de poliéster (que le da una durabilidad de 10 años) y PVC que mejora la calidad de impresión. Sin embargo, tras los recientes acontecimientos la vulnerabilidad de la cédula digitalizada quedó al descubierto.

DOS CONTRATOS, DOS UNISYS

En la historia de los plásticos, son dos las compañías protagonistas:

❖ UNISYS WORLD TRADE, INC.

Con base en el estado de Delaware, Estados Unidos, es una subsidiaria de Unisys Corporation, una transnacional que en el tercer cuarto del 2002 obtuvo ingresos por 1.33 billones de dólares.

En 1997 firmó un contrato por 13.9 millones de dólares con el Estado panameño para entregarles un millón de plásticos para la confección de cédulas.

❖ UNISYS DE CENTROAMÉRICA, S.A.

Su centro de operaciones se encuentra en San José, Costa Rica y es también subsidiaria de Unisys Corporation.

La compañía ganó la licitación hace seis años con el Tribunal Electoral de Costa Rica para cambiar las cédulas tradicionales por las electrónicas.

El Tribunal Electoral de Panamá la contrató directamente en julio pasado para el suministro de 2 millones de plásticos e insumos para fabricar cédulas a un costo de 2 4 millones de dólares

La mayoría de los usuarios necesitará velocidades rápidas de descarga para sacar archivos de imágenes y música de los servidores de la Web, entre otro usos. A menos que esté cargando archivos masivos a una agencia de servicio o enviando archivos grandes desde la casa a la oficina, probablemente no necesitará una velocidad de carga superrápida.

Consejo Si usted es un usuario empresarial y debe tener cargas rápidas, considere la SDSL. Esta es una conexión DSL simétrica que provee la misma velocidad en ambas direcciones. Tendrá que pagar más por la conexión, pero también se puede instalar más rápido que una línea ADSL. Esto se debe a que los proveedores que venden SDSL evitan las listas de espera alquilando líneas de la compañía de teléfono.

Tanto ADSL como G.Lite tienen dos conveniencias extraordinarias a su favor. La primera es el precio. Usted puede hacerse de una conexión ADSL por US$30 y US$50 al mes, dependiendo de su ubicación. Si lo hace en el momento adecuado, podría conseguir el módem y la instalación DSL gratuitamente. Por ejemplo, al salir a imprenta, Pacific Bell, Southwestern Bell, Nevada Bell y Ameritech estaban promocionando eso precisamente: US$40 al mes, con la instalación y el módem DSL gratis.

Consejo Manténgase al tanto de los especiales que cada proveedor de DSL en su zona anuncie en sus sitios de Internet.

La segunda característica después del precio (para mí, la decisiva) es que ADSL y G.Lite le permiten usar una línea telefónica para voz y acceso rápido a datos simultáneamente (las conexiones de SDSL son para datos sólo). Ahorrarse el costo de una línea extra de teléfono para un módem normal justifica por sí solo la inversión en la DSL.

VELOCIDAD DE ALTO VUELO

HE AQUÍ cómo comprender las cifras y cómo ponerlas en perspectiva. Su lento módem analógico funciona a 56 kilobits por segundo. La velocidad típica de DSL corriente arriba oscila entre 128 kbps y 384 kbps, potencialmente casi 7 veces más rápido que su módem viejo. Las velocidades corriente abajo se miden en megabits por segundo; una línea de 1 mbps (1000 kbps) es casi 18 veces más rápida.

Las velocidades de ADSL se anuncian comúnmente como 384 kbps corriente abajo y 128 kbps corriente arriba. Esa es la velocidad garantizada, pero a veces es mucho más rápida porque ADSL puede manejar teóricamente velocidades de hasta 8 mbps para descargar y aproximadamente 800 kbps para cargar. (G.Lite es más lento, con descargas que llegan a 1,5 mbps y cargas de 384 kbps).

Los proveedores de DSL pueden garantizar estas velocidades porque son selectivos con sus clientes. La mayoría de ellos solamente acepta pedidos si usted está situado dentro de una distancia específica de la oficina central (OC). Por ejemplo, Pacific Bell y US West quieren que los clientes estén dentro de 5.334 m de la OC, mientras que el límite de Bell Atlantic es sólo de 4.572 m.

Consejo Para determinar los límites que los proveedores de DSL ponen